COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES

Documento Soporte

Diseño Regulatorio

Junio de 2026

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES

1. INTRODUCCIÓN

El presente documento aborda la problemática asociada al fraude en servicios de telecomunicaciones, particularmente aquel que se materializa a través de comunicaciones de voz y mensajes cortos de texto (SMS) tradicionales, mediante prácticas como la suplantación de identidad, la manipulación de identificadores de origen o el uso indebido de redes de telecomunicaciones para contactar a usuarios con fines engañosos. Este fenómeno se caracteriza por su complejidad, en la medida en que involucra múltiples etapas de la cadena de valor y la participación de diversos agentes del ecosistema, lo que requiere un análisis integral que reconozca la naturaleza distribuida del riesgo y las limitaciones para atribuir responsabilidades a un único actor.

En este contexto, el documento tiene como propósito servir de insumo técnico para la evaluación de alternativas regulatorias orientadas a la prevención y mitigación del contacto a usuarios con fines fraudulentos, contribuyendo así al fortalecimiento de la confianza en los servicios de comunicaciones y a la protección de los usuarios. Asimismo, constituye una herramienta para la toma de decisiones por parte de la Comisión y otros grupos de valor, incluyendo proveedores de redes y servicios de telecomunicaciones (PRST), autoridades públicas y diferentes actores del ecosistema digital, al proporcionar un análisis estructurado de las problemáticas identificadas, las alternativas de intervención y su análisis de viabilidad técnica y económica.

De esta manera, el presente documento contribuye al análisis y desarrollo de la estrategia propuesta por la Comisión para la prevención y mitigación de este flagelo, así como a la articulación de acciones entre los distintos actores involucrados en el ecosistema, en línea con los objetivos del proyecto regulatorio.

Para tal efecto, el contenido de este documento se organiza en varias secciones que permiten abordar de manera estructurada la problemática objeto de análisis, teniendo en cuenta los siguientes cuatro ejes generales de intervención: i) Temáticas enfocadas a mitigar el contacto a usuarios con fines fraudulentos mediante SMS; ii) Temáticas enfocadas a mitigar el contacto a usuarios con fines fraudulentos mediante llamadas de voz; iii) Temáticas enfocadas en la educación de la ciudadanía; y iv) Temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación regulatoria .

En el texto se presentan, en primer lugar, los antecedentes relevantes del proyecto; posteriormente, se desarrolla la identificación del problema, incluyendo sus causas y consecuencias. A continuación, se exponen los objetivos del proyecto y el sustento técnico que orienta la evaluación de medidas, así como

el análisis de experiencias internacionales. Finalmente, el documento incorpora de manera secuencial la propuesta regulatoria para cada uno de los ejes de intervención y las temáticas identificadas, lo cual resulta del ajuste de las alternativas regulatorias, publicadas el pasado 21 de noviembre de 2025, a raíz de los diferentes comentarios obtenidos por parte de la industria y los interesados en la etapa de participación, y la descripción y ejecución de la metodología de evaluación de dichas alternativas siguiendo los lineamientos, parámetros y metodologías establecidos para el adecuado desarrollo del Análisis de Impacto Normativo - AIN.

2. ANTECEDENTES

Los antecedentes del presente proyecto muestran que el fraude cibernético a través de servicios móviles de voz y mensajes de texto tradicionales constituye una problemática creciente y de carácter multidimensional, que exige una respuesta regulatoria integral. Desde la perspectiva técnica, se identificó que los servicios de voz y SMS presentan vulnerabilidades que facilitan prácticas como el *vishing*, el *smishing*, la suplantación de la identidad de la línea llamante y el uso irregular de recursos de identificación. En particular, se evidencian limitaciones en la autenticación del originador de las comunicaciones, desafíos de trazabilidad en el ecosistema A2P y la necesidad de fortalecer los mecanismos de monitoreo, detección y control del tráfico atípico.

Desde el punto de vista económico, los antecedentes muestran que estas modalidades de fraude generan afectaciones significativas para los usuarios y para distintos sectores de la economía, especialmente el financiero. La información recopilada evidencia una tendencia creciente en las reclamaciones asociadas a *smishing* y *vishing* en Colombia, así como la existencia de costos relevantes para la implementación de medidas de prevención, monitoreo y control por parte de los agentes del sector.

En el ámbito jurídico y regulatorio, los antecedentes dan cuenta de la evolución de las disposiciones aplicables a la remuneración del servicio de SMS, a la administración de recursos de identificación y al Registro de Números Excluidos (RNE), así como de la necesidad de armonizar estos instrumentos con los objetivos de prevención del fraude. Igualmente, la revisión de experiencias internacionales permitió identificar buenas prácticas orientadas a mitigar la suplantación de llamadas, el envío de mensajes fraudulentos y otras modalidades de contacto indebido a los usuarios, lo cual aporta referentes relevantes para el análisis regulatorio nacional.

En conjunto, estos antecedentes confirman que la problemática no obedece únicamente a la ausencia de reglas, sino también a la limitada efectividad de algunas herramientas existentes frente a un fenómeno dinámico y cambiante. Por esta razón, constituyen el sustento para la evaluación de alternativas regulatorias orientadas a fortalecer la prevención, trazabilidad, control y mitigación del fraude cibernético por medio de servicios móviles.

La consulta detallada de estos antecedentes puede encontrarse en el documento de formulación del problema y en el documento de alternativas de solución disponibles en el micrositio[1] del proyecto regulatorio.

3. PROBLEMA IDENTIFICADO

El 4 de julio de 2025, la CRC publicó para conocimiento y participación de los interesados el documento con la formulación del problema del proyecto regulatorio *Identificación de medidas para mitigar el fraude cibernético por medio de servicios tradicionales de voz y mensajes de texto*[2].

En dicho documento se identificaron las causas y consecuencias que permitieron delimitar la existencia del siguiente problema: «Ausencia de herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto». Posteriormente, con ocasión de la recepción de comentarios al documento de formulación del problema, se identificó la necesidad de modificar la formulación del problema, considerando en que en la regulación general expedida por la CRC a la fecha sí existen algunas herramientas dirigidas a la prevención y contención del fraude. Así las cosas, en el documento de formulación de alternativas regulatorias se modificó la formulación del problema a abordar, de la siguiente forma: «Baja efectividad de las herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto».

El siguiente esquema resume las causas identificadas y las consecuencias que se derivan de la presencia del referido problema.

[1] Disponible en: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-41-7-1
[2] Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 1. Árbol del problema publicado

Fuente: Elaboración CRC

Ahora bien, en este punto resulta necesario resaltar que en el marco del proyecto regulatorio «Esquemas de remuneración mayorista de redes móviles», la Comisión optó por mantener el esquema tarifario vigente aplicable a la mensajería SMS A2P, mientras se adelantaba una revisión integral de este segmento en el proyecto orientado a la mitigación del fraude cibernético, incluyendo el análisis de responsabilidades e incentivos de los agentes que intervienen en la cadena de valor.

En ese contexto, la Comisión identifica como causa adicional del problema que, históricamente, la regulación sobre mensajes cortos de texto (SMS) ha tendido a aplicarse de manera equivalente a los segmentos P2P y A2P, en particular desde la perspectiva de las condiciones de remuneración y del diseño regulatorio asociada a la gestión de ese tráfico. Esta equivalencia regulatoria resulta relevante porque, aunque ambos tipos de mensajería comparten una base técnica común y hacen uso de recursos de red compartidos, la demanda y el comportamiento operativo pueden variar significativamente según el tipo de tráfico cursado (P2P vs. A2P). En especial, el tráfico A2P suele presentar volúmenes mayores y necesidades de entrega más exigentes que generan picos de tráfico y requieren reservas de capacidad (medidas, por ejemplo, en transacciones por segundo – TPS) para sostener la calidad del servicio.

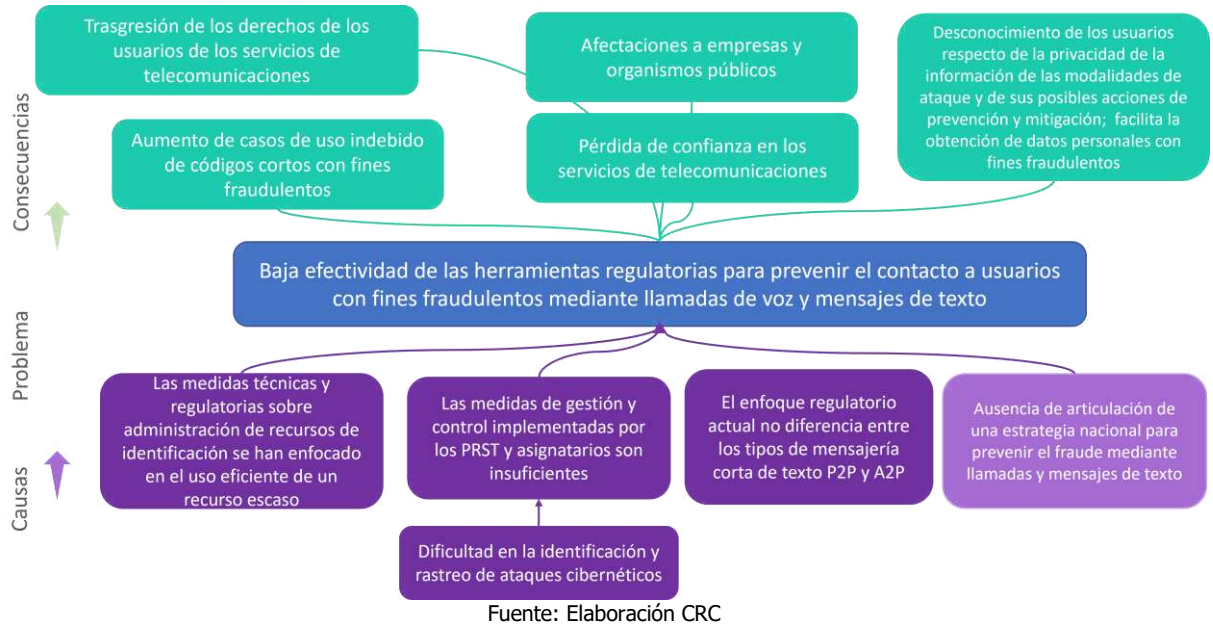
Adicionalmente, se ha reconocido que los topes y reglas de remuneración no solo inciden en el intercambio mayorista entre proveedores, sino que también se proyectan sobre la provisión del servicio

de SMS por parte de los PRSTM a los IT y PCA, lo cual refuerza el impacto de un tratamiento homogéneo sobre dinámicas donde la cadena de valor, la formación del tráfico y la capacidad de control pueden diferir entre segmentos.

Bajo estas consideraciones, y dado que la CRC identificó la necesidad de adoptar medidas preventivas de control del fraude, resulta necesario estudiar en este proyecto la remuneración e incentivos de la mensajería A2P de cara a las obligaciones específicas de control del fraude aplicables al segmento A2P. Por ello, la Comisión considera pertinente incorporar esta causa adicional en el árbol del problema, como base para sustentar la evaluación de medidas para el segmento A2P dentro del presente proyecto.

Como consecuencia de lo anterior, el árbol del problema definitivo es el que se muestra a continuación:

Ilustración 2. Árbol del problema definitivo



Fuente: Elaboración CRC

4. OBJETIVOS DEL PROYECTO

4.1. Objetivo general

Diseñar la estrategia de la CRC para la prevención y mitigación del contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4.2. Objetivos específicos

a) Evaluar la pertinencia de adoptar medidas regulatorias diferenciadas para el servicio de mensajes de texto tradicionales, a partir del análisis de las características y condiciones del mercado.
b) Identificar aspectos del régimen de recursos de identificación que sean susceptibles de adecuación desde una perspectiva de prevención del contacto a usuarios con fines fraudulentos.
c) Evaluar la implementación de herramientas regulatorias que mitiguen el contacto a usuarios con fines fraudulentos, teniendo en cuenta su viabilidad técnica y económica.
d) Determinar la necesidad de implementar acciones educativas que aumenten el conocimiento de los usuarios en la prevención contra el fraude cibernético.
e) Definir líneas de acción de la CRC y recomendaciones a otras autoridades para la construcción conjunta de una estrategia nacional de prevención en el contacto a usuarios con fines fraudulentos.

5. EXPERIENCIAS INTERNACIONALES DE FRAUDE

En el marco del presente proyecto regulatorio se efectuó una investigación minuciosa de experiencias internacionales que consistió en conocer la problemática relacionada con el fraude cibernético utilizando servicios de telecomunicaciones e identificar las medidas que implementaron con el fin de solucionarlo.

En términos generales, la experiencia internacional sugiere que las estrategias implementadas para combatir el fraude requieren de la acción y coordinación conjunta entre diferentes actores, tanto gubernamentales como no gubernamentales, así como de la ciudadanía en general. Estas estrategias buscan reducir la incidencia de los ciberdelitos en cada uno de los países revisados.

En particular los organismos que regulan el sector de las TIC, tanto de manera autónoma como en coordinación con entidades que regulan otros sectores, han adoptado medidas orientadas a combatir este flagelo mediante la expedición de normativas que contienen directrices tanto para los PRST como para los proveedores de contenidos y aplicaciones (PCA) y los integradores tecnológicos (IT).

Puntualmente, se revisaron y analizaron las experiencias de catorce países en el mundo, a saber:

1. Australia
2. Brasil
3. Canadá
4. Chile
5. España
6. Estados Unidos
7. India
8. Irlanda
9. Jordania

10. Malasia
11. Polonia
12. Portugal
13. Singapur
14. Reino Unido

A partir de este análisis se pudo concluir que las problemáticas identificadas por las autoridades regulatorias del sector TIC, y que buscaban articular soluciones por medio de la implementación de medidas normativas, se pueden agrupar en tres grandes temáticas:

i. Evitar la suplantación de la identificación del número llamante de las comunicaciones de voz cursadas por medio de las redes de telefonía fija o móvil;
ii. Combatir el envío de mensajes cortos de texto por parte de estafadores;
iii. Ejercer control de contenidos;

Si bien el abordaje de las tres temáticas en los diferentes países es dinámico y varía entre las regiones estudiadas, las estrategias implementadas para combatir la primera problemática se enfocan en validar que el número llamante no ha sido suplantado o enmascarado con otro número. Estas validaciones se realizan por medio de las siguientes tres metodologías:

1. **Verificación del CLI:** Consiste en revisar la información contenida en la funcionalidad del «Identificador de Línea Llamante» (Calling Line Identification o CLI) con el fin de bloquear llamadas que oculten el CLI, o cuyo CLI contenga números desde los cuales no se deben realizar llamadas (Do-Not-Originate list o DNO); o bloquear llamadas provenientes desde el extranjero que hacen uso de un número de origen del país de destino, con excepción de llamadas realizadas por usuarios que se encuentren en itinerancia.
2. **STIR/SHAKEN/RCD:** Radica en implementar el protocolo STIR/SHAKEN que permite verificar que el identificador de llamada transmitido coincide efectivamente con el número asignado al usuario llamante, usando técnicas de certificados digitales para verificar la identidad del proveedor de servicios que realiza la llamada. De manera articulada a la implementación de este protocolo, es usual encontrar la implementación de mecanismos de facilitación de información enriquecida a los usuarios, lo cual se conoce como RCD (Rich Call Data), a fin de incrementar su confianza en el acceso a los canales de voz tradicional.
3. **Cortafuegos (Firewall) de voz:** Consistente en implementar sistemas informáticos que permiten monitorear y establecer patrones de llamadas fraudulentas a partir de herramientas de análisis de datos en tiempo real, aprendizaje automático e inteligencia artificial, con el fin de detectar y tomar medidas sobre patrones inusuales presentes en los datos de señalización de la llamada o sobre volúmenes inusuales de tráfico.

Por su parte, para obstaculizar el envío de SMS provenientes de estafadores, las autoridades reguladoras han implementado las siguientes medidas:

1. **Limitaciones de envío de SMS:** Restringe la cantidad de SMS P2P que pueden ser enviados por un usuario dentro de un tiempo determinado.
2. **Verificación de clientes:** Define las verificaciones que se deben realizar sobre la identidad de los eslabones de la cadena de valor del SMS y los antecedentes de sus clientes.
3. **Registro de identificación y validación de remitentes de SMS:** Las organizaciones legítimamente constituidas que deseen remitir SMS publicitarios, o realizar algún tipo de notificación comercial a sus usuarios, deben registrarse y acceder tanto a los identificadores alfanuméricos que utilizarán para su envío, como a los sistemas de validación del origen y la trazabilidad de la comunicación. Esto a fin de tener una trazabilidad completa en el envío de SMS y una adecuada delegación de responsabilidades en caso de materializarse un fraude.
4. **Monitoreo de tráfico:** Despliegue e implementación de herramientas de monitoreo y análisis de tráfico que utilizan funcionalidades como escudos antispam y control de fraude para identificar y bloquear SMS sospechosos antes de su entrega a los consumidores.

Finalmente, para ejercer el control de contenidos, el regulador de Malasia implementó medidas consistentes en el trámite y la asignación de licencias a los proveedores de aplicaciones, por medio de las cuales se obligan a cumplir una serie de políticas y medidas orientadas a:

a) Controlar el acceso de contenidos a usuarios menores de edad.
b) Identificar y bloquear mensajes y contenidos maliciosos, tales como ciberacoso, estafa o captación de menores para fines sexuales.
c) Políticas y medidas para la moderación de los contenidos.
d) Medidas para gestionar *deepfakes* y contenido malicioso generado por Inteligencia Artificial (IA).

En la Tabla 1 se presentan las principales medidas adoptadas por los países estudiados con el objetivo de combatir el fraude cibernético mediante el uso de servicios de telecomunicaciones:

Tabla 1. Principales medidas adoptadas para combatir el fraude cibernético mediante servicios de telecomunicaciones

País	Medidas contra la suplantación del ID del número llamante				Medidas de contra el envío de SMS Fraudulentos				
	DNO	Bloqueo a Llamadas Internacionales con Número Local	STIR/SHAKEN	Firewall de Voz	Limitación de envío de SMS	Verificación de Clientes	Registro de ID de Remitentes	Monitores de Tráfico	Control de Contenidos
Australia	Si	Si					Si	Si	
Brasil	Si		Si	Si					
Canadá			Si						
Chile	Si								
España[3]	SI	Si					Si	Si	
Estados Unidos			Si						
India[4]							Si		
Irlanda	Si	Si		Si		Si	Si		
Jordania[5]									
Malasia									Si
Polonia	Si	Si					Si	Si	
Portugal	Si	Si							
Singapur[6]							Si	Si	
Reino Unido	Si	Si[7]			Si	Si[8]	Si[9]	Si[10]	

[3] Además de las medidas señaladas en la tabla, en España se ordena la obligación de bloquear SMS enviados del exterior con números locales y prohíbe la utilización de numeración móvil para realizar llamada con propósito comercial.

[4] Además de la medida señalada en la tabla, en la India se ordena el bloqueo de SMS enviados desde el exterior con encabezados alfanuméricos o que tengan un código de país +91.

[5] Jordania reglamentó las condiciones para el envío de SMS de forma masiva.

[6] Además de las medidas señaladas en la tabla, Singapur expidió normativas donde las instituciones financieras o los operadores de servicios móviles respondieran por las pérdidas de sus usuarios, en los casos donde se comprobara el incumplimiento de alguna de las directrices definidas para combatir el fraude.

[7] Se hace excepción a las llamadas internacionales entrantes cuyo rango de numeración comience con el código +44.

[8] Esa exigencia es realizada voluntariamente por los operadores de redes móviles, incluyendo dentro de las cláusulas de los contratos que suscriben con los agregadores de SMS las validaciones mínimas que estos deben realizar a sus clientes.

[9] Las organizaciones legítimas remitentes de contenido realizan de manera voluntaria el registro de los ID alfanuméricos utilizados para el envío de mensajes de texto SMS.

[10] Los PRST móviles han implementado de manera voluntaria herramientas de monitoreo de tráfico para identificar y bloquear SMS fraudulentos.

El anterior constituye un resumen ejecutivo del benchmark internacional realizado en el documento de formulación del problema publicado en el marco del presente proyecto regulatorio, sin embargo, la descripción y análisis completos sobre esta revisión de experiencias internacionales puede consultarse en el anexo[11] de dicho documento.

6. ASPECTOS TÉCNICOS, ECONÓMICOS Y JURÍDICOS

6.1. Caracterización técnica actual del manejo del fraude por parte de los PRSTM

Frente al requerimiento de información realizado a los operadores, se evidencia que los mecanismos técnicos, plataformas involucradas y protocolos de control difieren entre los servicios de voz y mensajería SMS, razón por la cual el análisis debe abordarse de manera separada para reflejar adecuadamente las capacidades actualmente desplegadas en cada entorno.

En el servicio de voz, los PRSTM reportan la utilización de plataformas antifraude, motores de reglas y herramientas de monitoreo de tráfico en tiempo real orientadas a la detección de comportamientos anómalos sobre los servicios de voz móvil. A nivel de arquitectura, algunos operadores indicaron que sus servicios de manejo del fraude se soportan sobre núcleos IMS y elementos de interconexión SIP, incluyendo Session Border Controllers (SBC), routers de señalización y plataformas de control de tráfico desplegadas en entornos virtualizados o de nube privada. Sin embargo, de manera transversal se identifica que actualmente no existen implementaciones activas de mecanismos de autenticación y verificación de identidad de llamadas basados en protocolos como el STIR/SHAKEN (STI-AS/STI-VS).

Los mecanismos de supervisión implementados se soportan principalmente en el monitoreo continuo de registros de detalle de llamadas (CDR) y metadatos asociados al tráfico cursado, incluyendo variables como origen y destino de llamadas, duración promedio, intentos por segundo, IMSI, IMEI, celdas utilizadas y comportamiento histórico del abonado. Sobre esta información se ejecutan procesos de correlación, análisis estadístico y validación de desviaciones frente a patrones normales de consumo, con el objetivo de detectar eventos de fraude o tráfico irregular.

Algunos proveedores señalaron controles específicos sobre clientes corporativos conectados mediante SIP Trunks y numeración DID, aplicando mecanismos de aseguramiento del número A de origen y monitoreo continuo de indicadores como CAPS (Call Attempts Per Second) y ACD (Average Call Duration), orientados a identificar alteraciones abruptas en el comportamiento esperado del tráfico.

Las respuestas también evidencian la implementación de modelos orientados a identificar escenarios específicos de fraude, tales como bypass internacional mediante SIMBOX, Wangiri, abuso de planes ilimitados, concentraciones atípicas de tráfico en determinadas celdas y consumos irregulares sobre líneas recientemente activadas. Asimismo, algunos operadores reportaron monitoreo de patrones asociados a vishing mediante la detección de ráfagas masivas de llamadas sobre ventanas de tiempo reducidas, y supervisión de tráfico proveniente de interconexiones internacionales que aparenta utilizar numeración nacional o presenta alteraciones en la estructura esperada de la identificación automática de números (ANI) -por sus siglas en ingles Automatic Number Identification- e identificación de línea llamante - CLI – (Calling Line Identification por sus siglas en inglés).

[11] Véase el documento de formulación del problema, disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf

De igual forma, se reportan análisis de comportamiento temporal y de destino, incluyendo supervisión de tráfico concentrado hacia rangos numéricos secuenciales, actividad intensiva en horarios nocturnos o festivos, y cambios abruptos hacia destinos premium o de tarificación especial. Cuando estas condiciones superan umbrales previamente definidos, las plataformas permiten ejecutar acciones automáticas de mitigación como bloqueo temporal o definitivo, restricción parcial del servicio, limitación de tráfico (throttling), inclusión en listas de monitoreo intensivo y suspensión automática de líneas.

En cuanto a SMS, los PRSTM informan que los controles de autenticidad sobre tráfico SMS A2P (de aplicaciones a personas) se realizan principalmente mediante conexiones que usan el protocolo SMPP establecidas entre Integradores Tecnológicos (IT), proveedores de contenidos y aplicaciones (PCA), operadores interconectados y las plataformas que concentran y administran el envío de los mensajes de texto en la red de los PRSTM, conocidos como SMSC. El esquema implementado corresponde a un modelo de autenticación por sesión bajo el protocolo SMPP, en el cual cada integrador o cliente dispone de credenciales únicas de acceso asociadas a una cuenta específica.

Cada conexión de un cliente SMPP es validada mediante listas blancas de remitentes autorizados, integradas por códigos numéricos o remitentes alfanuméricos previamente habilitados. Durante el procesamiento del mensaje, el SMSC valida automáticamente que el parámetro de origen corresponda a uno de los remitentes autorizados para dicha sesión del protocolo SMPP. Cuando el remitente no coincide con los valores previamente configurados y autorizados, el mensaje es rechazado automáticamente antes de ingresar al Core de mensajería, impidiendo su tránsito hacia la red móvil y el usuario final.

Desde el punto de vista operativo, la habilitación, modificación o retiro de remitentes requiere procesos internos coordinados entre áreas comerciales, mayoristas (Wholesale) y Core de red. Para ello, los IT o PCA deben presentar solicitudes formales acompañadas de la documentación soporte correspondiente a la asignación del recurso de identificación conocido como código corto. Posteriormente, las áreas técnicas realizan la parametrización manual sobre los nodos SMSC. Algunos operadores indicaron que las plataformas actualmente desplegadas no cuentan con APIs ni interfaces gráficas que permitan la administración dinámica del código corto, razón por la cual estas actividades se gestionan como cambios controlados sobre el Core, con SLA cercanos a tres días hábiles.

Las respuestas también evidencian que las plataformas SMSC actualmente utilizadas no incorporan mecanismos nativos de autenticación criptográfica, validación centralizada ni esquemas de autenticación o encriptación de la información del origen para servicios de mensajería. Asimismo, se indicó que los estándares tradicionales asociados al servicio SMS y SMPP no contemplan validaciones externas de los PCA/IT, sus plantillas de contenido, o mecanismos de autenticación extremo a extremo, por lo que cualquier implementación futura de modelos centralizados requeriría desarrollos específicos, integración de APIs externas y adecuaciones sobre plataformas SMSC y motores de routing.

Adicionalmente, algunos operadores reportaron la utilización de plataformas antifraude especializadas integradas al entorno de mensajería, las cuales permiten ejecutar monitoreo en tiempo real, captura de metadatos e inspección de tráfico SMS mediante motores de reglas, expresiones regulares y análisis de patrones semánticos. Estas herramientas permiten identificar campañas masivas, patrones

asociados a smishing, URLs sospechosas, dominios recientemente creados, dispersión anómala de destinos y comportamientos volumétricos atípicos.

No obstante, las respuestas también evidencian diferencias operativas entre operadores respecto al nivel de automatización aplicado sobre el tráfico SMS. Mientras algunos reportan capacidades de bloqueo automático basadas en análisis de comportamiento y umbrales de volumen, otros indican que determinados controles continúan ejecutándose de forma manual y reactiva para evitar falsos positivos y minimizar afectaciones sobre tráfico legítimo.

6.2. Afectaciones económicas del smishing y del vishing en Colombia en el contexto del sector financiero

Las acciones irregulares con fines de fraude se basan en una diversidad de estrategias de ingeniería social orientadas a manipular a los usuarios para obtener información sensible, credenciales de acceso, códigos de autenticación o autorizaciones de transacciones financieras. En el contexto de los servicios móviles, modalidades como el smishing y el vishing se han consolidado como algunos de los principales mecanismos utilizados por organizaciones criminales para ejecutar fraudes financieros, aprovechando la confianza de los usuarios en los canales de comunicación SMS y voz.

En el documento de formulación del problema del presente proyecto regulatorio[12] se señaló que el smishing consiste en el envío de mensajes SMS fraudulentos que simulan provenir de entidades legítimas, como bancos, comercios o entidades públicas, con el propósito de inducir a los usuarios a acceder a enlaces maliciosos, descargar aplicaciones fraudulentas o suministrar información confidencial. Por su parte, en el mismo documento se señaló que el vishing utiliza llamadas telefónicas en las cuales las personas fraudulentas suplantan la identidad de entidades reconocidas para persuadir a las víctimas de realizar transacciones, entregar claves o autorizar operaciones financieras.

De acuerdo con el documento, «*Scam Calls and Texts in Irland - Costs and benefits of interventions*» los principales perjuicios causados a los individuos por los intentos de fraude a través de los SMS y llamadas de voz son los siguientes:[13]

[12] CRC. Documento de Formulación del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles - Documento de formulación del problema». Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf

[13] Europe Economics. Scam Calls and Texts in Ireland – Costs and Benefits of Interventions (2023, United Kingdom). Disponible en: https://www.comreg.ie/media/2023/06/ComReg-2352a.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 3. Afectación del smishing y vishing

Fuente: Documento «Scam Calls and Texts in Irland - Costs and benefits of interventions»[14].

No todos los perjuicios listados en la Ilustración 3 pueden estimarse debido a que algunos datos no pueden cuantificarse, bien sea por la indisponibilidad de la información o por la incertidumbre para cuantificar los mismos. Sin embargo, a partir de la revisión realizada por esta Comisión, se logró obtener información correspondiente a las pérdidas financieras causadas por estafas generadas bajo las modalidades de smishing y vishing, los cuales fueron obtenidos a partir de las consultas realizadas por la Superintendencia Financiera de Colombia[15] a 50 establecimientos de crédito, distribuidos entre 30 bancos, 16 compañías de financiamiento y 4 cooperativas financieras.

Aunque todas las entidades respondieron al requerimiento, 15 bancos, 10 compañías de financiamiento y 2 cooperativas financieras indicaron que no podían reportar datos específicos, en razón a que no registraban eventos asociados con estas modalidades, o porque los clasifican dentro de categorías más amplias como phishing o ingeniería social, lo que impidió su desagregación.

Teniendo en cuenta lo anterior, es evidente que el impacto de estas dos modalidades de fraude tiene un efecto económico mayor al reportado por la Superintendencia Financiera de Colombia. Sin perjuicio de lo anterior, a continuación, se presentan los análisis realizados con el fin de establecer una línea base para estimar los beneficios de implementar estrategias que disminuyan el smishing y el vishing en Colombia a partir de las alternativas que serán sujetas de evaluación en la sección 9.2 del presente documento.

De acuerdo con los datos reportados, en la Tabla 2 se presenta el valor de las reclamaciones discriminadas para cada una de estas dos modalidades de fraude durante los años 2022, 2023 y 2024[16], calculadas en pesos corrientes. Como se observa, entre en el año 2022 y el año 2023 los

[14] Ibid.
[15] Superfinanciera. Número de Radicación: 2025166778-000-000. Asunto: Radicado Remisión de información sobre la afectación económica de los usuarios por fraude cibernético (smishing y vishing)
[16] Superintendencia Financiera de Colombia, Remisión de información sobre la afectación económica de los usuarios por fraude cibernético (smishing y vishing), Radicado No. 2025166778-000-000 (24 de septiembre de 2025).

valores por las reclamaciones por smishing se incrementaron por un factor de nueve, y entre el 2023 y el 2024 se incrementaron en un 55,6%. Por su parte, las perdidas por vishing aumentaron entre el 2022 y el 2023 en un 17,5% y entre 2023 y 2024 un 38,3%.

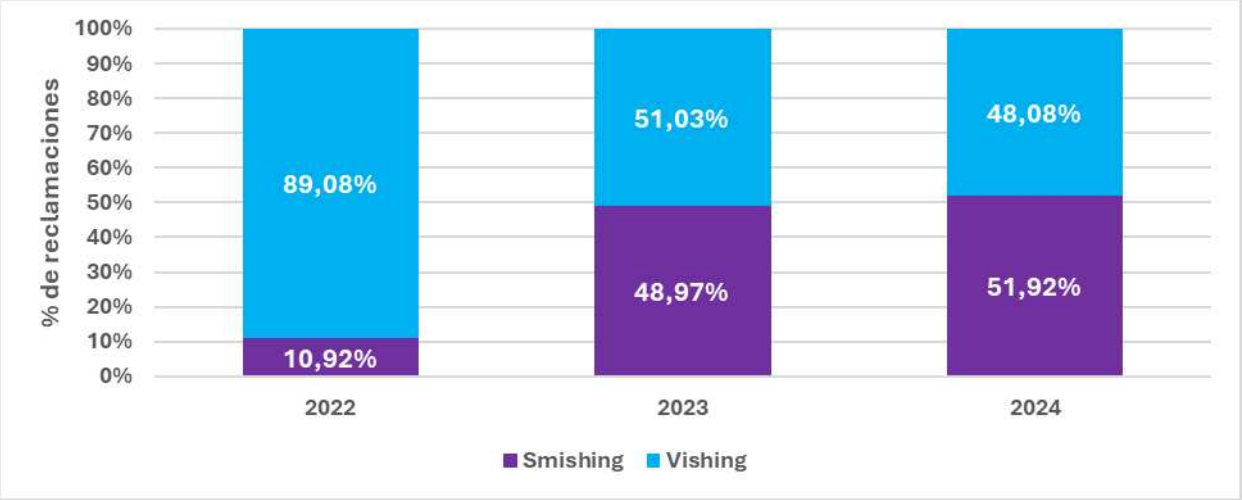
Tabla 2. Distribución de las reclamaciones de Vishing y Smishing en Colombia en millones de pesos Corrientes

	2022	2023	2024
Smishing	$ 3.343	$ 30.770	$ 47.892
Vishing	$ 27.279	$ 32.066	$ 44.342
TOTAL	**$ 30.622**	**$ 62.836**	**$ 92.235**

Fuente: Elaboración CRC a partir de la información remitida por la Superintendencia Financiera de Colombia[17]

Por su parte en la Ilustración 4 se presentan la distribución porcentual del valor de las reclamaciones discriminadas por estas dos modalidades de fraude entre los años 2022, 2023 y 2024. Se observa que mientras en el año 2022 los valores por smishing representaban un 10,92% del total de las reclamaciones, para los años 2023 y 2024 el porcentaje del valor de las reclamaciones se distribuyeron aproximadamente de forma equitativa entre las dos modalidades de fraude (smishing – vishing).

Ilustración 4. Distribución porcentual de las reclamaciones de vishing y smishing en Colombia



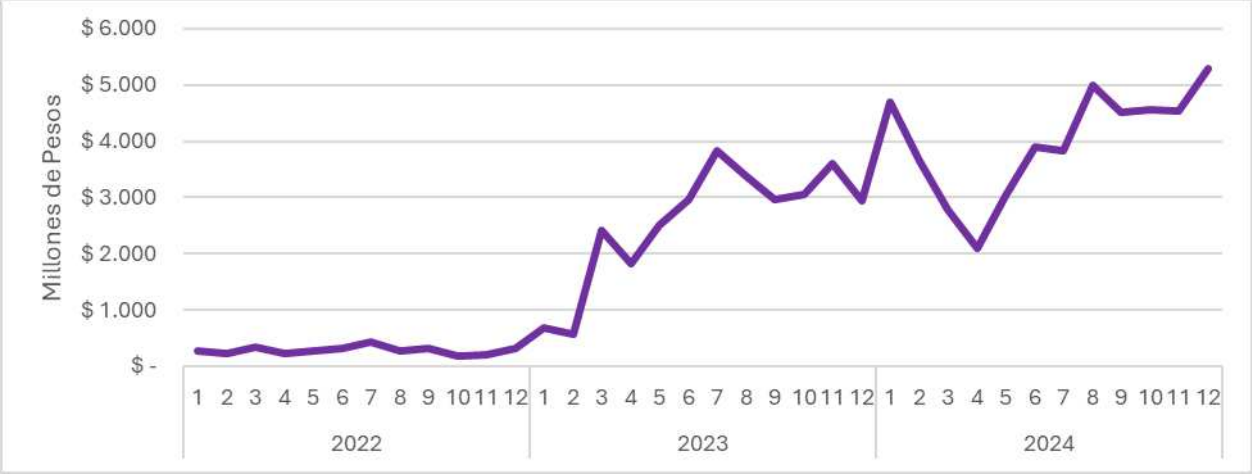
Fuente: Elaboración propia a partir de la Superintendencia Financiera de Colombia[18]

En línea con los resultados agregados previamente descritos, la Ilustración 5 y la Ilustración 6 evidencian que tanto el smishing como el vishing presentan una tendencia creciente y sostenida en el valor económico reclamado por los usuarios del sistema financiero entre 2022 y 2024. En particular, el smishing muestra un crecimiento acelerado a partir de 2023, pasando de niveles mensuales inferiores a $1.000 millones durante 2022 a valores cercanos e incluso superiores a $5.000 millones

[17] Ídem
[18] Ídem

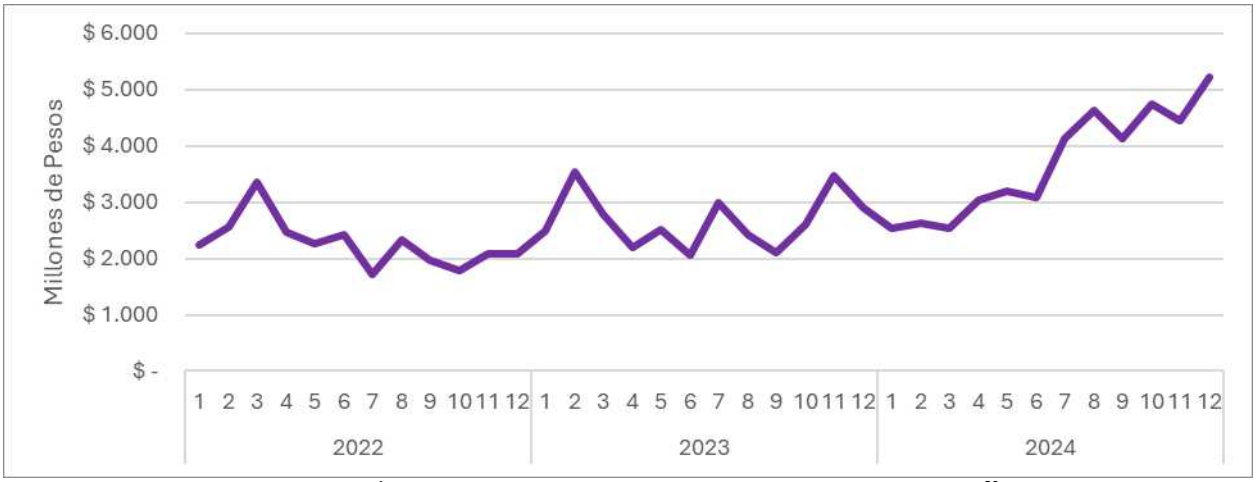
mensuales hacia finales de 2024, lo que sugiere una expansión significativa de este mecanismo de fraude y un aumento progresivo en su capacidad de afectación económica. Por su parte, aunque el vishing presenta niveles elevados desde el inicio del periodo analizado, también evidencia una trayectoria ascendente, especialmente durante 2024, año en el que las reclamaciones mensuales superan recurrentemente los $4.000 millones.

Ilustración 5. Valor reclamado en millones de pesos corrientes por smishing



Fuente: Elaboración propia a partir de la Superintendencia Financiera de Colombia[19]

Ilustración 6. Valor reclamado en millones de pesos corrientes por vishing



Fuente: Elaboración propia a partir de la Superintendencia Financiera de Colombia[20]

De manera consistente, tanto el smishing como el vishing presentan un patrón de alta persistencia temporal, sin observarse señales claras de estabilización o reducción sostenida en los montos

[19] Ídem
[20] Ídem

reclamados. Este comportamiento sugiere que los mecanismos de fraude asociados a llamadas y mensajes fraudulentos continúan adaptándose y manteniendo capacidad de afectación sobre los usuarios. En consecuencia, de no implementarse medidas orientadas a prevenir y mitigar estas prácticas, es razonable esperar que los perjuicios económicos continúen incrementándose en el tiempo, tanto por la sofisticación de las estrategias de fraude como por el aumento en el alcance y frecuencia de este tipo de ataques.

6.3. Caracterización del comportamiento del servicio de voz y SMS

En el marco del análisis y desarrollo de mecanismos para la trazabilidad del tráfico y el diseño de medidas regulatorias proporcionales y focalizadas que tengan como propósito mitigar el fraude cibernético desde la evidencia empírica, resulta pertinente tener en cuenta un enfoque basado en el análisis del comportamiento de los usuarios. En particular, el estudio de patrones de uso atípico o de distribuciones que se desvían del comportamiento esperado de los usuarios finales, puede aportar insumos relevantes para fortalecer la implementación de estos mecanismos. En este sentido, y con el propósito de profundizar en el análisis de las dinámicas actuales asociadas al uso de los servicios de voz móvil y SMS, esta Comisión realizó un requerimiento de información[21] a los PRSTM orientado a recopilar insumos técnicos y económicos que permitieran:

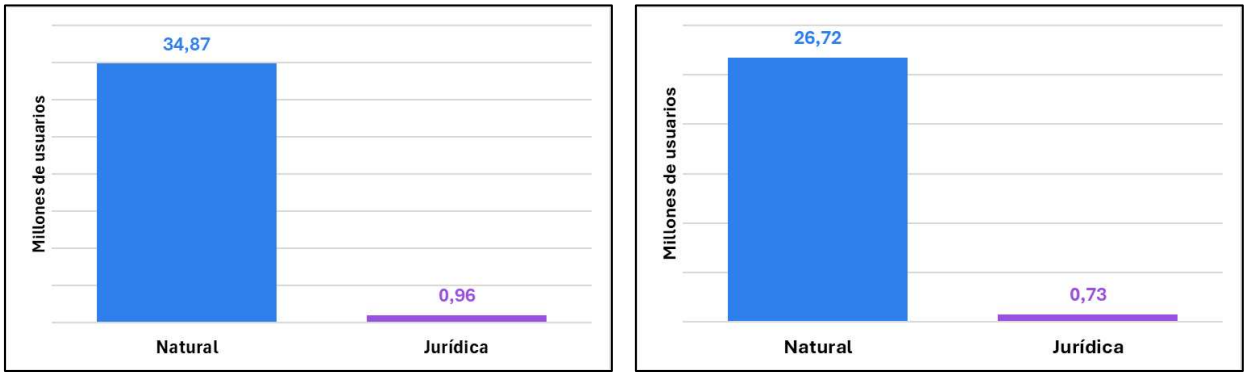
(i) caracterizar el comportamiento del tráfico de voz y SMS en condiciones normales;
(ii) identificar patrones atípicos o inusuales en el tráfico de voz y SMS;
(iii) determinar posibles prácticas irregulares asociadas a la originación de comunicaciones y
(iv) analizar la concentración del tráfico por tipo de servicio, origen y naturaleza del remitente.

Para dar respuesta a esta solicitud de información, se requirió a los PRSTM tomar como periodo de referencia el mes de diciembre de 2025, excluyendo los días 24 y 31, así como sábados, domingos y festivos, esto con el fin de evitar el sesgo que se podría generar por la estacionalidad que se deriva de estas fechas. Adicionalmente, se les solicitó considerar únicamente aquellos accesos o SIM Cards que hubieran generado tráfico efectivo en los servicios de voz o de mensajes cortos de texto (SMS) durante dicho periodo. Asimismo, se precisó que la originación de llamadas corresponde al intento de establecimiento de la comunicación, por lo que no implica necesariamente que estas hayan sido efectivamente completadas o respondidas en su destino.

Ilustración 7. Números móviles que presentaron al menos una interacción en los servicios de SMS y voz móvil durante el periodo de referencia

a) Servicio de voz móvil **b) Servicio de SMS**

[21] CRC. Requerimiento de información No. 2026-002. Información relacionada con fraude cibernético por medio de servicios de telecomunicaciones móviles.



Fuente: CRC. Elaboración propia con base en la información remitida por los PRSTM.

De igual manera, para desarrollar análisis de patrones de uso, se segmentó la información entre dos tipos de usuarios: personas naturales y personas jurídicas, considerando que cada tipo de usuarios puede presentar motivaciones de uso, intensidades de tráfico y estructuras de consumo sustancialmente distintas. De acuerdo con los resultados del requerimiento, los cuales se presentan de manera agregada, se evidencia una alta concentración del número de líneas con interacción asignadas a personas naturales, tanto en el servicio de voz como en SMS.

En particular, para el servicio de voz móvil, aproximadamente 34,87 millones de números asociados a personas naturales registran interacción, frente a cerca de 0,96 millones correspondientes a personas jurídicas, lo que implica que más del 97% de las líneas activas en este servicio pertenecen a usuarios naturales (ver panel a) de la Ilustración 7). De manera consistente, en el panel b) de la Ilustración 7 se observa una distribución similar para el servicio de SMS, con alrededor de 26,72 millones de números de personas naturales frente a 0,73 millones de personas jurídicas, confirmando la predominancia de este segmento en términos de volumen de usuarios.

Tabla 3. Estadísticas descriptivas del comportamiento del servicio de voz móvil por tipo de usuario.

Indicador	Cantidad de llamadas		Duraciones llamadas (Min)	
	Natural	Jurídica	Natural	Jurídica
Total	1.582.287.044	247.830.361	3.821.265.213	724.409.395
Promedio	44,1	42,9	6.478,5	6.527,5
Desv. Est.	74,1	291,2	1.672,6	1.857,8
Min	1,0	1,0	0,0	0,0
Max	200.827	386.230	27.391	51.003
Mediana	26,2	17,0	65,9	13,8
P25 aprox.	8,0	6,0	2,8	1,9
P75 aprox.	62,0	53,0	287,7	79,1

Fuente: CRC. Elaboración propia.

Por su parte, el análisis de las estadísticas descriptivas agregadas del sector descritas en la Tabla 3 permite caracterizar el comportamiento de las llamadas originadas, ya sea desde el punto de vista de

su cantidad o de su duración, diferenciando entre personas naturales y jurídicas, evidenciando tanto similitudes estructurales como diferencias relevantes en la distribución del tráfico.

En primer lugar, en términos de volumen, se observa que las personas naturales concentran la mayor cantidad de llamadas originadas, así como duración de las mismas, en contraste con el segmento de personas jurídicas. Este resultado es consistente con la predominancia de usuarios finales en el mercado móvil, previamente identificada, y confirma que el comportamiento agregado del sector está fuertemente influenciado por dicho segmento.

No obstante, las diferencias de medias del número de llamadas y la duración entre personas naturales y jurídicas son marginales y no resultan significativas en términos estadísticos[22], en la medida en que son considerablemente pequeñas frente a la alta dispersión observada en ambos segmentos. En particular, la diferencia en el número promedio de llamadas es de apenas 1,2 llamadas, mientras que en duración es de 49 minutos, valores que representan una fracción mínima en relación con sus desviaciones estándar.

No obstante, este resultado no implica homogeneidad en el comportamiento entre segmentos. Por el contrario, las diferencias más relevantes se evidencian en la forma de las distribuciones, donde el segmento de personas jurídicas presenta mayor dispersión, valores extremos más altos y una mediana significativamente inferior, lo que sugiere la presencia de comportamientos más heterogéneos y concentraciones atípicas de tráfico. Es pertinente señalar que esta diferencia entre promedio y mediana en ambos segmentos revela la presencia de asimetrías en la distribución del tráfico (sesgo positivo), lo que quiere decir que existe un subconjunto reducido de líneas que concentra una proporción significativa tanto del número de llamadas como de la duración total del tráfico.

Los percentiles refuerzan este análisis. Una aproximación desde el cálculo del rango intercuartílico, permite reducir la influencia de los valores extremos y ver en donde se concentra el comportamiento del 50% de las líneas móviles. En el caso de la cantidad de llamadas, las personas naturales se concentran entre 8 y 62 llamadas (P25 y P75), mientras que en personas jurídicas este rango esta entre 6 y 53 llamadas. Por su parte, la duración de las llamadas muestra que el 50% de las personas naturales se ubica entre 3 y 288 minutos aproximadamente, en contraste las personas jurídicas se localizan en el rango comprendido entre 2 y 79 minutos.

Así las cosas, en el caso del número de llamadas, ambos segmentos presentan niveles de dispersión relativamente similares en el rango central de la distribución, mientras que en la duración de las llamadas se evidencian patrones diferenciados en donde las personas naturales presentan una mayor variabilidad en el uso típico del servicio, y las personas jurídicas muestran una distribución más concentrada en valores bajos, acompañadas a su vez de valores máximos superiores.

Es importante resaltar que en el caso de las personas jurídicas se observa una combinación de una mediana de duración inferior en contraste a las personas naturales, es decir llamadas cortas, con la presencia de valores extremos elevados tanto en número como en duración, lo cual sugiere la coexistencia de dos tipos de comportamiento: (i) un gran volumen de llamadas breves, y (ii) un subconjunto reducido de líneas con uso intensivo. Este patrón de comportamiento es relevante ya que sugiere la presencia de comunicaciones automatizadas o masivas (alto número de llamadas, corta

[22] Para confirmar este resultado se aplicó la prueba estadística de diferencia de medias, a partir de la cual aceptó la hipótesis nula. Estos resultados pueden ser replicados tomando los valores presentados en la Tabla 3.

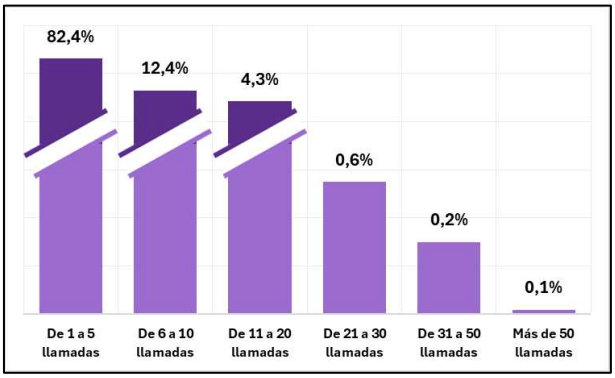
duración), plataformas de contacto o sistemas de marcación automática, y potencialmente, esquemas de generación artificial de tráfico o prácticas irregulares de originación.

Estos resultados son confirmados al analizar los rangos de distribución de la cantidad de llamadas por líneas móviles asignadas a personas naturales y jurídicas, los cuales se muestran en la Ilustración 8. En el panel a) de esta Ilustración, se puede observar que el 82,4% de las líneas móviles asignadas a personas naturales se concentra en un rango comprendido entre 1 y 5 llamadas, seguido de rangos de 6 a 10 llamadas (12,4%) y 11 a 20 llamadas (4,3%), mientras que proporciones marginales de líneas superan las 20 llamadas. Este comportamiento indica una alta concentración en los rangos más bajos de interacción y una disminución progresiva a medida que aumenta el número de llamadas, lo que refleja una distribución sesgada con cola hacia la derecha.

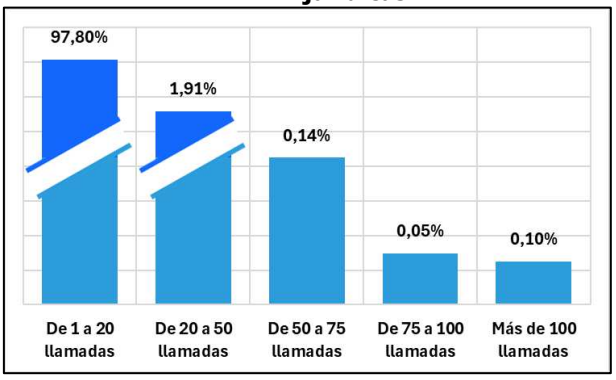
Por su parte, en el panel b) se muestra la distribución por rangos de interacción de las líneas asignadas a personas jurídicas. Se encuentra que la concentración en rangos bajos es aún más pronunciada, con aproximadamente 97,8% de las líneas en el rango entre 1 y 20 llamadas. No obstante, se identifican proporciones, aunque reducidas, de líneas en rangos superiores (más de 50 llamadas), lo que confirma la existencia de un subconjunto de líneas con niveles de uso significativamente más intensivos.

Ilustración 8. Rangos de distribución de la cantidad de llamadas por tipo de personas

a) Distribución de llamadas personas naturales



b) Distribución de llamadas personas jurídicas



Fuente: CRC. Elaboración propia.

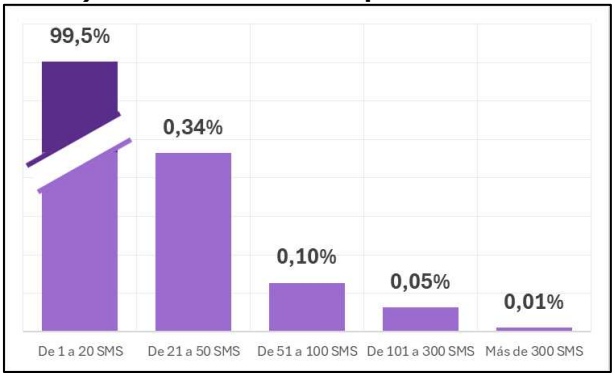
En conjunto, estas distribuciones refuerzan la evidencia previamente identificada respecto a la asimetría en el uso del servicio y la presencia de colas largas en la distribución, particularmente en el segmento de personas jurídicas. En efecto, mientras la mayor parte de las líneas se concentra en niveles bajos de tráfico, existe una fracción reducida que concentra un volumen desproporcionado de llamadas, lo cual es consistente con los valores extremos observados en la Tabla 3, donde se muestran las estadísticas descriptivas. Este patrón de comportamiento resulta relevante en la medida en que permite identificar estructuras de uso no homogéneas y potencialmente asociadas a comportamientos atípicos.

En cuando al servicio de mensajería móvil, el análisis de los rangos de distribución de la cantidad de SMS enviados por líneas móviles que se muestra en la Ilustración 9, confirma y profundiza los patrones de concentración previamente identificados en el servicio de voz. En particular, se observa una alta concentración de líneas en rangos bajos de envío de mensajes, tanto para personas naturales como

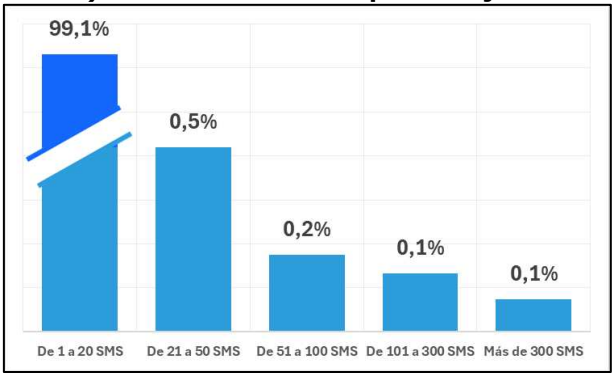
jurídicas, lo que evidencia que el uso de SMS es, en términos generales, de baja intensidad para la gran mayoría de los usuarios. Sin embargo, también se identifican proporciones pequeñas, pero no despreciables, en rangos de mayor volumen, lo que sugiere la presencia de líneas con usos más intensivos.

Ilustración 9. Rangos de distribución de la cantidad de SMS por tipo de personas

a) Distribución de SMS personas naturales



b) Distribución de SMS personas jurídicas



Fuente: CRC. Elaboración propia.

Las distribuciones del servicio de SMS evidencian un patrón aún más marcado que en el servicio de voz; una concentración extrema del tráfico en niveles bajos de uso, acompañada de una cola larga muy reducida pero relevante en términos del diseño de mecanismos de trazabilidad y monitoreo del tráfico, particularmente en el segmento de personas jurídicas. En particular, el análisis de este subconjunto de líneas con volúmenes relativamente altos de envío de SMS resulta especialmente importante, en la medida en que puede estar asociado a servicios de mensajería masiva, plataformas automatizadas o posibles esquemas de uso irregular de este servicio.

El requerimiento de información realizado por CRC también abordó el análisis de las llamadas de voz con una duración inferior a 10 segundos, considerando que este tipo de comunicaciones puede estar asociado a patrones de uso no convencionales, tales como esquemas de originación automatizada o prácticas conocidas como robocalls. En este sentido, se solicitó a los PRSTM reportar, para el periodo de referencia, la cantidad de números móviles y el total de llamadas originadas cuya duración promedio por llamada se ubicara en rangos específicos por debajo de dicho umbral, discriminando la información por tipo de persona, natural o jurídica.

Es importante tener en cuenta que los rangos de duración presentados en la Tabla 4 no son mutuamente excluyentes en términos de líneas, en la medida en que una misma línea puede registrar llamadas en múltiples rangos de duración durante el periodo de análisis; por tanto, la suma de las líneas por rango puede exceder el total de líneas únicas con interacción.

Tabla 4. Análisis de llamadas de voz con una duración inferior a 10 segundos

PRSTM	Rango de duración de la llamada en segundos	Cantidad de líneas móviles por tipo de persona		Cantidad de llamadas por tipo de persona	
		Naturales	Jurídicas	Naturales	Jurídicas

TOTAL	Menos de 2 segundos	10.049.537	2.063.635	77.914.816	5.690.772
TOTAL	Más de 2 – Igual o menos de 4 segundos	9.830.940	2.886.999	27.102.456	8.534.657
TOTAL	Más de 4 – igual o menos de 6 segundos	8.049.209	2.251.923	16.453.021	4.895.506
TOTAL	Más de 6 – Igual o menos de 8 segundos	7.519.518	1.913.942	15.335.240	4.312.786
TOTAL	Más de 8 – igual o menos de 10 segundos	7.747.327	1.845.703	17.120.997	4.588.384

Fuente: CRC. Elaboración propia con base en la información reportada.

En primer lugar, se observa que una proporción significativa de líneas móviles en ambos segmentos registra llamadas en todos los rangos de corta duración analizados. En el caso de las personas naturales, el mayor número de líneas se concentra en los rangos de menor duración, particularmente en llamadas de menos de 2 segundos (10,0 millones de líneas) y entre 2 y 4 segundos (9,8 millones), lo cual es consistente con comportamientos asociados a intentos de llamada no completados o interacciones de muy corta duración. Este patrón decreciente se mantiene en los rangos superiores, aunque con una ligera estabilización en el intervalo de 8 a 10 segundos (7,7 millones de líneas).

Por su parte, en el segmento de personas jurídicas, aunque el número absoluto de líneas es significativamente menor, se observa un patrón similar en términos de distribución por rangos, con mayor concentración en los intervalos de menor duración, destacándose el rango de 2 a 4 segundos (2,9 millones de líneas) como el de mayor participación. No obstante, al igual que en el análisis previo, este segmento presenta un comportamiento decreciente a medida que aumentan los rangos de duración.

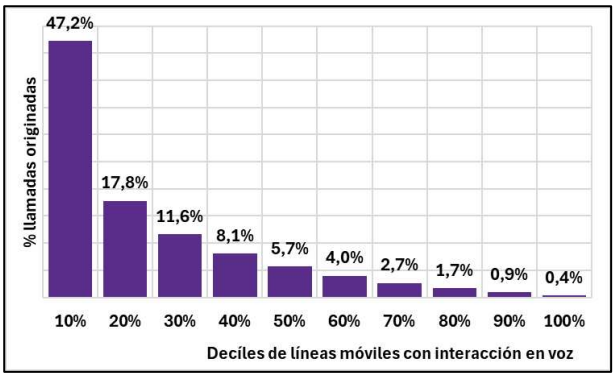
En términos de volumen de llamadas, los resultados refuerzan estos hallazgos. Para las personas naturales, el mayor número de llamadas se concentra en el rango de menos de 2 segundos (77,9 millones de llamadas), seguido por el rango de 2 a 4 segundos (27,1 millones), evidenciando una fuerte concentración en llamadas extremadamente cortas. Este comportamiento es consistente con la existencia de intentos de comunicación fallidos o interacciones breves propias del uso cotidiano. Al observar el comportamiento en personas jurídicas se registra un volumen considerable de llamadas en todos los rangos, destacándose especialmente los intervalos de 2 a 4 segundos (8,5 millones de llamadas) y menos de 2 segundos (5,7 millones). Este patrón, en conjunto con la evidencia previa de mayor intensidad por línea, confirma la existencia de una mayor concentración del tráfico de corta duración en este segmento.

De manera consistente, al analizar el grado de concentración del tráfico de llamadas originadas a partir de la distribución acumulada por deciles de líneas móviles, ordenadas de mayor a menor según su volumen de llamadas, se encuentra que un subconjunto reducido de líneas cuenta con una proporción significativa del tráfico total. El panel a) de la Ilustración 10 muestra que, en el caso de las personas naturales, el 10% de las líneas con mayor número de llamadas concentra aproximadamente el 47,2% del tráfico total, lo que evidencia un nivel importante de concentración. A medida que se amplía el porcentaje de líneas consideradas, la participación acumulada del tráfico crece de manera decreciente, alcanzando cerca del 75% del tráfico en el 30% de las líneas y aproximadamente el 90% en el 60% de las líneas.

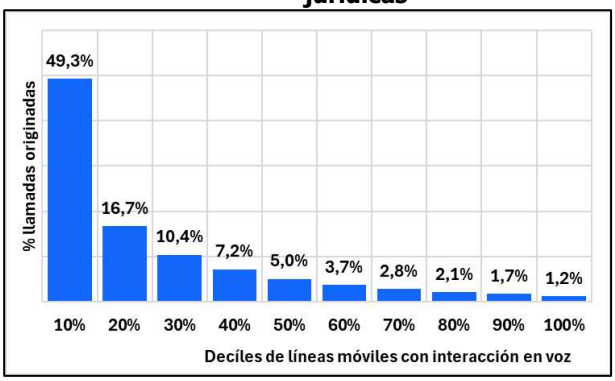
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 10. Concentración de llamadas originadas por deciles de líneas móviles

a) Distribución de llamadas personas naturales



b) Distribución de llamadas personas jurídicas

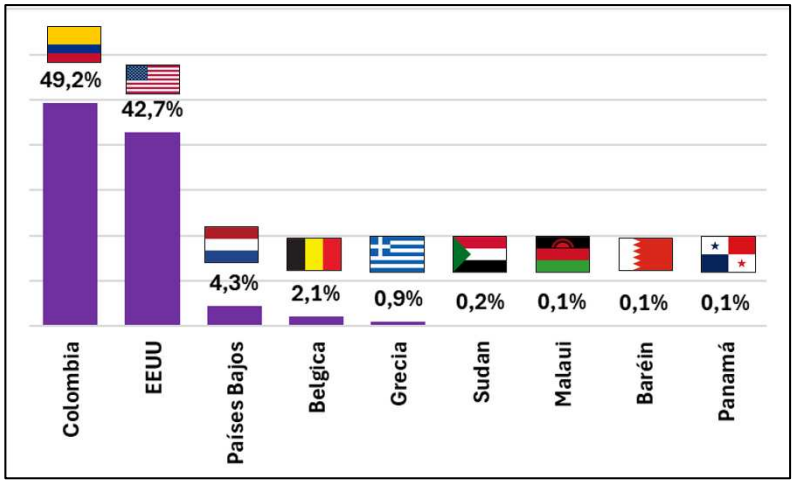


Fuente: CRC. Elaboración propia.

Por su parte, el panel b) muestra que, en el segmento de personas jurídicas, el nivel de concentración es ligeramente más pronunciado. En este caso, el 10% de las líneas concentra el 49,3% del tráfico total, superando ligeramente lo observado en personas naturales. Asimismo, a medida que se aumenta el porcentaje de distribución se encuentra que el 76,34% de las llamadas es originada por apenas un 30% de las líneas móviles asignadas a este segmento.

En conjunto, ambas distribuciones evidencian una alta concentración del tráfico, tipo Pareto, donde una proporción relativamente pequeña de líneas genera una fracción significativa del total de llamadas, lo cual resulta consistente con los hallazgos previos sobre mayor dispersión, presencia de valores extremos e intensidad por línea en este segmento. En particular, el hecho de que cerca de la mitad del tráfico se concentre en apenas el 10% de las líneas resalta la necesidad de atender potenciales focos de monitoreo prioritario, en la medida en que estos subconjuntos pueden estar asociados a usos irregulares del servicio.

Ilustración 11. Distribución por país de origen de llamadas con CLI potencialmente enmascarados



Fuente: CRC. Elaboración propia con base en la información reportada.

Por último, el análisis de la información reportada por los PRSTM frente a la identificación del país de origen de las llamadas con CLI[23] enmascarado evidencia limitaciones estructurales en la trazabilidad del tráfico internacional. En primer lugar, desde una perspectiva metodológica, los PRSTM coinciden en señalar que no es técnicamente posible determinar de manera directa y concluyente el país de origen real de este tipo de tráfico, debido a que las llamadas son cursadas a través de intermediarios, carriers internacionales y plataformas de tránsito. En este contexto, la información disponible se basa principalmente en puntos de entrega del tráfico, carriers o IPs de interconexión, o en criterios de señalización, lo que implica que la atribución geográfica debe interpretarse como una aproximación operativa y no como una identificación definitiva del origen.

A pesar de estas limitaciones, la información aportada permite identificar ciertos patrones relevantes a nivel sectorial. En particular, se observa que el tráfico con CLI enmascarado presenta una alta concentración en un conjunto reducido de orígenes reportados, destacándose de manera significativa aquellos asociados a Colombia y Estados Unidos, los cuales, en conjunto, representan la mayor proporción del total de llamadas detectadas con esta característica. Adicionalmente, se identifican otros países con participaciones mucho menores, como algunos ubicados en Europa y América Latina, lo que sugiere la existencia de múltiples rutas internacionales de entrada del tráfico.

Un hallazgo relevante es la presencia significativa de tráfico clasificado como de origen nacional que presenta indicios de enmascaramiento de CLI. Este resultado es consistente con lo señalado por los operadores, en el sentido de que parte del tráfico internacional puede ser reoriginado o presentado como tráfico nacional, ya sea por mecanismos de tránsito o por prácticas asociadas a la manipulación de la señalización. En consecuencia, la identificación de Colombia como país de origen no necesariamente implica que las llamadas se generen efectivamente dentro del territorio nacional, sino que puede reflejar procesos de enrutamiento o alteración del identificador de origen.

[23] CLI por sus siglas del inglés Calling Line Identification, traducido como Identificación de la Línea Llamante.

Los resultados expuestos a lo largo de esta sección permiten concluir que el comportamiento del tráfico de voz y SMS presenta patrones de uso heterogéneos, con una marcada concentración del tráfico en subconjuntos reducidos de líneas, especialmente en el segmento de personas jurídicas. En particular, la evidencia agregada muestra la coexistencia de varios elementos relevantes para el análisis regulatorio: una alta asimetría en la distribución del número y duración de las llamadas, la presencia de valores extremos, una concentración significativa del tráfico en los deciles superiores y un volumen importante de comunicaciones de muy corta duración. Considerados de manera conjunta, estos hallazgos sugieren la existencia de estructuras de uso no homogéneas que, en determinados casos, podrían ser consistentes con esquemas de originación automatizada, sistemas de marcación masiva, plataformas de contacto o prácticas irregulares de generación de tráfico.

No obstante, si bien el análisis agregado permite identificar señales relevantes y construir una caracterización sectorial sólida, resulta necesario profundizar en la individualización de perfiles que presenten un comportamiento irregular con fines de fraude. En particular, se requiere analizar de manera conjunta la frecuencia de llamadas y la distribución de su duración por línea móvil, con el fin de identificar patrones sistemáticos que no son observables en el análisis agregado. Bajo este enfoque adquieren especial relevancia las características identificadas en este análisis, entre estas:

(i) Alto número de llamadas de corta duración,
(ii) Baja duración promedio por llamada,
(iii) Alta concentración de llamadas en rangos inferiores a pocos segundos, y
(iv) Persistencia temporal de estos patrones durante el periodo de análisis.

Estas condiciones, cuando se presentan de manera simultánea, constituyen señales consistentes con esquemas de marcación automatizada o comportamientos irregulares en el uso de los servicios móviles objeto de estudio. En consecuencia, la profundización del análisis bajo este enfoque constituye un paso necesario para el diseño de mecanismos de trazabilidad más precisos y focalizados en el desarrollo de acciones de monitoreo, supervisión y eventual intervención en aquellos casos en donde se identifiquen patrones consistentes con prácticas de uso no convencional o potencialmente asociadas a fraude en el servicio de voz móvil.

- **Mecanismos de monitoreo y control sobre tráfico SMS P2P y A2P**

A partir de las respuestas remitidas por los PRSTM frente a las preguntas del requerimiento de información[24] asociadas al servicio de mensajería, se observa que, a nivel sectorial, existe una aproximación convergente hacia la detección y mitigación de prácticas irregulares en el tráfico de SMS, tanto en la modalidad P2P como en A2P. En términos generales, los operadores reportan la implementación de herramientas automatizadas de monitoreo, soportadas en reglas de negocio, umbrales de tráfico y generación de alarmas, orientadas a identificar comportamientos atípicos en el envío de mensajes. Este hallazgo sugiere que el sector cuenta con una base operativa de control preventivo y reactivo, centrada principalmente en el análisis de variables como el volumen de SMS, la dispersión temporal de los envíos, la recurrencia de patrones de tráfico y otras señales objetivas de riesgo.

[24] CRC. Requerimiento de información No. 2026-002. Información relacionada con fraude cibernético por medio de servicios de telecomunicaciones móviles.

De manera complementaria, las respuestas evidencian que estos mecanismos no se limitan al monitoreo puramente cuantitativo del tráfico, sino que en algunos casos incorporan controles adicionales sobre atributos del mensaje, tales como la longitud, la presencia de palabras clave sospechosas, la estructura del texto o la inclusión de enlaces y dominios potencialmente riesgosos. Desde una perspectiva sectorial, esto permite concluir que la detección de irregularidades en SMS combina dos enfoques: por una parte, el análisis del comportamiento del tráfico y, por otra, la identificación de elementos asociados a posibles campañas de smishing. Asimismo, se advierte la existencia de canales de denuncia y retroalimentación provenientes de usuarios, áreas internas de fraude y reportes interoperatorios, lo que refuerza el carácter reactivo y adaptativo de los controles implementados.

En relación con la dimensión temporal del fenómeno, la información reportada no permite identificar un patrón sectorial único sobre los días u horarios de mayor ocurrencia del tráfico atípico de SMS P2P. No obstante, sí se advierte que algunos operadores han identificado ventanas temporales de mayor riesgo, particularmente en horarios nocturnos y de madrugada, en franjas de baja actividad laboral, en fines de semana y en fechas cercanas a pagos de nómina o primas. En contraste, otros reportan no haber encontrado concentraciones temporales atípicas claramente diferenciables. En consecuencia, desde una lectura agregada, puede concluirse que la variable temporal constituye un factor contextual relevante, aunque no necesariamente determinante por sí solo, por lo que su utilidad parece estar más asociada al ajuste dinámico de reglas de monitoreo que a la definición de un patrón sectorial uniforme.

Respecto de los controles aplicados para prevenir el envío de SMS A2P con contenido fraudulento o con fines de suplantación, las respuestas sectoriales muestran una estrategia basada en la combinación de filtros automáticos, monitoreo continuo, gestión de alertas y escalamiento operativo hacia IT, PCA o agentes responsables del tráfico. En este ámbito, los operadores señalan que las denuncias se enfocan en señalar textos y URLs sospechosas o de dominios que presentan indicios de irregularidad.

Ahora bien, aunque las respuestas permiten identificar un conjunto relativamente amplio de prácticas de monitoreo y control, también ponen en evidencia que los mecanismos existentes se encuentran principalmente sustentados en reglas predefinidas, casuísticas históricas y análisis de eventos conocidos, lo cual podría limitar la capacidad de anticipación frente a nuevas modalidades de fraude o a esquemas más sofisticados de evasión. Adicionalmente, las diferencias observadas en la profundidad de los controles reportados sugieren que, a nivel sectorial, no necesariamente existe un estándar homogéneo respecto a las variables monitoreadas, la granularidad del análisis o el nivel de automatización de las respuestas.

En ese contexto, el análisis de las respuestas permite concluir que el sector cuenta con una infraestructura básica de prevención y control del tráfico irregular de SMS, por lo que aún existe espacio para fortalecer la estandarización de criterios, la interoperabilidad de alertas, el intercambio de información relevante y la definición de señales comunes de riesgo.

- **Patrones de tráfico y mecanismos de detección de uso irregular en el servicio de voz**

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En cuanto al servicio de voz móvil, a partir de la información reportada por los PRSTM[25], es posible identificar un conjunto consistente de patrones, métodos y criterios utilizados para la detección de tráfico atípico en este servicio, los cuales permiten construir una caracterización robusta del fenómeno desde una perspectiva de monitoreo y gestión del riesgo.

En primer lugar, los PRSTM en sus respuestas muestran una alta convergencia en torno a señales asociadas a desviaciones frente al comportamiento esperado del usuario, los cuales son acordes al análisis del comportamiento del servicio presentado anteriormente en esta sección del documento. Entre los principales patrones identificados a nivel agregado se encuentran:

(i) incrementos súbitos en el volumen de llamadas;
(ii) alta frecuencia de llamadas desde un mismo origen en periodos cortos de tiempo;
(iii) generación de tráfico hacia múltiples destinos de manera secuencial o simultánea;
(iv) concentración del tráfico hacia destinos específicos o de alto costo; y
(v) presencia de llamadas de corta duración en combinación con altos volúmenes.

Estos elementos, analizados de forma conjunta, reflejan estructuras de tráfico altamente intensivas y no lineales, que difieren del uso típico del servicio por parte de usuarios finales. Adicionalmente, los operadores reconocen la relevancia de variables técnicas complementarias, tales como la dispersión geográfica del tráfico, celdas o estaciones base, el uso simultáneo de múltiples dispositivos (IMEI), la generación de tráfico desde ubicaciones atípicas o de riesgo, y la incoherencia entre el perfil histórico del usuario y su comportamiento actual. En conjunto, estas variables permiten identificar configuraciones de tráfico potencialmente asociadas a esquemas como bypass, reoriginación, wangiri o suplantación de CLI.

En segundo lugar, respecto a los métodos y criterios de detección, las respuestas evidencian que el sector utiliza predominantemente esquemas de monitoreo automatizado basados en reglas, umbrales y análisis de desviaciones respecto a patrones históricos. Estos mecanismos incluyen el monitoreo en tiempo real del tráfico, el análisis de registros de detalle de llamadas (CDR), la aplicación de umbrales dinámicos de consumo, tanto en número de llamadas como en duración, y la detección de concentraciones anómalas por origen, destino o temporalidad. De manera complementaria, se identifican enfoques más avanzados que incorporan técnicas de analítica de datos, incluyendo modelos de aprendizaje automático orientados a identificar patrones complejos de tráfico.

En tercer lugar, en relación con la dimensión temporal del tráfico atípico, si bien no se identifica un patrón único a nivel sectorial, sí emergen ciertas regularidades. En particular, se observa que el tráfico irregular tiende a concentrarse en horarios nocturnos y de madrugada, así como en ventanas de baja actividad comercial, donde el tráfico legítimo disminuye y los comportamientos atípicos resultan más evidentes. Adicionalmente, se señalan eventos asociados a fechas específicas, tales como periodos de pago (como quincenas), temporadas comerciales o festivas, y ciertos días de la semana, lo cual sugiere que el fraude puede adaptarse a dinámicas contextuales del comportamiento de los usuarios.

No obstante, también se evidencia que, en algunos casos, el tráfico atípico no presenta una concentración temporal claramente definida, lo que indica que estos patrones pueden ser altamente dinámicos y adaptativos, variando en función del tipo de fraude, las rutas de tráfico y las estrategias utilizadas para evadir los controles existentes. En consecuencia, la variable temporal debe entenderse

[25] Ibidem.

como un factor complementario dentro de los modelos de detección, más que como un criterio determinante de forma aislada.

En general, se evidencia que los PRSTM cuentan con una base operativa sólida en términos de monitoreo y detección, sustentada principalmente en reglas y umbrales, con avances hacia enfoques más analíticos. Sin embargo, también se identifican oportunidades de fortalecimiento en términos de estandarización de criterios, integración de señales de riesgo y evolución hacia modelos más predictivos y coordinados a nivel sectorial, de tal manera que permitan identificar de manera más precisa comportamientos atípicos y orientar acciones focalizadas para la mitigación del fraude en el servicio de voz móvil.

7. APLICACIÓN DEL ARTÍCULO 31 DE LA LEY 1978 DE 2019

De acuerdo con la orientación de la política pública sectorial frente a la promoción del despliegue de infraestructura de redes de telecomunicaciones demarcada desde la Ley 1341 de 2009, la Ley 1978 de 2019 hizo énfasis especial en el objetivo de cierre efectivo de la brecha digital, así como en la promoción prioritaria y eficiente del acceso a las TIC para la población más vulnerable, en zonas rurales y apartadas del país.

Bajo este contexto, en el artículo 31 de la Ley 1978 de 2019, modificado por el artículo 141 de la Ley 2294 de 2023[26], el legislador introdujo el deber, en cabeza del Ministerio de TIC y la CRC, de evaluar en cualquier proyecto normativo, la pertinencia de establecer medidas o reglas diferenciales respecto de aquellos PRST que tengan menos de treinta mil (30.000) accesos, con el propósito de generar condiciones de prestación de los servicios que permitan la inclusión de actores locales, municipales y regionales, así como de establecer este tipo de medidas respecto de aquellos proveedores que extiendan sus redes o servicios a zonas no cubiertas y los que prestan sus servicios con total cobertura en los proyectos normativos que incentiven el despliegue de infraestructura y la provisión de servicios en zonas rurales o urbanas de difícil acceso, o en municipios focalizados por las políticas públicas[27]. El texto del artículo referenciado es del siguiente tenor:

> **«ARTÍCULO 31. ESTABLECIMIENTO DE CARGAS U OBLIGACIONES DIFERENCIALES.** El Ministerio de Tecnologías de la Información y las Comunicaciones y la Comisión de Regulación de Comunicaciones deberán siempre evaluar la pertinencia de establecer medidas o reglas diferenciales para los proveedores de redes y servicios de telecomunicaciones que tengan menos de treinta mil (30.000) accesos, en el desarrollo de cualquier tipo de proyecto normativo bajo el ámbito de sus competencias legales con el propósito de promover el servicio y acceso universal.
>
> Así mismo, deberán evaluar la pertinencia de establecer medidas o reglas diferenciales para los proveedores que extiendan sus redes o servicios a zonas no cubiertas, o para los que prestan sus servicios con total cobertura, en los proyectos normativos que incentiven el despliegue de infraestructura y la provisión de servicios en zonas rurales o inclusive en zonas urbanas de difícil acceso, o en aquellos municipios focalizados por las políticas públicas. De la evaluación adelantada se dejará constancia en los documentos soporte de la publicación de la medida normativa que se pretenda adoptar».

[26] «Por el cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida"».
[27] De conformidad con lo previsto en el artículo 31 de la Ley 1978 de 2019, este ejercicio de evaluación tiene que producirse en todo tipo de proyecto normativo que se desarrolle en ejercicio de las competencias regulatorias de la CRC y que deba ser publicado con sujeción a las reglas de publicidad previstas en el artículo 2.2.13.3.1. y siguientes del Decreto 1078 de 2015, y formalmente debe quedar constancia de dicho análisis en el documento soporte del proyecto regulatorio correspondiente objeto de dicha publicación.

En cumplimiento del artículo 31 de la Ley 1978 de 2019, modificado por el artículo 141 de la Ley 2294 de 2023, la CRC evaluó la pertinencia de establecer medidas o reglas diferenciales para los proveedores de redes y servicios de telecomunicaciones con menos de treinta mil (30.000) accesos en el marco del presente proyecto regulatorio.

Las obligaciones adoptadas en materia de prevención del fraude mediante el presente proyecto regulatorio recaen principalmente sobre los PRST que participan en el ecosistema de terminación de SMS y tráfico de voz móvil, y sobre los IT y PCA que operan en el mercado de mensajería A2P. En relación con los PRST, la CRC constató que los operadores activos en el mercado de terminación de SMS y en el ecosistema A2P en Colombia operan con volúmenes de acceso que superan significativamente el umbral de 30.000 accesos previsto en la norma, lo que hace que la evaluación concluya en la ausencia de pertinencia de establecer un régimen diferencial para ese grupo por razón de tamaño.

En lo que respecta al segundo supuesto del artículo 31 de la Ley 1978 de 2019, modificado por el artículo 141 de la Ley 2294 de 2023, la CRC evaluó si el presente proyecto normativo se enmarca en aquellos proyectos que incentivan el despliegue de infraestructura y la provisión de servicios en zonas rurales o urbanas de difícil acceso, o en municipios focalizados por las políticas públicas. La CRC constató que el presente proyecto tiene por objeto exclusivo la prevención y mitigación del fraude cibernético a través de los servicios móviles de mensajería de texto y voz, y no se orienta a incentivar el despliegue de infraestructura ni la extensión de redes a zonas no cubiertas.

En consecuencia, el supuesto de hecho que activa el mandato de evaluación de medidas diferenciales para proveedores que extienden sus redes a zonas no cubiertas o con cobertura total no se configura en el presente proyecto, por lo que no resulta aplicable este segundo mandato de evaluación. Sin perjuicio de lo anterior, se debe tener en cuenta que las obligaciones de monitoreo de tráfico que se propone adoptar en las modificaciones al artículo 2.1.10.7. de la Resolución CRC 5050 de 2016 están formuladas con flexibilidad metodológica suficiente para que cada proveedor adopte las herramientas técnicas y los criterios de detección que resulten más adecuados para su red, sin imponer un modelo único de implementación que pudiera resultar desproporcionado para operadores con infraestructuras más limitadas en zonas de menor densidad de tráfico.

8. ALTERNATIVAS DE SOLUCIÓN DEL PROYECTO REGULATORIO

8.1. Alternativas de solución identificadas previamente para mitigar el fraude cibernético por medio de servicios móviles

El 21 de noviembre de 2025, la CRC publicó para comentarios el documento en el que se presentaron las alternativas regulatorias correspondientes a los cuatro ejes temáticos contemplados en el proyecto regulatorio, respecto del cual se recibieron observaciones hasta el 22 de diciembre de 2025. Dicho documento puede ser consultado en el micrositio del proyecto regulatorio[28]. En el presente documento se recogen los comentarios remitidos por los agentes interesados y se presentan las alternativas definitivas resultantes del análisis de dichas observaciones, las cuales se someten al proceso de

[28] El vínculo para consulta directa del documento citado es el siguiente: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-alternativas-regulatorias-identificacion-medida-fraude-cibernetico-servicios-moviles.pdf

evaluación bajo los lineamientos del Análisis de Impacto Normativo (AIN), con el fin de definir las medidas que serán adoptadas para establecer mecanismos preventivos orientados a mitigar el fraude en los servicios móviles tradicionales de SMS y voz.

8.2. Comentarios del sector a las alternativas para mitigar el fraude cibernético por medio de servicios móviles

De conformidad con la publicación del documento de alternativas de solución mencionado anteriormente, la CRC recibió comentarios, observaciones y sugerencias de los siguientes agentes interesados:

REMITENTE	ABREVIATURA
ANDESCO	ANDESCO
ASOCIACIÓN BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA	ASOBANCARIA
ASOMÓVIL	ASOMÓVIL
AXESNET S.A.S.	ALDEAMO
CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO	CCE
CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES	CCIT
CÁMARA DE LA INDUSTRIA DIGITAL Y SERVICIOS	ANDI
COLOMBIA MÓVIL S.A. E.S.P.	TIGO
COLOMBIA TELECOMUNICACIONES S.A. ESP BIC	TELEFÓNICA
COMUNICACIÓN CELULAR S. A. COMCEL S. A	COMCEL
HABLAME COLOMBIA S.A. E.S.P.	HABLAME
INALAMBRIA	INALAMBRIA
PARTNERS TELECOM COLOMBIA S.A.S.	PTC
SISTEMAS SATELITALES DE COLOMBIA S.A. E.S.P.	SSC
SUPERINTENDENCIA FINANCIERA DE COLOMBIA	SFC
UNIVERSIDAD EXTERNADO DE COLOMBIA	U. EXTERNADO
ZANYA PINEDA MOLINA	ZANYA PINEDA

A continuación, se resumen los comentarios relacionados con cada una de las temáticas para las cuales se plantearon alternativas de solución, incluyendo una breve consideración de la CRC al respecto.

8.2.1 Comentarios generales

ASOBANCARIA

En relación con el problema identificado, **ASOBANCARIA** sugiere tener en cuenta que el problema central no radica exclusivamente en la ausencia normativa, ya que también se ha evidenciado que las herramientas regulatorias actualmente disponibles para prevenir el contacto fraudulento no son efectivas, lo cual justifica plenamente la gestión que se está realizando de revisión y fortalecimiento del marco regulatorio vigente.

En relación con las consecuencias disuasivas, la evaluación por impacto y la articulación intersectorial, **ASOBANCARIA** sugiere tener en cuenta que las exigencias normativas deben propender por una articulación efectiva de los actores del ecosistema y avanzar de manera complementaria en distintos frentes. En particular, **ASOBANCARIA** resalta la necesidad de incorporar consecuencias claras, progresivas y automáticas frente a la reincidencia en la facilitación del fraude, especialmente en relación con el uso indebido de códigos cortos, identificadores alfanuméricos y numeración nacional e internacional, en la medida en que la ausencia de medidas suficientemente disuasivas genera un alto retorno económico del fraude y traslada los riesgos y pérdidas al consumidor financiero y a las entidades vigiladas. Asimismo, dice, resulta fundamental que las medidas regulatorias se evalúen en función de su impacto real en la reducción del fraude financiero, y no únicamente con base en la implementación formal de controles técnicos.

En este contexto, **ASOBANCARIA** recomienda que, dentro de los actores clave involucrados en el diseño, implementación y seguimiento de las alternativas regulatorias, se incluya de manera expresa a la Superintendencia Financiera de Colombia, dada su competencia en materia de supervisión prudencial, protección al consumidor financiero y gestión de riesgos operativos y tecnológicos. De igual forma, **ASOBANCARIA** resalta la importancia de establecer mecanismos de seguimiento continuo que permitan evaluar la efectividad de las medidas adoptadas, evitando cargas excesivas, duplicidad de controles o impactos no deseados sobre la operación de las entidades financieras.

Finalmente, en materia de coordinación sectorial y cobertura de modalidades de alto impacto, **ASOBANCARIA** exige una articulación estructural y operativa entre el sector de telecomunicaciones y el sector financiero, particularmente en aspectos como el intercambio oportuno de señales de fraude, campañas activas, el uso controlado de capacidades propias de las redes móviles para robustecer procesos de autenticación financiera, la coordinación con autoridades de supervisión y judicialización, y la definición de protocolos de actuación ante eventos de suplantación.

ASOMÓVIL

Reconoce la pertinencia y oportunidad del proyecto regulatorio adelantado por la CRC para mitigar el fraude cibernético mediante servicios móviles tradicionales. No obstante, manifiesta que el documento de alternativas regulatorias omite consideraciones esenciales previamente advertidas por la industria, lo que limita la eficacia real de las medidas propuestas.

De manera transversal, el gremio insiste en que el principal déficit del marco regulatorio vigente no es la ausencia de normas, sino la falta de consecuencias efectivas frente a la reincidencia de ciertos PCA e integradores tecnológicos (IT) que facilitan de forma sistemática el fraude. En este sentido, considera que la simple recuperación de códigos cortos no genera un desincentivo real, pues los infractores pueden continuar operando mediante otros recursos o intermediarios. Por lo que reitera que debe introducirse la posibilidad de que los PRST puedan dar por terminada la relación de acceso con los PCA ante casos de reincidencia en el envío de SMS con contenidos fraudulentos.

CLARO

Reconoce que la CRC ha identificado correctamente la problemática asociada a la baja efectividad de las herramientas actuales para prevenir el fraude mediante servicios de voz y SMS. No obstante, señala que el documento de alternativas no responde adecuadamente al comentario reiterado de los PRST,

en particular aquellos orientados a permitir la terminación de contratos de acceso con PCA e integradores tecnológicos reincidentes.

El operador enfatiza que la ausencia de consecuencias contractuales frente a la reincidencia ha permitido que ciertos PCA/IT continúen enviando mensajes con contenido presuntamente fraudulento, aun después de la recuperación de códigos cortos, mediante el uso de otros códigos cortos asignados. Esta situación genera un incentivo perverso y traslada el problema operativo y reputacional a los PRST.

Destaca como un acierto probado la decisión administrativa de la CRC de suspender provisionalmente el tráfico de códigos cortos al inicio de una actuación administrativa, medida que, según evidencia operativa aportada, ha reducido de manera significativa los casos de fraude escalados a los PCA. A juicio del operador, este resultado demuestra que medidas focalizadas sobre la administración del recurso de numeración pueden ser más efectivas que la imposición de nuevas cargas tecnológicas generalizadas debido al mal uso de la numeración por ciertos actores identificados.

De manera transversal, insiste en que cualquier nueva obligación técnica debe estar precedida por un Análisis de Impacto Normativo (AIN), teniendo en cuenta los bajos cargos de acceso a SMS y la inviabilidad económica de implementar soluciones costosas en servicios de bajo margen.

TELEFÓNICA

Manifiesta su respaldo al diagnóstico general de la CRC sobre la pérdida de confianza digital derivada del incremento del smishing, vishing y la suplantación de identidad, y reconoce la necesidad de una estrategia regulatoria integral. No obstante, advierte que varias de las alternativas propuestas trasladan de manera desproporcionada cargas técnicas, operativas y económicas a los PRST, bajo la premisa errónea de que el control de la red equivale al control del origen del fraude.

El operador enfatiza que una porción sustancial del fraude se origina en eslabones de la cadena de valor con regulación más laxa (agregadores, integradores tecnológicos y PCA), por lo que cualquier intervención regulatoria debe basarse en el principio de responsabilidad en el origen, proporcionalidad regulatoria y viabilidad técnica y económica, sustentada en un Análisis de Impacto Normativo (AIN) previo.

Adicionalmente, plantea como condición habilitante central la creación de un «puerto seguro regulatorio» que faculte a los operadores a realizar bloqueos preventivos inmediatos ante patrones técnicos de fraude, sin riesgo sancionatorio posterior.

Considera que las tarifas de cargos de acceso para SMS y terminación de voz en Colombia se encuentran entre las más bajas de la región, respondiendo a una política regulatoria orientada a la reducción de costos. Por lo tanto, dice, la imposición de nuevas obligaciones tecnológicas complejas, como la implementación de Blockchain (DLT) para validación de mensajes, sistemas de monitoreo en tiempo real con inteligencia artificial o el despliegue de STIR/SHAKEN, generaría costos de transacción y operación que no son cubiertos por la estructura de ingresos actual de estos servicios. En ese contexto, **TELEFÓNICA** solicita que, previo a la adopción de cualquiera de estas alternativas tecnológicas, se realice un Análisis de Impacto Normativo (AIN) riguroso que cuantifique el costo de implementación para los agentes regulados y lo contraste con el beneficio esperado en reducción del fraude.

A juicio de **TELEFÓNICA**, existe un riesgo real de que, al elevar artificialmente los costos del canal SMS/Voz legítimo mediante cargas regulatorias excesivas, se termine incentivando el desplazamiento del tráfico corporativo hacia canales OTT (como WhatsApp) que operan fuera del alcance de la regulación nacional y donde la trazabilidad para las autoridades colombianas es aún más limitada. La regulación debe buscar el equilibrio: elevar el estándar de seguridad sin asfixiar económicamente el canal regulado.

TIGO

El operador enfatiza que, si bien el contacto inicial con el usuario suele producirse mediante SMS o llamadas, el fraude se concreta cuando el usuario es redirigido, vía datos móviles, a sitios web o aplicaciones fraudulentas, escenario que escapa al control del canal de transporte. En consecuencia, sostiene que una estrategia regulatoria efectiva no puede limitarse a imponer obligaciones técnicas sobre servicios de SMS, ni trasladar de forma desproporcionada responsabilidades a los PRST, quienes actúan como transportadores de tráfico y no como generadores ni moderadores de contenido.

Considera necesario que la CRC proceda lo antes posible a incorporar en la agenda regulatoria una segunda fase del presente proyecto, en donde se aborden alternativas para prevenir o mitigar el fraude en los servicios de datos especialmente para el control de fraude a través de aplicaciones OTT. Así mismo, sostiene que, las soluciones regulatorias deben ser costo-eficientes, en este sentido, cualquier paquete de medidas debe considerar criterios de proporcionalidad y sostenibilidad económica para los PRST, evitando exigir inversiones desmesuradas que serán ineficientes frente a la velocidad de adaptación del fraude.

U. EXTERNADO

Subraya la necesidad de que las medidas analizadas se encuentren alineadas con la Estrategia Nacional de Seguridad Digital 2025–2027, incorporando criterios de medición, trazabilidad y evaluación de impacto y, propone fortalecer el diagnóstico con tipologías (CLI spoofing, SIM swap/port-out, smishing, riesgos SS7) y alinear el paquete con estándares internacionales (E.164, ECC/CEPT, STIR/SHAKEN incl. out-of-band).

Manifiesta que, en lo que corresponde a cualquier tratamiento de datos personales que se requiera para implementar las medidas propuestas debe ajustarse a la Ley Estatutaria 1581 de 2012, el mismo se realice con énfasis en legalidad, finalidad, proporcionalidad y seguridad, y se coordine con los lineamientos de elaborados por la Superintendencia de Industria y Comercio en materia responsabilidad demostrada y privacidad desde el diseño.

Indica que, para robustecer el diagnóstico, conviene desagregar tipologías de fraude:

(i) suplantación y spoofing de CLI (Calling Line Identification) en llamadas internacionales que aparentan números nacionales;
(ii) SIM swap y port-out fraud, con toma de control de cuentas mediante cambio de SIM o portaciones maliciosas;
(iii) campañas de smishing y robo de credenciales por SMS; y
(iv) abusos en interconexión y señalización (SS7) que facilitan filtrado o manipulación de mensajes/llamadas.

Asimismo, menciona que el diagnóstico debe incorporar cifras y trazabilidad de incidentes, con métricas de call setup y patrones de tráfico, para fundamentar la proporcionalidad de las intervenciones. En su criterio, conviene desagregar las tipologías de fraude porque ello permite una caracterización más precisa de los vectores de ataque y sus impactos diferenciados.

En efecto, cada modalidad presenta mecanismos técnicos, actores involucrados y riesgos específicos que no pueden abordarse con medidas uniformes. Al segmentar estas tipologías, se facilita la adopción de soluciones regulatorias proporcionales y focalizadas, evitando respuestas genéricas que podrían resultar ineficaces o excesivamente restrictivas para la innovación.

En suma, una clasificación desagregada no solo fortalece la evidencia técnica del problema, sino que también contribuye a diseñar un marco regulatorio equilibrado, adaptable y alineado con las mejores prácticas globales.

De igual manera, a su criterio resulta esencial reforzar la autenticación en cambios de SIM y portaciones, con notificación inmediata al usuario, métodos multifactor, biometría (cuando sea proporcional y conforme a Ley 1581) y ventanas de latencia antes de habilitar cambios sensibles. La regulación comparada de la FCC introduce requisitos concretos en CPNI/LNP para obligar a los operadores a verificar y alertar ante solicitudes de SIM swap/port-out.

Indica que Colombia podría adaptar ese esquema, coordinándolo con la SIC en materia de protección de datos. A su vez, trae a colación que las recomendaciones ITU sobre riesgos SIM sugieren controles como validación IMSI/ICCID en tiempo real, detección de cambio de dispositivo (device-binding) y notificación preventiva a Proveedores de Servicios Financieros para evitar fraude en autenticaciones basadas en SMS

De manera complementaria, se sugiere fijar KPIs verificables:

(a) reducción trimestral del volumen de llamadas/SMS maliciosos detectados;
(b) tiempo medio de respuesta a incidentes (detección–mitigación–alerta al usuario);
(c) porcentaje de llamadas con autenticación (IP y out-of-band) en redes móviles;
(d) disminución de reclamaciones por SIM swap/port-out; y
(e) satisfacción del usuario (percepción de confianza). Estos KPI pueden integrarse en el tablero de control del proyecto y publicarse en informes periódicos de transparencia.

ZANYA PINEDA

Indica que el fenómeno del fraude en llamadas de voz en redes móviles constituye uno de los principales desafíos actuales para el sector de las telecomunicaciones en Colombia. No obstante, su análisis y abordaje regulatorio exige partir de una comprensión integral del ecosistema, evitando soluciones parciales que, aunque técnicamente viables, pueden generar efectos adversos sobre la competencia, la innovación y los derechos de los usuarios. En particular, menciona que las propuestas orientadas a concentrar el control del tráfico de voz en los operadores móviles, especialmente respecto de llamadas internacionales que ingresan por rutas de larga distancia, deben evaluarse con especial cautela, en la medida en que no atacan la causa estructural del problema y pueden derivar en una exclusión injustificada de actores legítimos del mercado.

Menciona que el fraude en servicios de voz no es un fenómeno aislado ni atribuible a un único segmento de la cadena de valor, y que su origen se encuentra en fallas históricas en la administración y control de la numeración móvil, derivadas de la comercialización masiva de SIM Cards sin esquemas robustos de identificación y trazabilidad del titular real. Esta situación permitió que la numeración móvil, recurso escaso administrado por el Estado, fuera utilizada de manera indebida por estructuras criminales, generando un problema que necesariamente se materializa en la terminación de llamadas en redes móviles. En este contexto, las respuestas regulatorias deben orientarse a soluciones integrales, proporcionales y técnicamente neutrales, que partan del usuario final, preserven la diversidad de actores del ecosistema y fortalezcan la confianza en el servicio de voz.

Respuesta de la CRC:

Con respecto al comentario de **ASOBANCARIA** y **ASOMOVIL** en donde sugiere que la problemática identificada no se deriva exclusivamente de la ausencia de disposiciones normativas, sino también de la limitada efectividad de las herramientas regulatorias actualmente vigentes para prevenir el contacto fraudulento a los usuarios, es importante señalar que esta Comisión evidenció la persistencia de restricciones asociadas a la eficacia práctica de los instrumentos existentes para mitigar conductas fraudulentas a través de llamadas de voz y mensajes de texto. En este sentido, la problemática no se circunscribe únicamente a la existencia formal de reglas, sino a su capacidad real de generar efectos correctivos y preventivos frente a dinámicas delictivas que evolucionan de manera constante.

En este sentido, esta Comisión acoge la sugerencia realizada por estas entidades con el fin de reflejar de manera más precisa la naturaleza del fenómeno analizado. En consecuencia, el problema central se redefine, en la sección 3 del presente documento, de la siguiente manera:

> «Baja efectividad de las herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto»

Con relación a la observación de **CCIT** en donde indica que la adopción de las medidas técnicas no puede ser considerada como neutra en costos, por lo que solicita que la evaluación regulatoria considere explícitamente el descalce entre la estructura económica del SMS y las inversiones requeridas, para evitar distorsiones e ineficiencias en el ecosistema A2P/P2P. **CLARO** y **TELEFÓNICA** opinan, en esa misma línea, que cualquier nueva obligación técnica debe estar precedida por un Análisis de Impacto Normativo (AIN), teniendo en cuenta los bajos cargos de acceso a SMS y la inviabilidad económica de implementar soluciones costosas en servicios de bajo margen. Estos aportes económicos constituyen un insumo relevante para el análisis regulatorio, los cuales serán considerados en el marco del análisis de las alternativas de esa temática, el cual forma parte del alcance ampliado de este proyecto.

Actores como **ASOBANCARIA**, **ASOMÓVIL**, **CLARO** y **TELEFÓNICA** sugieren que existen una necesidad de incorporar consecuencias claras, progresivas y automáticas frente a la reincidencia en la facilitación del fraude, en la medida en que la ausencia de medidas suficientemente disuasivas genera un alto retorno económico del fraude y traslada los riesgos y pérdidas al consumidor financiero. En concreto, **CLARO** subraya que se debe permitir la terminación de contratos de acceso con PCA e integradores tecnológicos reincidentes. Al respecto, la Comisión advierte que todos los comentarios relacionados con medidas para los escenarios de reincidencia para los PCA/IT serán abordadas por la CRC en el numeral 9.2.4. del presente documento de este escrito, en el marco de las temáticas objeto

de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación.

ASOBANCARIA advierte sobre la importancia de una articulación estructural y operativa entre el sector de telecomunicaciones y el sector financiero, particularmente en aspectos como el intercambio oportuno de señales de fraude y campañas activas. Además, recomiendan que debe incluirse a la Superintendencia Financiera de Colombia como un actor clave en la implementación y seguimiento de las alternativas regulatorias. Sobre el particular, la Comisión advierte que todos los comentarios relacionados con medidas pedagogías, campañas educativas y articulación interinstitucional serán abordadas por la CRC diferentes temáticas de evaluación presentadas de este escrito.

En relación con la facultad administrativa de la CRC de suspender provisionalmente el tráfico de códigos cortos al inicio de una actuación administrativa, **CLARO** considera que la ejecución de esa medida es un acierto y que ha reducido de manera significativa los casos de fraude escalados a los PCA. Al respecto, la CRC anticipa que todos los comentarios relacionados con la facultad de la CRC para suspender provisionalmente el tráfico, en el marco de trámites administrativos de recuperación de códigos cortos, serán abordadas por la Comisión en el numeral 9.2.4 de este escrito, en el marco de las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación.

Frente a la observación de **TELEFÓNICA** en donde expresa la posibilidad de experimentar un aumento de la carga regulatoria sobre los agentes del ecosistema de telecomunicaciones a partir de las alternativas publicadas, es importante resaltar que esta Comisión comparte la necesidad de integrar criterios de viabilidad y proporcionalidad en el marco del proceso de evaluación de alternativas con el fin de evitar efectos no deseados, tales como la transferencia de costos a determinados actores o la generación de incentivos que puedan afectar la competitividad de los canales regulados frente a otras plataformas de comunicación digital. En este sentido, el control de la infraestructura de red no implica, por sí solo, la responsabilidad exclusiva sobre el origen de las conductas fraudulentas, razón por la cual las medidas regulatorias propuestas guardan un enfoque de corresponsabilidad entre los distintos eslabones de la cadena de valor que intervienen en la provisión de servicios de comunicaciones.

Frente a las observaciones de **TELEFONICA** relacionadas con la potencial migración del tráfico legítimo hacia plataformas OTT que no se encuentran sujetas a las mismas obligaciones normativas, fenómeno que podría debilitar la capacidad de trazabilidad institucional y reducir la efectividad de las acciones de supervisión y control, es necesario señalar que el proceso de evaluación de las alternativas regulatorias implica de manera explícita el análisis de impactos competitivos, costos de implementación y efectos sobre la sostenibilidad del ecosistema digital.

En este contexto, la CRC reitera que las medidas contempladas en el proyecto no constituyen decisiones definitivas, sino alternativas sujetas a evaluación integral en el marco del AIN, instancia en la cual se valoran de forma comparativa los beneficios esperados, los costos regulatorios y la proporcionalidad de cada intervención. Dicho análisis permite identificar aquellas medidas que, además de fortalecer la prevención del fraude, resulten técnica y económicamente viables, evitando cargas innecesarias y preservando el equilibrio competitivo del sector.

Con respecto a la observación de **TIGO** en donde indica el posible traslado de las acciones fraudulentas desde los servicios tradicionales de voz y SMS hacia canales alternativos menos vigilados, como sitios web o aplicaciones fraudulentas, es preciso considerar que esta situación fue identificada por esta

Comisión, en el documento de formulación[29] y en el de alternativas regulatorias[30] del presente proyecto, al señalar que dicho fenómeno se incluye en la causa «Dificultad en la identificación y rastreo de los ataques cibernéticos», en la cual se reconoce la dinámica evolutiva de esta problemática y la capacidad de los actores maliciosos de adaptarse rápidamente a los controles regulatorios y tecnológicos. En este contexto, la CRC reconoce que el internet actúa como un habilitador transversal en la cadena del fraude, razón por la cual, las alternativas planteadas incluyen herramientas para limitar el direccionamiento hacia sitios fraudulentos, aplicaciones no verificadas o contenidos que faciliten la suplantación, cuidando la consistencia con las competencias regulatorias.

En relación con el comentario presentado por **TIGO**, mediante el cual sugiere que la CRC incorpore en la agenda regulatoria una segunda fase del presente proyecto orientada a analizar alternativas para la prevención o mitigación del fraude a través de servicios de datos, particularmente en aplicaciones OTT, esta Comisión reconoce que la evolución de las modalidades de fraude digital evidencia que los actores fraudulentos utilizan múltiples canales de comunicación, incluidos servicios de mensajería y aplicaciones que operan sobre redes de datos, lo cual plantea desafíos adicionales para las autoridades en materia de trazabilidad, coordinación institucional y alcance regulatorio. En este sentido, la CRC coincide en que el análisis de estos fenómenos requiere una aproximación integral que considere las dinámicas tecnológicas del ecosistema digital y la interacción entre distintos servicios de comunicaciones.

No obstante, es importante precisar que la incorporación de nuevas iniciativas regulatorias en la agenda de trabajo de la Comisión se realiza a través de un proceso institucional formal de planeación regulatoria. En particular, la CRC define anualmente su Agenda Regulatoria, a partir de un proceso de priorización de iniciativas, que incluye la consulta pública a los diferentes actores interesados. Este proceso cuenta con un Banco de Proyectos Regulatorios, que funciona como un repositorio de iniciativas potenciales que pueden ser analizadas y priorizadas para su eventual inclusión en futuras agendas regulatorias. Sin embargo, es necesario considerar que este proceso de viabilización tiene en cuenta el marco de competencias institucionales, las cuales se circunscribe a la provisión de redes y servicios de telecomunicaciones, dentro de los cuales se encuentran los servicios móviles de voz y datos prestados por los proveedores de redes y servicios de telecomunicaciones (PRST). Por tanto, el abordaje de la temática propuesta sobre el fraude materializado en las aplicaciones se requiere de un análisis del marco de competencias regulatorias directas sobre el funcionamiento, diseño o gobernanza de estas plataformas.

Con respecto a la sugerencia presentada por la **U. EXTERNADO**, en donde resalta que las medidas analizadas se encuentran alineadas con la Estrategia Nacional de Seguridad Digital 2025 – 2027, esta Comisión resalta la necesidad de articular los esfuerzos orientados a mitigar el fraude cibernético entre las diferentes entidades públicas, privadas, organismos de seguridad, así como agremiaciones que integran el ecosistema de los servicios de telecomunicaciones. Tanto es así que el eje temático que trata sobre las acciones enfocadas en la educación de la ciudadanía contempla estrategias de trabajo

[29] CRC. Documento de formulación del proyecto «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Página 44. Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf

[30] CRC. Documento de alternativas regulatorias del proyecto «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Página 43. Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-alternativas-regulatorias-identificacion-medida-fraude-cibernetico-servicios-moviles.pdf

conjunto con algunos agentes de dicho ecosistema como respuesta a la problemática asociada con la «ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensaje de textos», así como con la consecuencia «Desconocimiento de los usuarios respecto de la privacidad de la información, de las modalidades de ataque y de sus posibles acciones de prevención y mitigación; facilita la obtención de datos personales y la comisión de fraudes».

En relación con el comentario de la **U. EXTERNADO**, respecto de la necesidad de que las medidas planteadas por la CRC respeten los lineamientos de la Ley 1581 de 2012, la Comisión se permite aclarar que todo el proyecto ha tenido una robusta validación jurídica desde el punto de vista del respeto de los datos personales.

Ahora, con respecto a la solicitud de «fortalecer el diagnóstico con tipologías (CLI spoofing, SIM swap/port out, smishing, riesgos SS7)», así como incorporar métricas de trazabilidad, KPIs y referencias a estándares internacionales, esta Comisión considera pertinente precisar que en el presente documento se cuenta con un mayor detalle de las afectaciones económicas derivadas de distintas modalidades de fraude que afectan a los usuarios a través de servicios de voz y SMS de acuerdo con las noticias criminales. Sin embargo, también necesario aclarar que no todas las tipologías mencionadas se encuentran comprendidas dentro del objeto y alcance del presente proyecto regulatorio.

En particular, fenómenos como el SIM swap o el port-out fraud, si bien pueden relacionarse con afectaciones a la seguridad de los usuarios en el ecosistema digital, responden a dinámicas específicas de autenticación, portación y gestión de identidad móvil que no se agotan en el problema regulatorio aquí analizado. Por esta razón, tales elementos pueden servir como referencia contextual o como insumo para futuras líneas de análisis, pero no necesariamente como componentes centrales del paquete de medidas objeto de evaluación en el presente proyecto.

Frente a la sugerencia en la cual propone que el diagnóstico debe «incorporar cifras y trazabilidad de incidentes, con métricas de call setup y patrones de tráfico, para fundamentar la proporcionalidad de las intervenciones», esta Comisión considera que el planteamiento resulta pertinente y metodológicamente consistente con el AIN. En efecto, la construcción de indicadores y elementos de seguimiento permite mejorar la capacidad de evaluación ex ante y ex post de las medidas regulatorias, así como verificar su efectividad, oportunidad y razonabilidad. En este sentido, la CRC incluye en las secciones 6.2 y 6.3 la información correspondiente para el servicio de SMS, así como del servicio de voz, a partir del requerimiento de información particular realizar a los PRSTM y a las entidades financieras.

Sin perjuicio de lo anterior, la Comisión considera necesario precisar que la definición de KPIs específicos, como los sugeridos por la **U. EXTERNADO**, como por ejemplo, «reducción trimestral del volumen de llamadas/SMS maliciosos detectados», «tiempo medio de respuesta a incidentes», «porcentaje de llamadas con autenticación» o «disminución de reclamaciones por SIM swap/port-out», debe evaluarse a la luz de la disponibilidad, calidad, periodicidad y comparabilidad de la información efectivamente observable por los PRSTM. Por tanto, aunque estos indicadores constituyen referentes útiles, su adopción no puede anticiparse sin validar previamente su viabilidad técnica, la posibilidad de medición homogénea y su correspondencia con el alcance del proyecto.

Respecto a la sugerencia de «alinear el paquete con estándares internacionales (E.164, ECC/CEPT, STIR/SHAKEN incl. out of band)», la Comisión considera que los referentes y estándares

internacionales son insumos relevantes para la evaluación de alternativas regulatorias, particularmente cuando permiten identificar buenas prácticas, condiciones de implementación y experiencias comparadas. En ese sentido, la CRC acoge la utilidad de estos referentes como elementos de análisis. Sin embargo, la eventual adopción de medidas inspiradas en dichos estándares debe valorarse con arreglo a la realidad técnica, económica y competencial del entorno nacional, así como a la arquitectura actual de redes y a los costos de transición asociados. Por ello, los estándares internacionales constituyen un marco orientador, mas no un mandato automático de incorporación regulatoria.

Finalmente, frente a la propuesta de «reforzar la autenticación en cambios de SIM y portaciones, con notificación inmediata al usuario, métodos multifactor, biometría (...) y ventanas de latencia», así como la referencia a esquemas de la FCC y recomendaciones de la ITU, esta Comisión considera que dichos planteamientos son valiosos como insumo técnico y de política pública, pero no serán acogidos en esta fase como parte del núcleo regulatorio del presente proyecto, dado que corresponden a problemáticas y medidas que exceden parcialmente el alcance material aquí definido y que, además, podrían involucrar competencias concurrentes con otras autoridades, particularmente en materias de protección de datos personales, autenticación reforzada y protección del consumidor. En este sentido, estos aportes podrán ser tenidos en cuenta como insumo para eventuales análisis futuros o para ejercicios de articulación interinstitucional, pero no como parte inmediata de las alternativas objeto de evaluación dentro de este proyecto.

En relación con el comentario presentado por **ZANYA PINEDA**, en el cual se afirma que «las propuestas orientadas a concentrar el control del tráfico de voz en los operadores móviles, especialmente respecto de llamadas internacionales que ingresan por rutas de larga distancia, deben evaluarse con cautela, pues no atacan la causa estructural del problema y podrían excluir actores legítimos del mercado», esta Comisión considera pertinente realizar las siguientes precisiones:

En primer lugar, la CRC coincide con la apreciación según la cual el fenómeno del fraude en llamadas de voz constituye un problema complejo que involucra múltiples eslabones de la cadena de valor de los servicios de telecomunicaciones. En ese sentido, el fraude asociado a la suplantación de identidad, llamadas engañosas o manipulación del identificador de línea no puede atribuirse exclusivamente a un actor específico del ecosistema, por lo que su mitigación requiere medidas que reconozcan la participación de diversos agentes en el desarrollo de las acciones preventivas y correctivas, tales como operadores de red, proveedores de servicios, intermediarios de tráfico, originadores de comunicaciones y, en algunos casos, actores que operan fuera del ámbito directo de regulación nacional.

No obstante, esta Comisión considera necesario aclarar que las alternativas regulatorias analizadas en el marco del presente proyecto no buscan trasladar de manera exclusiva a los operadores móviles la responsabilidad de controlar el origen del fraude, ni establecer esquemas que restrinjan injustificadamente la participación de actores legítimos del mercado. Por el contrario, las medidas objeto de evaluación se orientan a fortalecer los mecanismos de monitoreo, trazabilidad y gestión del tráfico en los puntos de interconexión donde resulta técnicamente viable identificar patrones de comportamiento irregular, sin desconocer que el origen del fraude puede encontrarse en etapas previas de la cadena de valor o incluso fuera de la jurisdicción nacional.

En este sentido, la CRC precisa que las alternativas presentadas responden a un enfoque de gestión del riesgo distribuido, en el cual los distintos agentes del ecosistema pueden adoptar mecanismos de detección y prevención acordes con sus capacidades técnicas y su posición dentro de la cadena de

provisión del servicio. Por lo tanto, el objetivo de estas medidas no es excluir actores legítimos ni alterar las condiciones de competencia del mercado, sino fortalecer la capacidad del sistema para identificar y mitigar comportamientos fraudulentos que afectan a los usuarios. En todo caso, también necesario considerar que el análisis de proporcionalidad y balance en la asignación de responsabilidades es parte fundamental del proceso de evaluación de alternativas regulatorias.

En segundo lugar, frente a la afirmación según la cual «el origen estructural del problema se encuentra en fallas históricas en la administración y control de la numeración móvil derivadas de la comercialización masiva de SIM cards sin esquemas robustos de identificación del titular», esta Comisión reconoce que la gestión de los recursos de numeración y la identificación de los titulares de líneas móviles constituyen elementos relevantes dentro del ecosistema de seguridad de los servicios de telecomunicaciones. En este sentido, por medio de la Resolución CRC 7684 de 2025[31] se definieron «parámetros para la activación de SIM Cards, que permitan garantizar que el PRSTM recopile, verifique y registre los datos de identificación del usuario, antes de que este pueda utilizar los servicios de comunicaciones móviles a través de la SIM Card adquirida, y prohibir que el PRSTM registre como titulares de líneas móviles prepago a quienes adquieran sus SIM Cards con el fin de distribuirlas o comercializarlas a terceros».

Sin embargo, el fraude en servicios de voz responde a múltiples vectores de ataque que no se limitan al uso indebido de SIM cards, sino que también incluyen técnicas como la manipulación del identificador de llamadas (CLI spoofing), el uso de rutas internacionales irregulares, la explotación de debilidades en la señalización o el uso de plataformas tecnológicas para la generación automatizada de campañas fraudulentas.

Por esta razón, la CRC considera que atribuir la causa estructural del problema exclusivamente a la comercialización de SIM cards resulta una interpretación parcial del fenómeno, ya que no explica por sí sola las modalidades de fraude observadas actualmente en el mercado. En consecuencia, las respuestas regulatorias deben abordar el problema desde una perspectiva integral que contemple distintos puntos de control a lo largo de la cadena de comunicaciones.

Finalmente, la Comisión coincide con la observación realizada por la señora **ZANYA PINEDA** sobre la importancia de que las soluciones regulatorias se diseñen bajo criterios de proporcionalidad, neutralidad tecnológica y protección de los derechos de los usuarios, puesto que son los principios rectores del quehacer regulatorio de esta entidad. Precisamente por esta razón, para garantizar una mirada integral las alternativas regulatorias analizadas en el presente proyecto son evaluadas en el marco del AIN, con el propósito de verificar su efectividad, proporcionalidad y viabilidad económica antes de adoptar cualquier medida definitiva.

8.2.2 Respuesta a las preguntas generales de la consulta

- Considerando que la atención coordinada del fraude mediante una estrategia nacional es una necesidad urgente para el país y los usuarios, y que este proyecto regulatorio será un paso de varios en la lucha contra un fenómeno tan dinámico, ¿qué tiempos de implementación

31 CRC. Resolución CRC 7684 de 2025 «Por la cual se adoptan medidas para la promoción de la competencia, se modifican algunas disposiciones de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones». Diario Oficial No. 53.063 de 19 de marzo de 2025. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/resolucion_crc_7684_2025.htm

estima necesarios para cada una de las medidas propuestas, teniendo en cuenta los desarrollos y capacidades actuales de los PRST y agregadores? ¿Qué retos técnicos, operativos o regulatorios podrían influir en esos plazos? ¿Qué esquemas de transición o fases intermedias propondría para garantizar una metodología ágil con victorias tempranas que permita atender oportunamente la creciente oleada de comunicaciones fraudulentas en el país?

ASOBANCARIA

Comenta que el proyecto regulatorio tendrá un impacto relevante en el fortalecimiento de la seguridad de las comunicaciones en el país, lo que se traducirá en un incremento de la confianza de los usuarios para adquirir productos y servicios, así como para realizar y gestionar sus operaciones financieras de manera segura. **ASOBANCARIA** considera que los controles previstos se implementen de forma gradual a lo largo de 2026, priorizando en una primera fase aquellos mecanismos que generen beneficios inmediatos para los usuarios y permitan obtener resultados tempranos y medibles en la prevención y mitigación del fraude, sin afectar la continuidad ni la eficiencia de los servicios.

CLARO

Expone que, frente al fraude de SM, la CRC debe realizar un análisis de necesidad y proporcionalidad sustentado en evidencia reciente, lo anterior a que el proyecto reconoce reconocer cualquier obligación tecnológica debe pasar por un Análisis de Impacto Normativo (AIN), teniendo en cuenta que la suspensión provisional de tráfico ha generado una reducción significativa, y que la respuesta del mercado ha sido inmediata, sin necesidad de imponer nuevas cargas tecnológicas.

Considera que establecer plazos de implementación para medidas adicionales como autenticación obligatoria, trazabilidad avanzada, plataformas únicas, validación cruzada o estándares técnicos, la CRC debe determinar si persisten las brechas operativas que justifiquen la inversión, en la medida que las tecnológicas seguridad implican cosos superiores al ingreso asociado por mensajería -a su juicio extremadamente bajo- lo que podría generar distorsiones económicas que afectan el ecosistema A2P y traslados de cargas injustificadas a los PRST y agregadores.

Señala, que mientras la CRC evalúa formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, el país puede continuar obteniendo resultados con medidas de bajo costo, alto impacto y rápida implementación tal como el fortalecimiento de procesos de recuperación, reglas claras ante reincidencia y mayor articulación sectorial.

Concluye, que solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya existentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos, a fin de garantizar una política eficiente, proporcional y basada en evidencia. Destaca en su escrito que, si se permite a los operadores bloquear de manera inmediata los mensajes que sus herramientas tecnológicas identifiquen como presuntamente fraudulentos, el fraude a través de SMS se reduciría casi en su totalidad, y esta medida por sí misma pudiera eliminar el fenómeno.

En cuanto a las medidas móviles, señala que, si se impone la obligación regulatoria de bloqueo de llamadas internacionales enmascaradas, y que no cumplan con los requisitos técnicos y regulatorios de la numeración en Colombia, con consecuencias para los PRSTM que no cumplan, se puede controlar la problemática. Medida que no implica altas inversiones para los PRSTM y tampoco altos tiempos de implementación.

Concluye, que la CRC debe evaluar su esfuerzo en este tipo de medidas, evaluar su resultado, y de ser necesario implementar medidas como STIR/SHAKEN/RCD, las cuales son altamente costosas. Señala que las medidas propuestas tienen los siguientes retos:

- Técnicos: Integración y coordinación de sistemas de los PRST, agregadores, Carrier y operadores internacionales y entes de control, estandarización de datos y seguridad de la información.

- Operativos y financieros: Capacidad de atención y respuesta tanto de recursos humanos, de infraestructura y financieros. En un sector tan decaído, imponer medidas que generen un impacto económico tan fuerte como el propuesto, pone en riesgo la prestación del servicio.

- Regulatorios: Definición clara de obligaciones para los involucrados en la cadena de valor.

- Tiempos de implementación: implican altísimos tiempos en su implementación, poniendo en riesgo la efectividad de las mismas, pues como es sabido, el fraude se perfecciona, cambia, muta con rapidez, pudiendo hacer ver tardía e innecesaria la solución.

PTC

En relación con la alternativa consistente en la asignación y uso de un código alfanumérico (Sender ID), **PTC** estima un plazo de un (1) año para su adecuada implementación, a partir de la definición de la medida regulatoria y de los lineamientos técnicos para la gestión de los Sender ID. Sobre el punto, señala que el periodo debe cubrir ajustes en plataformas de mensajería, adecuaciones de enrutamiento y validación, y coordinación con agregadores y proveedores de servicios A2P. Además, identifica como retos principales el alto procesamiento de ESME por mayores controles de validación y la correcta implementación de enrutamiento de códigos alfanuméricos en redes de interconexión, así como también la operación continua para habilitar, eliminar y adicionar códigos. Recomienda, adicionalmente, un esquema claro de organización y unicidad para evitar duplicidades y conflictos, y propone una implementación gradual con actividades piloto controladas para remitentes de alto volumen y marcas críticas, complementado con socialización a agregadores.

Respecto de la alternativa consistente en realizar la identificación exclusiva mediante códigos cortos y numeración E.164, **PTC** estima un plazo de un (1) año para la implementación completa una vez sea asignado y habilitado el NDC 940. Indica que el tiempo se explica por la necesidad de adecuación de plataformas, la reasignación de recursos de numeración y la formalización de procesos de validación con marcas y agregadores. Como reto, resalta que la ejecución exige coordinación estrecha entre la CRC, los PRST y los agregadores, especialmente en la asignación y administración de numeración exclusiva para una correcta configuración y gestión. En este sentido, recomienda un despliegue por etapas, priorizando marcas con mayor volumen de tráfico A2P y habilitando progresivamente al resto del ecosistema.

Frente a la alternativa dirigida al establecimiento de control de patrones de tráfico atípicos, **PTC** indica que, aunque esta se asocia a actividades de aseguramiento continuo, se requeriría un (1) año para su implementación, pues los mecanismos de detección y análisis deben ajustarse a las disposiciones específicas que se adopten frente al fraude. Señala como reto clave la necesidad de mantener modelos dinámicos de detección para evitar afectaciones al uso legítimo del servicio. Para efectos de la

transición, **PTC** propone fortalecer controles existentes e incrementar gradualmente umbrales de detección, con el objetivo de permitir una adaptación progresiva y obtener resultados tempranos.

Sobre la prohibición total del enmascaramiento de la identidad del originador de la llamada, **PTC** estima un plazo de seis (6) meses, al tratarse principalmente de ajustes en reglas de enrutamiento y validación de señalización. Identifica retos operativos vinculados a órdenes de trabajo, coordinación entre áreas técnicas y ejecución de cambios en ventanas programadas para minimizar impactos en la red y propone un despliegue progresivo, al iniciar con el bloqueo de rangos de alto riesgo previamente identificados y ampliar gradualmente la cobertura conforme se consoliden los controles.

Acerca de la definición y asignación de rangos de numeración exclusivos para comunicaciones comerciales, **PTC** estima un plazo de un (1) año contado desde la creación y definición de los rangos E.164. Señala que la implementación requiere ajustes de tarificación, enrutamiento y señalización, así como una migración ordenada de actores que hoy usan numeración no diferenciada. Como fase intermedia, propone una migración gradual, iniciando con nuevos asignatarios y permitiendo un periodo de convivencia con la numeración actual.

En relación con la creación de un registro DNO, de carácter nacional y administrado por la CRC, **PTC** estima un plazo de un (1) año desde la creación y puesta en operación del registro para lograr su integración completa con los sistemas de red de los PRST. Identifica como retos la integración técnica con los sistemas de los operadores y la definición de mecanismos de actualización en tiempo real y sugiere un enfoque de transición basado en una versión mínima viable del registro, ampliando progresivamente su alcance y funcionalidades.

TELEFÓNICA

Identifica tres retos estructurales que condicionan los plazos de implementación. El primero, relacionado con la infraestructura de red (voz), ya que la implementación de protocolos de autenticación criptográfica como STIR/SHAKEN no es una simple actualización de software. A su juicio, depende de que la cadena de interconexión (nacional e internacional) curse sobre protocolo IP (SIP), mientras persistan interconexiones TDM o legadas, la «firma» de autenticación se perderá en el tránsito, inutilizando la inversión. Por tanto, **TELEFÓNICA** considera que el plazo debe estar atado a la evolución natural de las redes hacia All-IP y no a mandatos administrativos inmediatos. El segundo reto está relacionado con la interoperabilidad internacional, ya que gran parte del spoofing proviene de tráfico internacional. **TELEFÓNICA** considera que imponer reglas locales estrictas sin acuerdos de interoperabilidad con carriers internacionales y de larga distancia (LDI) podría aislar a Colombia o degradar la calidad del servicio de voz legítimo sin detener el fraude. Finalmente, el tercero reto es regulatorio, ya que en su opinión los operadores enfrentan un riesgo sancionatorio si bloquean tráfico unilateralmente.

En virtud de lo anterior, **TELEFÓNICA** propone un esquema de transición que con un enfoque de «victorias tempranas basadas en facultades» antes que en «Obligaciones tecnológicas masivas». Este esquema tendría dos fases. En la primera fase se habilitaría de manera expresa («Puerto Seguro») a los operadores para que bloqueen códigos cortos y tráfico internacional con patrones de spoofing o reportes de fraude, sin riesgo de sanciones por obstrucción. En la segunda fase se implementarían obligaciones de proceso (KYC/KYB) reforzadas para Agregadores y PCAs. Además, el operador propone el establecimiento de mesas técnicas para definir estándares de intercambio de información (APIs) entre operadores (modelo federado).

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

TIGO

Manifiesta que los tiempos de implementación dependerán del tipo y alcance de las medidas que finalmente se adopten. Señala que, en el eje de las temáticas asociadas al servicio de SMS, en el caso de la alternativa 4 de la temática 4, contribuiría el establecer un código corto o numeración E.164 único por marca.

Por su parte en el caso del eje de las temáticas de fraude a través del servicio de voz móvil, las medidas planteadas deben recaer en los Carrier internacionales, por ser quienes están en posición técnica y operativa determinante para contener el ingreso de tráfico irregular. Considera que la a alternativa 2 de la temática 3 sería la única que permitiría plantear controles para mecanismos de fraude como Robocall.

Considera que implementar todos los desarrollos propuestos en las alternativas regulatorias, implica necesariamente un horizonte de ejecución amplio y que razonablemente podría ser en mínimo 12 meses. Adicionalmente, indica que una victoria temprana es la suspensión temporal preventiva de cualquier código corto que esté cursando tráfico con indicios de fraude.

RESPUESTA CRC:

En relación con las respuestas a la consulta sobre los tiempos de implementación, los retos asociados y los posibles esquemas de transición para las medidas propuestas, la Comisión observa que, en términos generales, los aportes de los agentes evidencian varias coincidencias relevantes, así como algunas divergencias en torno al alcance y prioridad de las intervenciones regulatorias.

En primer lugar, se identifica un consenso amplio respecto a la conveniencia de adoptar esquemas de implementación gradual o por fases, priorizando aquellas medidas que puedan generar beneficios tempranos para los usuarios y resultados verificables en la mitigación del fraude, sin afectar la continuidad ni la eficiencia de los servicios. Los aportes recibidos coinciden en señalar que una estrategia progresiva permitiría reducir riesgos operativos, facilitar la adaptación del ecosistema y optimizar la relación costo-beneficio de las medidas. En este sentido, varios aportes destacan la importancia de estructurar etapas iniciales orientadas a «victorias tempranas», complementadas posteriormente con medidas de mayor complejidad técnica o institucional.

En segundo lugar, los agentes coinciden en que la definición de plazos de implementación debe considerar las capacidades técnicas actuales del ecosistema, así como los desarrollos requeridos en plataformas, sistemas de enrutamiento, mecanismos de validación y procesos de coordinación entre operadores, IT y otros actores de la cadena de valor. En particular, resaltan que la implementación de ciertas medidas podría implicar adecuaciones en infraestructuras de red, ajustes en plataformas de mensajería y fortalecimiento de mecanismos de validación e interoperabilidad, lo cual requiere horizontes de implementación realistas y esquemas de transición que permitan una adopción progresiva.

En tercer lugar, se observa una convergencia en señalar que los tiempos de implementación pueden variar significativamente según la naturaleza de cada medida. Mientras algunas intervenciones operativas, por ejemplo, ajustes en reglas de enrutamiento, validaciones de identificación o fortalecimiento de controles existentes, podrían implementarse en plazos relativamente cortos, otras

alternativas que implican cambios en procesos operativos, desarrollo de nuevas capacidades de monitoreo o coordinación entre múltiples actores podrían requerir horizontes de implementación más amplios. En varios comentarios se plantea que, en escenarios de mayor complejidad técnica, los plazos podrían situarse alrededor de un año para lograr una adopción completa en el ecosistema.

En cuarto lugar, varios aportes reiteran la necesidad de evaluar cuidadosamente la proporcionalidad de las medidas regulatorias, particularmente en lo relacionado con los costos de implementación, los requerimientos técnicos y los posibles impactos operativos para los distintos agentes del sector. En este sentido, se plantea que las medidas regulatorias deberían sustentarse en evidencia sobre la persistencia del problema y en análisis que permitan determinar si las herramientas existentes son suficientes o si resulta necesario introducir desarrollos adicionales. La Comisión considera que estas observaciones resultan consistentes con la metodología del AIN que orienta el desarrollo del presente proyecto.

Adicionalmente, algunas respuestas resaltan la importancia de considerar factores estructurales que pueden incidir en los tiempos de implementación, tales como la interoperabilidad entre redes nacionales e internacionales, la evolución tecnológica de las infraestructuras de telecomunicaciones y la necesidad de establecer mecanismos claros de coordinación entre los distintos actores del ecosistema. Estos elementos son particularmente relevantes en el caso de medidas que involucren autenticación de comunicaciones, validación de origen del tráfico o intercambio de información entre múltiples agentes.

En este contexto, la CRC considera que los comentarios recibidos aportan elementos valiosos para el desarrollo del proyecto regulatorio. En particular, estos aportes serán empleadas como insumo técnico para complementar la estructuración de las alternativas regulatorias, al aportar estimaciones sectoriales en la medida que provee elementos para establecer los tiempos de implementación, dependencias tecnológicas y necesidades de coordinación operativa.

- ¿Qué ventajas, desventajas, retos y oportunidades identifica en la implementación por parte de la CRC de mecanismos de evaluación periódica de las medidas adoptadas para mitigar el fraude mediante servicios móviles tradicionales de voz y SMS? ¿Qué criterios, metodologías o frecuencias de evaluación considera más adecuados para asegurar la efectividad y actualización continua de estas medidas?

RESPUESTAS:

ASOBANCARIA

En su sentir, para una implementación exitosa se necesita contar con un esquema de seguimiento y evaluación continua que permita medir tanto la adopción de las medidas como su efectividad en la mitigación del fraude. Añade que este seguimiento podría realizarse mediante espacios periódicos de revisión, por ejemplo, de carácter trimestral, con la participación de los principales actores del ecosistema (PRST, IT, entidades financieras y comercios), en los que se presenten los controles implementados y los resultados observados. Opina que la evaluación periódica facilita ajustes regulatorios oportunos, fortalece la corresponsabilidad entre los actores y mejora la transparencia y confianza del ecosistema.

En relación con las oportunidades, **ASOBANCARIA** sostiene que este enfoque permite identificar tempranamente nuevas tipologías de fraude, promover el intercambio de información y priorizar la adopción de medidas más efectivas. Por su parte, en lo que respecta a los criterios y metodologías, **ASOBANCARIA** recomienda utilizar indicadores claros y comparables, como la evolución de eventos fraudulentos, tiempos de detección y respuesta, y niveles de adopción de los controles.

CLARO

Expone que la implementación de mecanismos de evaluación periódica por parte de la CRC ofrece ventajas, siempre que se orienten a verificar necesidad real de nuevas medidas regulatorias, tal como evidencia de la evolución del fraude, tendencias emergentes y ajustes de los instrumentos existentes sin incurrir en cargas regulatorias innecesarias. En cuanto a las desventajas, señala que la evaluación periódica mal diseñada podría dar lugar a medidas tecnológicas costosas sin evidencia suficiente, generando cargas desproporcionadas para PRST, PCA e IT, especialmente en cuyo cargo de acceso es extremadamente bajo y no soporta inversiones de alto costo.

Concluye, que la evaluación no debe limitarse a describir el fenómeno, sino que debe determinar si persiste un problema residual que justifique nuevas intervenciones regulatorias, especialmente cuando medidas recientes ya han demostrado un impacto extremadamente positivo.

TELEFÓNICA

Identifica como ventajas que se permite ajustar la regulación a la mutación del delito, evitando normas obsoletas. Sin embargo, advierte como desventajas o riesgos el hecho de medir la efectividad basándose únicamente en el volumen bruto de PQR o reportes, lo cual puede ser engañoso (un aumento en reportes puede significar mayor conciencia del usuario, no necesariamente más fraude). Adicionalmente, **TELEFÓNICA** considera que las evaluaciones excesivamente frecuentes pueden generar una carga administrativa que desvía recursos operativos de la prevención real. Con base en todo lo anterior, **TELEFÓNICA** propone que la evaluación debe ser anual y basada en indicadores de efectividad técnica (por ejemplo, volumen de tráfico bloqueado preventivamente gracias a las nuevas facultades) y no solo en percepción. Adicionalmente, dice, la evaluación debe distinguir entre vulnerabilidades de la red móvil y fraudes de ingeniería social donde la red funcionó correctamente, pero el usuario fue engañado.

TIGO

Considera importante que la CRC lidere y articule mesas de trabajo multisectoriales que permita evaluar si las medidas son eficientes y pueda replantear las estrategias. Resulta necesario que la CRC establezca una metodología de evaluación y ajuste continuo que pueda implementarse con una velocidad similar a la dinámica de los ciberdelincuentes, de modo que la respuesta regulatoria mantenga su efectividad.

Las medidas que eventualmente se adopten deberían privilegiar un enfoque costo-eficiente, procurando que mantengan su efectividad en el tiempo y evitando escenarios de obsolescencia temprana ante la evolución de las estrategias delictivas. Indica que, dado lo anterior, exigir a los PRST inversiones significativas en desarrollos sobre sus sistemas de información o en la red podría no resultar coherente ni proporcional, considerando los plazos de implementación y el retorno esperado en términos de mitigación del fraude.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

RESPUESTA CRC:

Los aportes de **ASOBANCARIA, CLARO, TELEFÓNICA** y **TIGO** en relación con los mecanismos de evaluación periódica de las medidas adoptadas para mitigar el fraude mediante servicios móviles tradicionales de voz y SMS, así como los criterios, metodologías o frecuencias de evaluación que estos agenten consideran más adecuados para asegurar la efectividad y actualización continua de estas medidas son insumos técnicos y económicos relevantes para la estructuración de las medidas que la CRC pretende implementar en el marco de este proyecto. En consecuencia, dichos elementos serán considerados dentro del análisis técnico que se desarrolla en el marco del Análisis de Impacto Normativo (AIN).

- ¿Cuáles considera que son los principales aciertos y limitaciones de las alternativas propuestas para mitigar el contacto fraudulento a través de servicios tradicionales de voz y mensajes de texto? ¿Qué elementos adicionales o diferentes propondría para mejorar la eficacia de estas medidas?

RESPUESTAS:

ASOBANCARIA

Sostiene que el principal acierto es que las medidas en su conjunto permiten una mitigación integral del fraude que actualmente se genera a través de estos medios. No obstante, de manera complementaria a los controles propuestos, **ASOBANCARIA** considera necesario: (i) establecer mecanismos colaborativos que permitan alimentar y fortalecer los controles de monitoreo; (ii) definir niveles de servicio (SLA) para aquellas alternativas que impliquen monitoreo, bloqueo y generación de alertas; (iii) establecer procesos de KYC y validación de identidad por parte de los operadores para todos los adquirentes de líneas telefónicas, medida que ha mostrado resultados positivos en otros países, como Alemania; (iv) abordar de manera específica la problemática asociada a la reexpedición de tarjetas SIM; y (v) reforzar las medidas orientadas a la mitigación del phishing.

CLARO

Considera como acierto la implementación de la suspensión provisional de los códigos cortos cuando se está adelantando investigación administrativa por indebido uso, y que se permita el bloqueo del envío de códigos cortos cuando se evidencia que los mismos tienen contenidos presuntamente fraudulentos.

En cuanto a servicios móviles, consideran como acierto la obligación de bloquear llamadas cuando el número entrante este enmascarado, en cuanto a las demás medidas señalan que adicional a no contar con un AIN, imponen cargas onerosas a los PRSTM, situación que debe analizarse de cara a los valores de cargo de acceso.

Insiste que no obra un análisis que permita la terminación de contrato PCA/IT reincidentes, una obligación en cabeza de la CRC para realizar campañas educativas, metodologías para evaluar las solicitudes de códigos cortos, un análisis de costos que le implicaría a los PRSTM implementar las medidas, y el contraste correspondiente por los bajos montos establecidos para cargos de acceso.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

TELEFÓNICA

Considera un acierto el hecho de que la CRC reconozca la problemática del spoofing y la necesidad de validar la identidad de los remitentes en SMS. Además, a su juicio, considera que es un acierto proponer el uso de identificadores únicos y exigir mayores controles a la cadena de valor (IT/PCAs).

Por su parte, **TELEFÓNICA** opina que los costos ocultos y el internet móvil son limitaciones. Frente a los costos ocultos dice que no se evidencia una valoración de los costos de CAPEX/OPEX para los operadores al implementar tecnologías como DLT o STIR/SHAKEN, los cuales no son recuperables vía tarifas actuales. Respecto del internet móvil, **TELEFÓNICA** sostiene que el alcance limitado a SMS y Voz deja por fuera el eslabón final de la cadena de fraude (URLs maliciosas y OTTs como WhatsApp), lo que limita la eficacia integral de la estrategia.

En complemento de lo anterior, **TELEFÓNICA** propone que el modelo debe basarse en la responsabilidad en el origen. En concreto, dice que la carga de la prueba, la validación y los costos tecnológicos de autenticación deben recaer sobre quien se lucra del envío del mensaje (el Agregador/PCA), no sobre la red de transporte. Por lo tanto, este agente propone un modelo donde el operador consulta la validación realizada por el Agregador, bajo un esquema de responsabilidad legal estricta de este último.

TIGO

Señala que uno de los principales aciertos es la formulación de medidas específicas aplicables a los PCA. Considera que las medidas se deberían extender a los IT. Así como prever consecuencias aplicables a los representantes legales cuando se evidencie un uso indebido de los recursos de numeración.

Asimismo, espera un enfoque equivalente con los carriers internacionales considerando que, en la actualidad, estas empresas no cuentan con un régimen específico que regule de manera integral su actividad ni con obligaciones explícitas en materia de prevención y mitigación del fraude.

Adicionalmente, considera que medidas como el validador externo con asignación de Sender ID o STIR/SHAKEN implican desafíos relevantes, tanto presupuestales como técnicos, para su implementación. Considera que las medidas a priorizar deberían ser de implementación sencilla, rápidamente ajustables y costo-eficientes, de manera que permitan una respuesta oportuna y sostenible frente a la evolución de las modalidades de fraude.

SFC

Comenta al respecto que los principales aciertos de las alternativas propuestas se relacionan con el enfoque preventivo más activo del fraude. Para la SFC, resulta relevante que la regulación busque reducir el anonimato que hoy facilita la actuación de los delincuentes. En este sentido, medidas como la asignación de recursos de identificación exclusivos por marca, la restricción al enmascaramiento de llamadas internacionales y la validación previa de plantillas de mensajes constituyen avances importantes, en la medida en que eliminan esquemas de identidad compartida, fortalecen la confianza del usuario en el remitente y mejoran la trazabilidad para la atención de incidentes, lo que al final podría reducir los eventos de materialización de fraudes y los impactos negativos que estos incidentes

generan en los consumidores financieros, además de constituirse en un incentivo para las entidades financieras para el fortalecimiento de sus estrategias y la consolidación de una cultura de prevención.

No obstante, señala que se identifican algunas limitaciones que podrían afectar el alcance de las medidas propuestas. Una de las principales corresponde a la brecha tecnológica, en la medida en que varias de las soluciones más avanzadas como el etiquetado de llamadas o los datos enriquecidos dependen de las capacidades del dispositivo del usuario, lo que podría dejar en desventaja a quienes utilizan equipos básicos. Adicionalmente, señala que existe el riesgo de un efecto de desplazamiento, en el que los esfuerzos por controlar el fraude en el canal A2P incentiven una mayor migración de estas conductas hacia el canal P2P.

Finalmente, la SFC sugiere tener en cuenta que, de acuerdo con la complejidad técnica de algunas alternativas, como los esquemas basados en DLT o protocolos de autenticación como STIR/SHAKEN, se podrían extender los plazos de implementación.

Finaliza indicando que, para fortalecer la eficacia del marco regulatorio, la SFC considera necesario profundizar los mecanismos de colaboración entre los actores del sector. Asimismo, sugiere que la plataforma de intercambio de alertas promovida por la CRC se articule con los sistemas antifraude de las entidades financieras, de modo que se habiliten acciones coordinadas y oportunas frente a eventos de fraude.

RESPUESTA CRC:

En relación con la consulta sobre los principales aciertos y limitaciones de las alternativas propuestas para mitigar el contacto fraudulento a través de servicios tradicionales de voz y mensajes de texto, así como sobre posibles elementos adicionales que permitan mejorar su eficacia, la Comisión observa que los comentarios recibidos evidencian varias coincidencias relevantes entre los agentes, así como algunas divergencias respecto al alcance, enfoque y priorización de las medidas regulatorias.

En términos generales, se identifica una convergencia importante en reconocer como un acierto del proyecto regulatorio el enfoque integral adoptado por la CRC para abordar el fraude en comunicaciones, particularmente mediante medidas orientadas a fortalecer la trazabilidad del originador, reducir el anonimato en el uso de los recursos de identificación y establecer controles más estrictos sobre los actores que participan en la cadena de generación y entrega de mensajes o llamadas. Dentro de este enfoque preventivo, varios comentarios resaltan positivamente medidas como la asignación de recursos de identificación exclusivos, la validación de la identidad de los remitentes, el fortalecimiento de controles sobre intermediarios del ecosistema de mensajería y la posibilidad de adoptar mecanismos operativos de reacción temprana frente a indicios de fraude.

Asimismo, existe coincidencia en destacar la importancia de fortalecer la trazabilidad y la identificación del originador de las comunicaciones, en la medida en que la reducción del anonimato constituye un elemento clave para mitigar modalidades de fraude como el smishing, el spoofing o la suplantación de identidad. En este sentido, los comentarios sugieren complementar las medidas regulatorias con mecanismos adicionales de validación de identidad, controles sobre el uso de recursos de numeración, fortalecimiento de procesos de verificación de usuarios y mayores exigencias de debida diligencia para los actores que gestionan el envío masivo de comunicaciones.

De igual manera, los aportes recibidos resaltan la relevancia de fortalecer la coordinación y colaboración entre los distintos actores del ecosistema, incluyendo operadores, agregadores, entidades financieras y autoridades competentes, con el fin de mejorar la detección temprana de campañas fraudulentas y facilitar la adopción de medidas coordinadas de mitigación. En esta línea, algunos comentarios sugieren profundizar mecanismos de intercambio de información, alertas sectoriales y esquemas de cooperación que permitan alimentar los sistemas de monitoreo y fortalecer las capacidades de respuesta frente a eventos de fraude.

Por otra parte, los comentarios también coinciden en señalar ciertas limitaciones o desafíos asociados a las alternativas propuestas, particularmente en lo relacionado con los costos de implementación de algunas soluciones tecnológicas avanzadas, la necesidad de evaluar su viabilidad operativa y la conveniencia de analizar su proporcionalidad frente a los beneficios esperados. En este sentido, varios agentes destacan la importancia de considerar los impactos económicos y técnicos que podrían derivarse de la adopción de determinadas tecnologías, así como la necesidad de realizar evaluaciones rigurosas que permitan determinar la pertinencia de estas medidas dentro del contexto del mercado colombiano.

Adicionalmente, algunos comentarios resaltan posibles limitaciones estructurales asociadas al alcance del proyecto regulatorio, particularmente en lo relacionado con la evolución de las modalidades de fraude hacia canales digitales distintos a los servicios tradicionales de voz y SMS. En este sentido, se plantea que el control del fraude en estos canales podría generar efectos de desplazamiento hacia otros mecanismos de comunicación o plataformas digitales. Si bien esta observación refleja la naturaleza dinámica del fenómeno, la CRC considera que ello no desvirtúa la necesidad de fortalecer las medidas aplicables a los servicios que se encuentran dentro del ámbito de competencia regulatoria de la Comisión.

Por otra parte, se identifican algunas divergencias en cuanto a la distribución de responsabilidades dentro de la cadena de valor de las comunicaciones, particularmente respecto a cuál actor debería asumir un mayor rol en la validación de la identidad de los remitentes y en la implementación de ciertos controles técnicos. Mientras algunos comentarios plantean que estas responsabilidades deberían concentrarse principalmente en los actores que originan o comercializan los servicios de mensajería, otros resaltan la necesidad de fortalecer controles a lo largo de toda la cadena de provisión del servicio. Frente a este punto, la CRC considera que la mitigación efectiva del fraude requiere un enfoque de responsabilidades compartidas entre los distintos actores del ecosistema, acorde con sus capacidades técnicas y su rol dentro del proceso de generación, transporte y terminación de las comunicaciones.

Con base en lo anterior, la Comisión identifica que los comentarios recibidos aportan elementos relevantes para el desarrollo del proyecto regulatorio en diferentes dimensiones.

En este sentido, los aportes constituyen insumos útiles para complementar la estructuración de las alternativas regulatorias, particularmente en lo relacionado con el fortalecimiento de mecanismos de trazabilidad, la validación de identidad de los remitentes, los controles sobre intermediarios y la coordinación sectorial en la detección y mitigación de campañas fraudulentas. Así mismo, estos comentarios aportan insumos técnicos relevantes para la posterior evaluación de impacto regulatorio, especialmente en lo relacionado con los posibles costos de implementación, las dependencias tecnológicas, los retos operativos y las consideraciones de proporcionalidad que deben tenerse en cuenta en el análisis comparativo de las alternativas.

Finalmente, los aportes también constituyen consideraciones generales para el desarrollo de la propuesta regulatoria, en particular en lo relacionado con la necesidad de fortalecer la colaboración interinstitucional, promover esquemas de prevención más activos, evaluar cuidadosamente los impactos de las medidas tecnológicas avanzadas y reconocer la naturaleza dinámica del fraude en el ecosistema digital.

- ¿Qué métricas, indicadores o criterios considera que deberían establecerse en la industria para evaluar de manera efectiva la reducción del fraude y el impacto de las alternativas regulatorias propuestas en este documento? ¿Qué variables cuantitativas o cualitativas serían más útiles para medir la evolución del fraude, la protección al usuario y la eficacia de las medidas implementadas, y cómo podrían ser recolectadas y/o reportadas de forma coordinada entre los diferentes actores del sector?

RESPUESTAS:

ASOBANCARIA

Sostiene que un criterio relevante para evaluar el impacto de las medidas en la mitigación del fraude es el volumen de contactos y reportes recibidos por las entidades financieras y las entidades gubernamentales asociados a eventos de smishing y vishing. A su juicio, la evolución de este indicador permitiría identificar patrones, evaluar la efectividad de las alternativas regulatorias implementadas y medir su impacto en la protección al usuario. De manera complementaria, **ASOBANCARIA** opina que es necesario contar con un compendio consolidado de las casuísticas más recurrentes, que permita analizar los principales patrones y modalidades de fraude reportados. A su sentir, esta información serviría como insumo para la retroalimentación y ajuste continuo de los controles existentes, así como para la adopción o priorización de nuevas medidas, y podría ser recolectada y compartida de forma coordinada entre los distintos actores del sector, bajo criterios comunes de reporte y estandarización de la información.

CLARO

Expone que se debe evaluar el número de casos escalonados a los PCA, el número de recursos de numeración recuperados por la CRC por uso indebido, y el tiempo promedio de respuesta ante incidentes por parte de la CRC.

SFC

Comenta que un insumo de seguimiento en el comportamiento del fraude y sus diferentes modalidades se tiene en las cifras estadísticas de las inconformidades presentadas, y añade que la SFC hace seguimiento a la gestión de las quejas presentadas por los consumidores financieros en contra de las entidades vigiladas y consolida información estadística sobre dicha gestión.

Indica que esta información la puede consultar en la página web de la superintendencia, pestaña de Estadísticas e informes, Estadísticas de quejas:

(https://www.superfinanciera.gov.co/publicaciones/11211/consumidor-financieroinformaciongeneralquejas-contra-entidades-vigiladasdatos-estadisticos-cifras-11211/).

Añade que, posterior a junio de 2022, se cambió la metodología tanto a nivel de estructura de datos como de recepción de la información, debido a la implementación de un desarrollo tecnológico que centraliza la recepción y gestión de las quejas o reclamos, así como el seguimiento estadístico de la información.

Esta información la puede consultar en la página web de la superintendencia, pestaña de Estadísticas e informes, Estadísticas dinámicas (PowerBI)

(https://www.superfinanciera.gov.co/powerbi/reportes/506/).

TELEFÓNICA

Sugiere tres (3) métricas enfocadas a una gestión preventiva y no solo reactiva. La primera, tasas de bloqueo preventivo correspondiente a volumen de SMS y llamadas bloqueadas por filtros antispam/antifraud (muestra la proactividad de la red). El segundo, tiempo de reacción, entendido como el tiempo promedio entre la detección/reporte de un patrón de fraude masivo y su bloqueo efectivo. Finalmente, sugiere una tasa de establecimiento de llamadas (csr) anómalo equivalente a un monitoreo de picos de tráfico en rutas internacionales que no corresponden a patrones de tráfico humano (indicador de robocalling).

Finalmente, en materia de recolección, **TELEFÓNICA** considera que la información debe ser reportada de manera agregada y anonimizada para proteger la privacidad de los usuarios y la estrategia comercial de los operadores. En particular, **TELEFÓNICA** rechaza la creación de repositorios centralizados de datos crudos (PQR detallados o CDRs) por los riesgos de ciberseguridad que implican. En su opinión, la coordinación debe darse mediante mesas de trabajo donde se compartan insights y patrones (Inteligencia de Amenazas), no bases de datos de clientes.

TIGO

Señala que no resulta viable definir indicadores que permitan atribuir de manera directa la no materialización de un fraude específico a una medida aislada (p. ej., una campaña pedagógica particular) o a un actor específico. Esto se debe a que el fraude es un fenómeno multicausal, dinámico y adaptativo, y los insumos disponibles suelen provenir de reportes ex post (denuncias, PQR, quejas ante autoridades, reportes de entidades financieras), los cuales no permiten establecer con certeza una relación causal directa entre una intervención y la ausencia del evento.

RESPUESTA CRC:

La CRC valora el esfuerzo realizado por **ASOBANCARIA**, **CLARO**, la **SFC** y **TELEFÓNICA** en la elaboración de propuestas de métricas, indicadores o criterios que consideran que deberían establecerse en la industria para evaluar de manera efectiva la reducción del fraude y el impacto de las alternativas regulatorias propuestas por esta Comisión. En efecto, son interesantes las variables cuantitativas y cualitativas propuestas para medir la evolución del fraude, la protección al usuario y la eficacia de las medidas implementadas. Además, la Comisión subraya la forma en la que algunos de estos agentes interesados proponen la forma de recolección y reporte de información de forma coordinada entre los diferentes actores del sector.

A su turno, para la CRC también es relevante el aporte realizado por **TIGO**, en el sentido de indicar que no resulta viable definir indicadores que permitan atribuir de manera directa la no materialización de un fraude específico a una medida aislada y las razones que sustentan su dicho.

En consecuencia, dichos elementos serán considerados y estudiados por esta Comisión dentro del análisis técnico que se desarrolla en el marco del Análisis de Impacto Normativo (AIN) y, además, se tendrán en cuenta para el eventual análisis de impacto ex post de las medidas que finalmente sean adoptadas por la CRC.

8.2.3 Sobre las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

8.2.3.1 Comentarios generales en el contexto de las medidas asociadas al servicio SMS

ALDEAMO

Aporta un argumento económico: el bajo precio regulado del SMS en Colombia incrementa la rentabilidad del fraude; propone evaluar desregular el precio para desincentivar intentos masivos y financiar controles. Recalca que las medidas deben definirse en mesas técnicas multi-actor para evitar diseños impracticables.

ANDESCO

En las temáticas asociadas al canal SMS, plantea que varias de las alternativas técnicas discutidas, tales como mecanismos de autenticación/validación, trazabilidad del origen, controles A2P/P2P, estandarización de listas antifraude o aprovechamiento de APIs de red; requieren ser sometidas a un AIN específico que estime costos, beneficios y efectos competitivos.

En particular, advierte que los cargos de acceso a SMS con los que se remunera a los PRSTM serían bajos frente a los costos de implementación de soluciones tecnológicas avanzadas, de modo que imponer obligaciones costosas en un servicio con ingresos reducidos podría generar ineficiencias, distorsiones y riesgos de sostenibilidad del ecosistema.

Con este marco, sostiene que la regulación debería ser estrictamente necesaria, proporcional y sostenible, y que se debe descartar duplicidad de cargas cuando existan instrumentos que ya estén mostrando resultados operativos. Solicita a la CRC que analice con detalle los efectos que ya han tenido las herramientas vigentes, particularmente el bloqueo provisional de mensajes de texto asociados a investigaciones por uso indebido, mecanismo que, según los resultados operativo experimentado por los operadores, ha reducido considerablemente la problemática.

Insiste en que, antes de incorporar obligaciones tecnológicas adicionales, la CRC debe evaluar el desempeño de herramientas ya implementadas, asegurar un Análisis de Impacto Normativo (AIN) que sustente proporcionalidad y viabilidad, y evitar que el diseño regulatorio traslade de manera predominante a los PRST móviles (PRSTM) cargas y responsabilidades que también recaen en PCA/IT

(proveedores de contenido/aplicaciones e integradores tecnológicos) y en la propia administración del recurso de identificación.

ANDI

Advierte que es fundamental que la CRC tenga en cuenta las tarifas de cargos de acceso a SMS con los cuales se remunera a los PRSTM por el envío de estos mensajes de texto y que dichos valores no contemplan ni soportan los costos que se generan por la implementación de estas medidas. Por lo anterior, la ANDI sostiene que la adopción de nuevas obligaciones tecnológicas para mitigar el fraude mediante servicios móviles exige un Análisis de Impacto Normativo (AIN) que permita evaluar su viabilidad técnica, económica y jurídica. En su opinión, este análisis es indispensable para garantizar que las soluciones regulatorias sean proporcionales, consistentes con el problema identificado y compatibles con los principios de economía, eficiencia, interoperabilidad, trazabilidad y cooperación interinstitucional. En concreto, la ANDI considera que, sin un AIN para cada una de las medidas acá presentadas, se genera el riesgo de imponer cargas regulatorias excesivas o inaplicables, especialmente en áreas donde la tecnología evoluciona rápidamente y requiere validación rigurosa antes de convertirse en mandato obligatorio.

A manera de conclusión, la ANDI considera que es fundamental considerar que las medidas planteadas implican altos costos de implementación tecnológica, los cuales no se corresponden con la estructura económica del servicio, especialmente cuando se comparan con el bajo valor del cargo de acceso de un SMS. Para la ANDI, imponer soluciones costosas en un entorno donde el ingreso por mensaje es mínimo puede generar ineficiencias, distorsiones competitivas e incluso afectar la sostenibilidad del ecosistema A2P/P2P. Por lo tanto, dice, un AIN resulta imprescindible para balancear costos y beneficios, estimar impactos sobre operadores, PCA/IT y usuarios, y asegurar que cualquier obligación adicional sea realmente necesaria, proporcional y sostenible.

En este sentido, se hace necesario que antes de analizar las propuestas regulatorias planteadas, la CRC, entre otras cosas, permita el bloqueo de SMS/llamadas/nacionales/internacionales, cuando se evidencie posible fraude.

ASOMÓVIL

Subraya que muchas de las alternativas propuestas imponen cargas técnicas y económicas significativas a los PRST, pese a que estos no controlan el origen del contenido fraudulento. Por ello, enfatiza que cualquier nueva obligación debe estar precedida por un Análisis de Impacto Normativo (AIN) que evalúe su viabilidad técnica, legal y económica, especialmente considerando que los servicios de voz y SMS son productos en declive.

CCE

De manera transversal, la CCE reconoce que la CRC ha identificado las grandes temáticas del proyecto (SMS, voz, educación y régimen de numeración), pero advierte que es fundamental que la CRC tenga en cuenta las bajas tarifas de cargos de acceso a SMS con los cuales se remunera a los PRSTM por el envío de estos mensajes de texto, ya que son valores que no contemplan ni soportan los costos que se generan por la implementación de estas medidas.

En consecuencia, en opinión de la CCE, la adopción de nuevas obligaciones tecnológicas para mitigar el fraude mediante servicios móviles exige un Análisis de Impacto Normativo (AIN) que permita evaluar su viabilidad técnica, económica y jurídica, con la finalidad de garantizar que las soluciones regulatorias sean proporcionales, consistentes con el problema identificado y compatibles con los principios de economía, eficiencia, interoperabilidad, trazabilidad y cooperación interinstitucional. Para la CCE, sin un AIN para cada una de las medidas acá presentadas, se genera el riesgo de imponer cargas regulatorias excesivas o inaplicables, especialmente en áreas donde la tecnología evoluciona rápidamente y requiere validación rigurosa antes de convertirse en mandato obligatorio.

La CCE insiste en que es fundamental considerar que muchas de las medidas planteadas implican altos costos de implementación tecnológica, los cuales no se corresponden con la estructura económica del servicio, especialmente cuando se comparan con el bajo valor del cargo de acceso de un SMS. A su juicio, imponer soluciones costosas en un entorno donde el ingreso por mensaje es mínimo puede generar ineficiencias, distorsiones competitivas e incluso afectar la sostenibilidad del ecosistema A2P/P2P. En concreto, para la CCE en AIN resulta imprescindible para balancear costos y beneficios, estimar impactos sobre operadores, PCA/IT y usuarios, y asegurar que cualquier obligación adicional sea realmente necesaria, proporcional y sostenible.

CCIT

Advierte que, aunque la CRC plantea medidas técnicas amplias (autenticación/validación, trazabilidad, controles A2P/P2P, listas anti-fraude, herramientas para administración de recursos de identificación, mitigación de redireccionamiento a sitios fraudulentos y uso de APIs/datos de red), su adopción no puede asumirse como neutra en costos. En particular, subraya que los cargos de acceso a SMS que remuneran a los PRSTM son bajos y, en su criterio, no contemplan ni soportan los costos que implicaría implementar obligaciones tecnológicas adicionales para mitigar fraude en este canal. Desde esta perspectiva, pide que la evaluación regulatoria considere explícitamente el descalce entre la estructura económica del SMS y las inversiones requeridas, para evitar distorsiones e ineficiencias en el ecosistema A2P/P2P.

Insiste en que la CRC realice un AIN «para cada una de las medidas» que se pretenda adoptar, con el fin de balancear costos y beneficios, estimar impactos sobre operadores, PCA/IT y usuarios, y asegurar que cualquier obligación sea necesaria, proporcional y sostenible. Además, plantea un orden de análisis: primero evaluar el efecto de herramientas vigentes asociadas a control del recurso (como el bloqueo/suspensión provisional en investigaciones por uso indebido) para determinar si las medidas adicionales son realmente necesarias; y, solo después, desarrollar el AIN de las propuestas tecnológicas restantes.

TIGO

Manifiesta que el documento publicado sobre las alternativas regulatorias incorpora la definición de agregador como «empresas que envían SMS en nombre de otras». En este sentido, señala que dicha definición no se encuentra actualmente prevista en la Resolución CRC 5050 de 2016, por lo que resulta necesario precisar su alcance y efectos regulatorios. Indica que no es claro si esta categoría pretende cobijar o diferenciar a los actuales agentes que, en la práctica, pueden ostentar la calidad de asignatarios de códigos cortos, tales como los PCA y los IT.

Señala que el documento antes indicado sugiere que los agregadores deben verificar la legitimidad de sus clientes (marcas), lo cual podría interpretarse como una obligación dirigida principalmente a quienes mantienen una relación comercial directa con dichas marcas (típicamente, los PCA). Adiciona que esta medida dejaría por fuera a los IT quienes pueden ser asignatarios de códigos cortos y, por tanto, podrían habilitar directa o indirectamente el envío de SMS bajo su asignación. En tal escenario, se generaría una asimetría regulatoria y un incentivo a reconfigurar modelos de operación para eludir controles, trasladando el riesgo hacia los eslabones menos exigidos.

Solicita que las medidas que se definan se estructuren bajo un principio de cobertura completa del riesgo: las obligaciones de debida diligencia, trazabilidad, controles de abuso y verificación de legitimidad deben recaer sobre todo asignatario del recurso de identificación que soporte el servicio de SMS A2P.

Respuesta de la CRC:

Respecto a los comentarios presentados por **ALDEAMO**, **ANDESCO**, **ANDI**, **ASOMOVIL**, **CCE** y **CCIT** en relación con la necesidad de someter las alternativas técnicas asociadas al canal SMS a un análisis específico de impacto regulatorio, así como a la preocupación sobre la sostenibilidad económica de eventuales obligaciones en un servicio con ingresos decrecientes, esta Comisión considera pertinente señalar que el presente proyecto regulatorio se desarrolla bajo la metodología establecida por el Análisis de Impacto Normativo (AIN), la cual contempla precisamente la evaluación sistemática de los costos, beneficios y proporcionalidad de las alternativas regulatorias identificadas. En este sentido, las medidas relacionadas con mecanismos de autenticación, validación, trazabilidad, controles sobre tráfico A2P/P2P y herramientas de prevención del fraude no constituyen decisiones adoptadas, sino hipótesis regulatorias sujetas a valoración técnica, jurídica y económica en el marco del AIN.

En concreto, el análisis regulatorio desarrollado en el presente documento tiene en cuenta los potenciales costos de implementación de cada una de las medidas propuestas como un criterio de evaluación, con el propósito de evitar imponer cargas desproporcionadas que puedan generar distorsiones en la estructura de costos o afectar la viabilidad del servicio. No obstante, es necesario resaltar que, tal como se indica en el árbol de problema identificado en capítulos precedentes (ver sección 3), el uso indebido del canal SMS para fines fraudulentos genera externalidades negativas relevantes, tales como la pérdida de confianza de los usuarios, costos asociados a la gestión de incidentes de fraude y afectaciones reputacionales para el sector. En consecuencia, el análisis de proporcionalidad regulatoria aplicado permite balancear los costos de implementación con los beneficios asociados a la mitigación de riesgos sistémicos.

Respecto al orden de análisis propuesto por **ANDESCO** y **ASOBANCARIA**, orientado a evaluar inicialmente la efectividad de herramientas vigentes antes de considerar medidas adicionales, la Comisión considera que dicha aproximación resulta consistente con los principios de mejora regulatoria. En este sentido, el AIN incorpora la revisión de los instrumentos actualmente disponibles para la gestión del riesgo bajo la alternativa del Statu Quo, la cual es parte integral de todas las temáticas analizadas. En particular, esta alternativa incluye los mecanismos asociados al control del recurso de identificación vigentes, tales como el bloqueo o la suspensión provisional de servicios en el marco de investigaciones por uso indebido. En este sentido, el AIN incluye del análisis de las herramientas actuales para determinar la efectividad relativa de cada alternativa, la existencia de

brechas o problemas residuales y la necesidad de fortalecer o complementar el marco regulatorio vigente.

Así mismo, esta Comisión coincide en que la regulación debe evitar duplicidades innecesarias cuando existan instrumentos que ya estén generando resultados operativos. En este sentido, la evaluación de nuevas alternativas no parte de la premisa de ausencia de reconocimiento de las herramientas existentes, sino de valorar si los instrumentos actuales son suficientes para atender la problemática identificada o si requieren fortalecimiento.

Respecto al comentario presentado por **TIGO** en relación con la definición de «agregador» incluida en el documento de alternativas regulatorias y su posible alcance frente a las categorías previstas en la Resolución CRC 5050 de 2016, esta Comisión considera pertinente realizar las siguientes precisiones:

En primer lugar, la Comisión aclara que la referencia a «agregadores» contenida en el documento tiene un propósito descriptivo para ilustrar funciones de intermediación presentes en la cadena de provisión del servicio SMS A2P. No obstante, con el fin de evitar ambigüedades terminológicas, se precisa que dicha referencia correspondía en realidad a los integradores tecnológicos (IT) en los términos definidos por la regulación vigente. En consecuencia, se realizará la corrección correspondiente en el documento soporte para mantener coherencia con las categorías regulatorias existentes. En segundo lugar, es importante señalar que el uso de dicha expresión no tiene como finalidad crear una nueva categoría jurídica ni modificar implícitamente las definiciones previstas en el marco regulatorio, sino facilitar la comprensión de los roles operativos que intervienen en el ecosistema A2P.

Por otro lado, la CRC reconoce el análisis realizado por este operador en lo relacionado con las diferentes configuraciones operativas, en las que se indica que los actores clasificados como PCA o IT pueden desempeñar funciones similares dentro de la cadena de provisión del servicio. En este contexto, las medidas regulatorias en evaluación, no se orientan a imponer obligaciones con base en denominaciones formales, sino a analizar la pertinencia de asignar responsabilidades conforme al rol funcional que cada actor desempeñe en el uso y gestión del recurso de identificación y en el control efectivo del tráfico cursado.

Respecto a la preocupación presentada por **TIGO** sobre una posible asimetría regulatoria en la imposición de obligaciones de verificación de legitimidad, es necesario indicar que esta Comisión comparte la importancia de evitar vacíos de exigibilidad que puedan generar incentivos para reconfigurar esquemas operativos con el fin de eludir controles. En este sentido, el análisis regulatorio considera relevante evaluar la conveniencia de que adoptar obligaciones relacionadas con la debida diligencia, verificación de legitimidad, trazabilidad y control del uso del recurso recaigan sobre todos aquellos actores que ostenten la calidad de asignatarios de recursos de identificación o que ejerzan control efectivo sobre su utilización.

Bajo este enfoque, la determinación de responsabilidades no se limita a la naturaleza jurídica del agente, sino a su participación material en la cadena de provisión del servicio y a su capacidad de control sobre el uso del recurso de identificación. Este criterio funcional busca reducir asimetrías regulatorias, cerrar brechas de exigibilidad y mitigar incentivos de arbitraje regulatorio.

Finalmente, la evaluación de la pertinencia de realizar precisiones conceptuales sobre roles, definiciones y responsabilidades en el ecosistema SMS A2P en el marco de la cobertura integral del

riesgo, forman parte del análisis integral que se adelanta en el marco del presente proyecto regulatorio, particularmente en lo relacionado con la revisión del Régimen de Administración de Recursos de Identificación.

8.2.3.2 Subtemática 1: Falta de identificación clara del remitente en SMS A2P

ALDEAMO

Propone que la decisión de adopción de dicha medida no sea consecuencia del tipo de mensaje «transaccional vs promocional», sino que sea a discreción de la entidad que lo desee. Plantea la creación de varios niveles:

- Entidades que quieran identificarse con Sender ID alfanumérico. «recomendable para aquellas que son suplantadas en los intentos de fraude».
- Entidades que quieran tener un código corto exclusivo. «recomendable para entidades que envían muchos mensajes y que no tienen riesgo de fraude. Ej: mensajes de mercadeo»
- Entidades que estén dispuestas a compartir un código corto

En este mismo sentido señala que las entidades más utilizadas para engañar a usuarios, entidades financieras, empresas de servicios públicos y operadores móviles, adopten Sender ID alfanuméricos sin volverlos obligatorios para todos.

Sobre el proceso de asignación del Sender ID manifiesta que este debe ser corto, sencillo, coordinado por los operadores móviles y que permita fácilmente a una empresa enviar mensajes.

Adicionalmente, considera útil que una empresa pueda configurar varios Sender IDs alfanuméricos para diferenciar su tráfico, por ejemplo:

- Banco XX – Citas
- Banco XX – Transacciones
- Banco XX Mercadeo

ASOBANCARIA

Recomienda que el uso de nombres o marcas vinculadas a entidades vigiladas esté respaldado por mecanismos robustos de validación, que prevengan la utilización indebida de denominaciones reconocidas por parte de terceros no autorizados, de lo contrario, se podría generar una falsa percepción de seguridad en los usuarios y, en consecuencia, incrementar la efectividad de esquemas de fraude de alcance masivo. En este sentido, resalta la necesidad avanzar hacia criterios uniformes, esquemas centralizados y reglas claras de gestión que permitan mitigar de manera estructural el uso indebido de marcas bancarias. En complemento de lo anterior, sostiene que la asignación de códigos alfanuméricos debería otorgarse exclusivamente a comercios y entidades reales, evitando su uso por empresas fachada o estructuras creadas con fines fraudulentos, lo cual fortalecería la trazabilidad de la cadena de valor y maximizaría el impacto preventivo de la medida.

Por su parte, **ASOBANCARIA** sostiene que las alternativas basadas exclusivamente en la diferenciación de mensajes promocionales no se consideran suficientemente eficaces, pues es precisamente en este tipo de tráfico en donde se concentra una proporción significativa del fraude por smishing. En complemento de lo anterior, **ASOBANCARIA** considera necesario que las alternativas regulatorias incorporen de manera expresa la obligación de implementar controles técnicos preventivos a nivel del canal SMS.

ASOMÓVIL

Coincide con el diagnóstico de la CRC sobre las debilidades estructurales de trazabilidad en el tráfico A2P, pero rechaza la premisa de que estas falencias se deban a la inexistencia de lineamientos regulatorios. A su juicio, la regulación vigente ya establece obligaciones claras para PCA y PRST en materia de seguridad, prevención del fraude y monitoreo del tráfico.

El problema central identificado por el gremio es la reincidencia sistemática de ciertos actores, quienes asumen la recuperación del código corto como un costo marginal frente al beneficio económico obtenido. En consecuencia, considera indispensable que la CRC incorpore un régimen específico contra reincidentes, con medidas escalonadas y efectivas, tales como: prohibición temporal o definitiva de recibir nuevas asignaciones de numeración, periodos de mora para la entrega de nuevos códigos y, en casos graves, la pérdida del registro como proveedor.

Asimismo, ASOMÓVIL advierte que las alternativas basadas en plataformas, monitoreo en tiempo real, mecanismos de autenticación/verificación, integraciones y reportes, pueden resultar ineficientes si no se ataca el problema desde el origen y si no se asignan responsabilidades claras al eslabón de mayor riesgo.

CLARO

Manifiesta que la CRC debe hacer una evaluación exhaustiva de los solicitantes de la numeración, en donde constate las calidades, condiciones, y demás requisitos que permitan dar tranquilidad del uso que se va a dar al potencial asignatario de la numeración, y no trasladar con posterioridad el problema a los PRSTM quienes se ven obligados a implementar medidas tecnológicas para evitar el envío de mensajes con contenido fraudulento.

Así mismo, indica que frente al uso indebido de los códigos cortos se debe recuperar y no volver a asignar hasta tanto demuestre que implementó medidas que evidencien su buen uso. Solicita que en los casos en que se evidencie de manera reiterada el mal uso de este recurso de identificación por parte de los mismos PCA/IT se inicié el proceso de terminación de los acuerdos de acceso con los infractores reincidentes.

Recomienda que en las alternativas 2 y 3, de la temática «Falta de identificación clara del remitente en SMS A2P», deben dejar claramente establecido en la regulación que el encargado de cumplir con estas obligaciones es el PCA/IT, dado que a su parecer es el dueño del código y es quien conoce el contenido del mensaje que va a remitir.

Advierte que, en ausencia de una asignación clara de responsabilidades, los PCA continúan operando en la ambigüedad regulatoria, incumpliendo obligaciones sin consecuencias efectivas. Así mismo,

señala que debe evitarse la asignación de identificadores que generen confusión al usuario mediante variaciones mínimas de marcas legítimas.

En adición, solicita a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determinar si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada.

HABLAME

Coincide con el objetivo de mejorar la identificabilidad del originador de contenidos A2P, pero cuestiona que ello se logre mediante esquemas que introduzcan fricciones regulatorias o cuellos de botella operativos. En particular, apoya la asignación clara de identificadores por remitente, y propone como práctica «estándar» en consolidación internacional la inclusión, al inicio del cuerpo del mensaje, de un identificador entre corchetes con el nombre de la empresa o persona que origina el contenido (p. ej., « [EMPRESA XYZ] …»), por considerarlo un mecanismo inmediato, informativo y que no sacrifica la agilidad del mercado.

En contraste, rechaza que se imponga obligatoriamente el uso de IDs alfanuméricos, numeración internacional identificable o numeración no geográfica 940, argumentando que la asignación y habilitación de esos recursos puede tardar varios meses y, por tanto, resulta inviable para emprendimientos y dinámicas comerciales que requieren operar en plazos de horas o días. De fondo, enfatiza que diseñar estas obligaciones sin reconocer las particularidades del mercado A2P - y tratándolo como si fuese homogéneo o equivalente al P2P - constituye, en su criterio, un error técnico y regulatorio con potencial de frenar innovación y competencia.

PTC

Considera que la alternativa que propone la obligatoriedad del uso de Sender ID alfanuméricos únicos para tráfico A2P constituye una medida efectiva y proporcional para mitigar el fraude por suplantación de identidad en SMS. En su criterio, el valor central de esta medida está en que la identificación sea inequívoca y verificable a nivel de encabezado del mensaje, para reducir la posibilidad de que actores maliciosos se hagan pasar por marcas legítimas.

Este operador complementa esta posición indicando que, para que el esquema funcione, debe existir una organización clara de los códigos (evitando duplicidades y conflictos entre marcas o remitentes) y una implementación gradual, idealmente iniciando con un piloto controlado concentrado en remitentes de alto volumen y marcas críticas, acompañado de socialización con agregadores, de forma que se logren resultados tempranos en reducción de fraude.

SFC

Apoya la identificación verificada prioritaria para el sector financiero y exige mecanismos que eviten afectación al tráfico legítimo (continuidad sistema de pagos). Resalta necesidad de canales de coordinación operador-usuarios masivos del canal SMS para evitar bloqueos indebidos y delimitar sujeto obligado (operador vs usuario del canal), y destaca la conveniencia de que las entidades financieras participen activamente en plataformas de intercambio de alertas relacionadas con tráfico A2P fraudulento, aportando información relevante sobre eventos detectados.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

TELEFÓNICA

El operador considera que la identificación clara del remitente mediante sender ID único y validado es un elemento positivo para reducir la suplantación, siempre que esté acompañado de procesos rigurosos de validación previa de marcas y campañas en el origen.

No obstante, enfatiza que la simple obligatoriedad del identificador, sin controles robustos de registro y validación, puede generar una falsa sensación de seguridad al usuario. La responsabilidad por el registro, custodia y actualización de los sender ID debe recaer en agregadores y PCA, no en los PRST.

TIGO

Identifica como uno de los principales inconvenientes del ecosistema SMS A2P la indeterminación del sujeto responsable dentro de la cadena de provisión del servicio, derivada de la ausencia de obligaciones según el rol de cada asignatario de códigos cortos. Así mismo, indica que las definiciones para los PCA e integradores tecnológicos (IT), vigentes en la regulación, pueden solaparse funcionalmente según las actividades que desarrollen lo que habilita la coexistencia de múltiples configuraciones en este mercado y con ello una mayor complejidad para determinar responsabilidades cuando ocurre un caso de fraude.

Adicionalmente, manifiesta que tanto PCA como IT pueden ubicarse en una posición equivalente desde el punto de vista de la asignación del recurso, pero el régimen solo expresa obligaciones para los PCA respecto del acceso a las redes móviles para la provisión de contenidos y aplicaciones mediante SMS/USSD. De igual forma, señala que las obligaciones relacionadas con la identificación del asignatario recaen únicamente sobre los PCA, dejando por fuera a los IT, pese a que estos también pueden ostentar la calidad de asignatarios de códigos cortos. Este operador concluye que se evidencia una asimetría regulatoria: la norma reconoce que los IT y PCA pueden ser asignatarios y pueden intervenir materialmente en la cadena de envío, pero sólo impone obligaciones explícitas a los PCA en el marco del acceso.

En consistencia, solicita que el marco regulatorio incorpore obligaciones específicas para los IT en relación con el acceso a las redes móviles y la provisión de SMS/USSD; incluso tales obligaciones deberían ser idénticas para ambos agentes. Adiciona que, tanto quien puede solicitar el recurso de identificación, como quien tiene el rol de utilizarlo a través del acceso que establezca con las redes de los PRST no pueden quedar fuera del régimen de obligaciones mínimas.

Señala que si bien la «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)», contemplada en la alternativa 2 de esta temática, podría facilitar que el usuario identifique el nombre de la entidad originadora del mensaje (marca), ello no garantiza, por sí mismo, que el usuario no termine siendo víctima de una campaña de smishing debido a que la simple visualización del «remitente» puede incluso generar una falsa sensación de legitimidad. Plantea que el mayor valor de esta medida podría materializarse si se articula como insumo dentro de un esquema de trazabilidad y atribución del tráfico como el planteado en la temática 2, en el cual la identificación del originador no solo sea un elemento informativo, sino un componente que permita rastrear el recorrido del mensaje de inicio a fin. En este sentido, solicita no implementar las medidas que incluyan la adopción de un Sender ID alfanumérico, concluye afirmando que las medidas con mayor potencial de efectividad son aquellas orientadas a fortalecer la atribución única de un código corto por marca

que permita tener la trazabilidad del origen del mensaje, así como, el asignatario responsable del debido uso del código corto

En sus comentarios, el operador señala que la regulación vigente reconoce tanto a PCA como a IT como posibles asignatarios de códigos cortos, pero solo impone obligaciones explícitas a los PCA, lo que introduce una asimetría regulatoria que es explotada por actores fraudulentos. En este contexto, TIGO considera necesario que cualquier alternativa regulatoria establezca obligaciones idénticas y mínimas para todos los asignatarios del recurso de numeración, independientemente de su rol contractual.

Respecto de las alternativas propuestas, TIGO descarta el statu quo y considera que los esquemas de trazabilidad deben centrarse en la atribución única del recurso por marca, de manera que sea posible identificar con claridad al responsable del tráfico.

Respuesta de la CRC:

En relación con el comentario de **ALDEAMO**, en el cual propone la adopción de una medida en donde se permita la discrecionalidad en la selección de la categoría del tipo de recurso de identificación para el envío de SMS A2P, esta Comisión agradece el aporte al proceso de construcción de alternativas regulatorias. Como resultado del análisis técnico se encontró que esta opción presenta problemas estructurales que podrían disminuir su efectividad a la hora de mitigar el riesgo de acciones irregulares con fines de fraude. En particular, permitir que las entidades escojan libremente entre Sender ID alfanumérico, código corto exclusivo o código corto compartido podría generar asimetrías en los estándares de seguridad aplicables a cada tipo de tráfico, debilitando el objetivo central de la medida, que es fortalecer la trazabilidad, autenticidad y confiabilidad del remitente.

Esta Comisión señala que un esquema discrecional podría generar efectos no deseados como: el riesgo de falsa percepción de autenticidad, persistencia de los problemas de trazabilidad en los códigos cortos compartidos, incentivos regulatorios subóptimos dado el potencial aumento de la carga administrativa y complejidad de supervisión y seguimiento debido a la dificultad de establecer reglas claras y suficientes para la asignación de este recurso de identificación.

Respecto a la propuesta en la que sugiere que determinadas entidades, como entidades financieras, empresas de servicios públicos u operadores móviles, adopten Sender ID alfanuméricos sin hacerlo obligatorio para todos, la Comisión reconoce que este enfoque puede resultar razonable desde una perspectiva de gestión de riesgo. Es necesario señalar que esta sugerencia podría enmarcarse dentro de la alternativa 3 formulada como posible solución a la problemática identificada. En específico, bajo esta medida se introduciría la «obligatoriedad de que el Sender ID alfanumérico sea aplicado únicamente a mensajes transaccionales, mientras que el tráfico promocional continúa identificándose mediante códigos cortos o números E.164.». Es preciso señalar que esta alternativa debe ser evaluada bajo criterios objetivos que permitan definir su viabilidad y desempeño frente a las demás alternativas, y de igual manera, establecer qué entidades estarían obligadas y cuáles no, evitando generar vacíos regulatorios o incentivos de arbitraje.

Frente a la recomendación de **ALDEAMO** en donde solicita que el uso de Sender ID's alfanuméricos sean diferenciables (p. ej.: Banco XX – Citas), es importante señalar que dentro de la alternativa que propone su adopción se contempla que aquellos que sean asignatarios de dicho recurso de

identificación puedan establecer un encabezado único asignado a la marca o razón social de las empresas con un límite de caracteres determinado por las condiciones técnicas del servicio. En este sentido, en el caso en que esta alternativa llegase a ser implementada, el asignatario de este recurso de identificación podría solicitar diferentes códigos alfanuméricos, siempre que cumpla con los requisitos técnicos de extensión, así como con los siguientes:

- Cada identificador esté previamente validado y asociado inequívocamente a la empresa o razón social.
- Exista trazabilidad individual por identificador.
- No se generen riesgos de confusión o uso indebido.
- Se demuestre la necesidad razonable y uso frecuente del recurso.

No obstante, como se señaló anteriormente, las alternativas regulatorias contempladas (en este caso específico el uso de múltiples identificadores de códigos alfanuméricos con una raíz común) deben evaluarse a la luz de criterios objetivos tales como su impacto en la experiencia del usuario y en la claridad del ecosistema de identificación, evitando fragmentar la percepción de autenticidad.

En esta misma línea, frente a la solicitud de **ASOBANCARIA, CLARO, PTC** y **TELEFÓNICA** relacionada con la implementación de mecanismos centralizados y el uso de reglas para la asignación del recurso de identificación, es importante resaltar que esta Comisión reconoce la necesidad de contar con herramientas robustas para mitigar el riesgo de uso indebido de marcas, particularmente aquellas asociadas a entidades vigiladas como las del sector financiero. En efecto, el uso no autorizado de denominaciones ampliamente reconocidas por los usuarios, como marcas bancarias, empresas de servicios públicos u operadores de telecomunicaciones, puede generar una falsa percepción de legitimidad, lo que incrementa significativamente la probabilidad de éxito de esquemas de fraude por medio del uso SMS (smishing). Desde una perspectiva de gestión de riesgos, este fenómeno no solo afecta la confianza en el canal SMS, sino que también erosiona la credibilidad del sistema de identificación del remitente en su conjunto.

Por lo anterior, se aclara que, en el marco del análisis, construcción y evaluación de las alternativas regulatorias, el recurso de identificación que resulte seleccionado para soportar el servicio de SMS deberá incluir los siguientes elementos en la descripción de la propuesta regulatoria:

- Generación de criterios de asignación de recursos de identificación.
- Diseño de un esquema centralizado para la coordinación, consulta y validación del recurso de identificación.
- Reglas de gestión, modificación y revocatoria del recurso asignado.

En este sentido, esta Comisión coincide con la observación presentada en que la adopción de un código alfanumérico, así como el uso de cualquier otro recurso, exige la implementación de mecanismos de validación robustos, criterios uniformes de asignación y reglas claras de administración del recurso de identificación.

Con respecto a la observación de **ASOBANCARIA**, según la cual la diferenciación de mensajes promocionales no sería suficientemente eficaz, es importante precisar que el diseño de las alternativas regulatorias debe considerar criterios de proporcionalidad, incluyendo el efecto de señalización que cumplen los mensajes transaccionales y los costos de implementación asociados tanto a medidas aplicables a un segmento específico del tráfico como a aquellas de aplicación general. En este sentido,

será el AIN, por medio de su proceso de ponderación de los atributos que constituyen cada una de medidas, el que determine la pertinencia y conveniencia de esta medida en particular.

Respecto a las observaciones de **ASOMÓVIL** y **CLARO** en donde manifiestan que el problema central no radica en la falta de lineamientos, sino que se deriva de la reincidencia sistemática de ciertos actores, es preciso indicar que la CRC, en el marco del documento de formulación del problema[32], identificó que «las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes», lo cual dificulta «la identificación y rastreo de ataques cibernéticos». En este sentido, el enfoque vigente se encuentra orientado a un esquema reactivo que limita la identificación oportuna y el rastreo efectivo de los originadores de acciones irregulares con fines de fraude. En consecuencia, el problema no se limita a la ausencia normativa, sino a la efectividad práctica y a los incentivos asociados al esquema actual.

En este contexto, la Comisión comparte que la reincidencia constituye un elemento crítico del fenómeno, sin embargo, es preciso indicar que la reincidencia es una manifestación del problema, pero no necesariamente su causa estructural. Este fenómeno se relaciona precisamente con los elementos descritos en el documento de formulación antes citado[33], como la ausencia de trazabilidad del tráfico A2P, mecanismos insuficientes de validación previa y la adopción de procesos reforzados para la recuperación de recursos en los casos de actos previamente sancionados. En consistencia, en el documento de alternativas regulatorias se propusieron mecanismos orientados a fortalecer el régimen de recursos de identificación por medio de la adopción de herramientas técnicas, así como medidas correctivas y sancionatorias que busquen disuadir la reincidencia por parte de los distintos actores de la cadena de valor del servicio de SMS A2P.

Adicionalmente, frente a los comentarios de **ASÓMOVIL** y **CLARO** en los que se identifica como problema estructural del ecosistema A2P la indeterminación del sujeto responsable dentro de la cadena de provisión del servicio, derivada de la coexistencia de múltiples configuraciones operativas entre PCA, integradores tecnológicos (IT) y PRST; y considerando el comentario de **TIGO** en donde la expresa la existencia de una asimetría regulatoria y la necesidad de establecer obligaciones similares para todos los asignatarios del recurso de identificación para el envío de SMS; esta Comisión coincide en que la arquitectura del mercado A2P se caracteriza por una estructura de intermediación compleja.

Esta heterogeneidad operacional dificulta la identificación clara del responsable último frente a eventos de smishing, particularmente cuando existen múltiples capas de agregación, integración tecnológica o tránsito internacional del tráfico. Por esta razón, se acoge este comentario en el sentido de incluir de forma clara en la propuesta regulatoria las responsabilidades de cada uno de actores que participan en la cadena de valor del servicio de SMS A2P. Bajo este enfoque se garantiza la minimización de potenciales fricciones regulatorias y el equilibrio en la distribución de responsabilidad acorde con la función que desempeña cada agente.

Respecto a la solicitud de **CLARO** en la que propone que antes de implementar medidas como la suspensión provisional del uso de códigos cortos la Comisión (i) evalúe formalmente su efectividad y determine la existencia de un problema residual, (ii) fortalezca los procesos de recuperación ágil,

[32] CRC. Documento de Formulación del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf
[33] Ibid.

establezca reglas claras sobre reincidencia y promueva mayor articulación sectorial, y (iii) adelante un Análisis de Impacto Normativo (AIN) específico sobre la propuesta, esta Comisión considera pertinente realizar las siguientes precisiones:

En primer lugar, la suspensión provisional del uso de códigos cortos, así como los mecanismos para la identificación de agentes reincidentes y la eventual restricción del tráfico cursado por este medio, se encuentran contemplados como alternativas regulatorias dentro del documento publicado, específicamente en las secciones 7.4.1 y 7.4.3. del documento de alternativas regulatorias publicado el pasado 21 de noviembre de 2025[34]. Es importante mencionar que estas alternativas no constituyen decisiones adoptadas, sino hipótesis de solución regulatoria sujetas al enfoque de evaluación propuesto.

En segundo lugar, con relación a la solicitud de realizar el AIN sobre la propuesta, es importante recordar que si bien la mayoría de las temáticas de este proyecto regulatorio serán evaluadas mediate esta metodología, las relacionadas con la recuperación de códigos cortos y la restricción del tráfico en este servicio serán evaluadas mediante el enfoque de simplificación regulatoria. En consecuencia, la evaluación solicitada por **CLARO** no constituye un ejercicio adicional o independiente, sino que forma parte integral del proceso metodológico desarrollado en consistencia con lo expuesto previamente por esta Comisión en documento de alternativas regulatorias antes citado[35].

Frente al comentario de **HABLAME** en el que señala que la adopción de obligaciones orientadas a identificar los originadores de contenido A2P podría generar fricciones regulatorias o cuellos de botella, y en donde propone la inclusión de un identificador dentro del cuerpo del mensaje entre corchetes (por ejemplo, [EMPRESA XYZ] …), es necesario aclarar que el análisis de la CRC se basa en un enfoque integral de evaluación de alternativas regulatorias que contempla, no solo la efectividad de las medidas sino también los criterios de eficiencia, costos y simplicidad operativa de las alternativas regulatorias. En este sentido, las preocupaciones relacionadas con posibles fricciones regulatorias forman parte estructural del proceso de AIN y son evaluadas dentro de la comparación sistemática de alternativas que se presenta en la sección 9.2.1 de este documento, es decir, que los aspectos señalados por este operador hacen parte integral del proceso de evaluación descrito.

Respecto de la preocupación sobre los tiempos que podría tomar la asignación y habilitación de los códigos alfanuméricos, numeración internacional identificable o numeración no geográfica 940, la CRC reconoce que este aspecto debe ser valorado dentro del análisis de viabilidad técnica y operativa de las alternativas regulatorias. Razón por la cual, para cada alternativa evaluada se considerará la posibilidad de poder contar con procesos ágiles de asignación, así como de esquemas proporcionales según el nivel de riesgo e incorporar tiempos adecuados para cualquier transición.

Sin embargo, la necesidad de agilidad operativa no puede comprometer la efectividad de las medidas en términos de reducción de fraude. El diseño regulatorio debe equilibrar dos objetivos: preservar la dinámica competitiva del mercado A2P y, al mismo tiempo, corregir vulnerabilidades estructurales que han permitido la suplantación masiva de marcas y la pérdida de confianza del usuario en el canal. Así mismo, es importante señalar que este diseño no parte de la premisa de equivalencia entre A2P y P2P,

[34] CRC. Documento de Alternativas Regulatorias del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-alternativas-regulatorias-identificacion-medida-fraude-cibernetico-servicios-moviles.pdf
[35] Ibid.

sino del reconocimiento de que el A2P involucra intermediarios, agregadores y modelos de negocio que requieren reglas claras de asignación de responsabilidad y validación.

Frente al comentario de la **SFC** en donde señala la importancia de contar con canales de coordinación operador-usuarios masivos del canal SMS para evitar bloqueos indebidos y delimitar sujeto obligado, esta Comisión coincide en que cualquier esquema orientado a fortalecer la identificación del originador de contenido A2P, especialmente en el sector financiero, debe diseñarse bajo el principio de proporcionalidad técnica y operativa, garantizando que las medidas de mitigación del fraude no generen interrupciones indebidas en servicios críticos como notificaciones transaccionales, OTP, alertas de seguridad o comunicaciones asociadas al sistema de pagos.

Respecto a la necesidad de establecer canales de coordinación entre operadores y usuarios masivos del canal SMS, la Comisión comparte que la efectividad del esquema requiere mecanismos de interacción estructurados y oportunos que permitan la notificación de incidentes, validación del tráfico legítimo, gestión ante eventos de suplantación y protocolos claros para el desbloqueo cuando proceda. En consecuencia, se acoge su solicitud en el sentido de incorporar dentro del análisis regulatorio la conveniencia de establecer lineamientos que promuevan espacios formales de coordinación entre PRST, integradores tecnológicos y grandes usuarios del canal, particularmente entidades financieras, sin que ello implique trasladar de manera indebida obligaciones regulatorias a quienes no ostentan la calidad de agente en la cadena de valor de este servicio.

Frente al comentario realizado por **TIGO**, en el que se señala (i) la indeterminación del sujeto responsable dentro de la cadena de provisión del servicio SMS A2P, (ii) la ausencia de obligaciones diferenciadas según el rol funcional de cada asignatario de códigos cortos, (iii) el posible solapamiento entre las definiciones regulatorias de PCA e IT, y (iv) la existencia de asimetrías regulatorias derivadas de que ambos actores pueden ser asignatarios e intervenir materialmente en la cadena de envío, pero solo los PCA cuentan con obligaciones explícitas en materia de acceso e identificación, esta Comisión reconoce que la evolución tecnológica y comercial del ecosistema A2P ha dado lugar a esquemas operativos diversos en los que un mismo agente puede desempeñar funciones múltiples o híbridas dentro de la cadena de valor. Esta ambigüedad funcional genera coexistencia de múltiples configuraciones operativas que pueden dificultar la determinación del responsable efectivo ante eventos de fraude, debilitar la trazabilidad y generar vacíos de exigibilidad.

Ahora, el análisis del posible solapamiento y asimetría entre las definiciones regulatorias y distribución de obligaciones de PCA e IT resulta especialmente relevante en un entorno donde la gestión de riesgos de fraude requiere claridad en la cadena de custodia del tráfico y en los deberes de diligencia de cada participante. Por lo anterior, esta Comisión reconoce la necesidad de revisar de manera integral el marco regulatorio aplicable a los asignatarios de recursos de identificación, con el fin de:

- Evaluar la pertinencia de ajustar las definiciones vigentes para reflejar la realidad funcional del mercado.
- Analizar la conveniencia de establecer obligaciones diferenciadas según el rol que cada actor desempeñe en la cadena de provisión del servicio.
- Fortalecer los criterios de asignación de responsabilidad con base en el control efectivo del recurso y del tráfico.
- Reducir zonas grises regulatorias que puedan facilitar la dilución de responsabilidades.

En este sentido, las precisiones planteadas por el operador **TIGO** son objeto de análisis dentro del estudio de cobertura del riesgo desarrollado en la sección 9.2.4 de este documento soporte, correspondiente a la revisión del Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación regulatoria.

En cuanto a comentario relacionado con la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» realizada por este operador, es necesario señalar que la CRC coincide en que la visualización de un identificador alfanumérico asociado al remitente no constituye, por sí sola, una garantía absoluta frente a esquemas de smishing. En este sentido, la efectividad de los mecanismos de identificación del remitente se materializa cuando estos hacen parte de un esquema integral de trazabilidad y atribución del tráfico, en el cual la identificación del originador no solo cumple un propósito informativo para el usuario final, sino que también permite rastrear de manera efectiva el recorrido del mensaje a lo largo de la cadena de provisión del servicio. Por este motivo, el documento de alternativas regulatorias debe entenderse como un conjunto de medidas complementarias que contribuye a generar un ecosistema de SMS A2P seguro como resultado de un análisis de gestión del riesgo.

Así las cosas, es preciso considerar que la alternativa asociada al uso de identificadores alfanuméricos no se concibe como una medida aislada ni sustitutiva de otros mecanismos de trazabilidad, sino como un posible componente complementario dentro de un conjunto de herramientas orientadas a fortalecer la autenticidad del remitente, mejorar la confianza del usuario en el canal y facilitar labores de supervisión e investigación.

Respecto al comentario de **TIGO** en donde solicita descartar la implementación de medidas relacionadas con Sender ID alfanuméricos y priorizar esquemas basados en la atribución única de códigos cortos por marca, la Comisión reconoce que los mecanismos de asignación exclusiva pueden ofrecer ventajas en términos de claridad de responsabilidades y trazabilidad del asignatario del recurso. Sin embargo, la idoneidad de esta alternativa debe evaluarse en el marco del proceso de AIN, valorando su efectividad, viabilidad técnica, costos, proporcionalidad e impacto sobre el mercado.

Por último, en relación con el comentario de **TIGO**, en donde manifiesta que los esquemas de trazabilidad deben centrarse en la atribución única del recurso por marca, es importante señalar que la valoración de esta alternativa debe ser el resultado del proceso de evaluación objetivo en el marco del AIN que se plantea en el presente documento soporte. Esto con el propósito de considerar los diferentes elementos identificados como resultado del aporte del sector, así como la proporcionalidad de las cargas en los diferentes segmentos del mercado y su balance con otros atributos como eficiencia y efectividad de cada alternativa.

8.2.3.3 Subtemática 2: Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude

ALDEAMO

Cuestiona el tratamiento regulatorio actual de los códigos cortos, señalando que no deben considerarse como un recurso escaso. Argumenta que la percepción de escasez obedece principalmente a restricciones normativas históricas, como límites en el dígito inicial y la longitud, que

hoy podrían revisarse para ampliar la disponibilidad. Sostiene que existen numerosos códigos cortos sin utilizar o ya recuperados, lo que evidencia que el sistema regulatorio vigente no está siendo efectivo para combatir el fraude, a pesar de los recursos dedicados por instituciones y privados.

Señala que el esquema regulatorio actual presenta fallas estructurales que afectan su eficacia y generan incentivos negativos. Expone que, por un lado, existen empresas víctimas de fraude que no se registran ni gestionan códigos cortos por desconocimiento o desconfianza en el proceso, y por otro, integradores adquieren códigos que luego ceden a terceros. En este sentido, critica que la principal medida de intervención actualmente sea la recuperación de códigos cortos, la cual considera ineficaz frente al incremento del fraude. Por ello, propone replantear el modelo, eliminando mecanismos poco efectivos y redirigiendo los esfuerzos institucionales hacia acciones con mayor capacidad de contención real.

En cuanto a la alternativa de «proceso de validación centralizado de originadores de contenido», la identifica como su preferida, y respalda especialmente la medida de KYC obligatorio para agregadores, pero condicionando su éxito a precisiones de diseño y alcance. De un lado, propone que los estándares de KYC se definan mediante un grupo de trabajo con participación de las partes interesadas, con el fin de evitar procedimientos excesivamente largos que terminen haciendo inviable la vinculación de nuevos clientes. De otro lado, insiste en que los estándares deben extenderse obligatoriamente a otros actores que, en la práctica, pueden operar como eslabones de originación del tráfico (operadores que incluyen SMS dentro de soluciones, empresas de cobranza, BPOs y, en general, cualquier entidad que envíe mensajes a nombre de terceros), para impedir que se generen vacíos aguas abajo en la cadena de valor.

Recomienda que la CRC sea el ente encargado de la validación centralizada, debido a su experiencia en la gestión de códigos cortos. Considera que sería más efectivo ajustar el sistema actual que designar un tercero, ya que esto generaría dudas sobre gobernanza y financiamiento. Además, advierte que una implementación incorrecta podría aumentar las cargas operativas para los actores involucrados, por lo que sugiere crear una mesa técnica para definir un procedimiento eficiente y equitativo.

Finalmente, hace observaciones específicas sobre las medidas de intervención en tráfico y transparencia hacia el usuario. Sobre la medida de bloqueo o marcado por PRSTM de tráfico no autorizado, considera que sería innecesaria si se habilita el uso de Sender ID alfanumérico y se ejecutan campañas masivas de educación que permitan a los usuarios reconocer remitentes oficiales, sin embargo, señala que podría considerase un esquema focalizado de etiquetado («sin verificar») para tráfico originado por call centers, BPOs, cobranzas o empresas internacionales que no acrediten el KYC.

Sobre la medida de categorización del contenido y consentimiento, articulada con RNE, la valora positivamente, pero pide profundizarla mediante un grupo interinstitucional que defina guías claras de clasificación. Y respecto de la medida de reglas de monitoreo por agregadores, la respalda en términos generales, aunque insiste en que el monitoreo no debe recaer en el eslabón más débil que son los agregadores, por lo que propone que los operadores, las empresas de cobranzas, los BPOs, los call centers y los actores internacionales también contribuyan a ese monitoreo, y, en paralelo, cuestiona la viabilidad financiera de las medidas propuestas en un entorno de precios regulados, por lo que sugiere explorar medidas diferenciales sobre precios, distinguiendo el envío de aquellos mensajes sobre los que se deban aplicar acciones de monitoreo de aquellos sobre los que no.

ANDESCO

Frente a esta temática, y en general, sobre la gestión de originadores en el ecosistema, **ANDESCO** pide que cualquier esquema que implique señalización o etiquetado de comunicaciones (por ejemplo, advertencias al usuario sobre posible fraude o estados de verificación) se soporte en parámetros técnicos objetivos, taxativos y estandarizados, para reducir el riesgo de falsos positivos y afectaciones a comunicaciones legítimas, especialmente de usuarios corporativos.

Complementariamente, **ANDESCO** reitera que, si la problemática se concentra en actores específicos del ecosistema (PCA/IT), el diseño regulatorio debe evitar que la solución «ponga en cintura» a un agente particular a costa de imponer obligaciones generales al conjunto de PRST y agregadores que sí cumplen, y sugiere focalizar esfuerzos en controles y gestión del recurso de identificación vinculados al tráfico SMS.

ASOBANCARIA

Apoya un enfoque integral: trazabilidad extremo a extremo (agregador-marca-campaña-plantilla), KYC robusto, monitoreo y bloqueo dinámico con SLAs, e incorporación de controles técnicos preventivos (incluyendo protección frente a vulnerabilidades de señalización). Pide reglas homogéneas y mecanismos de excepción/revisión para minimizar falsos positivos y no afectar mensajes críticos (OTP/alertas).

Considera necesario definir de manera clara los procesos de conocimiento del cliente (KYC, por sus siglas en inglés) aplicables para mitigar riesgos de suplantación y uso de estructuras fraudulentas, así como establecer reglas y penalizaciones en caso de participación en el envío de SMS fraudulentos. Adicionalmente, considera pertinente promover mecanismos de intercambio oportuno de información entre los actores afectados, que permitan la actualización continua de las reglas de monitoreo. En este mismo sentido, indica que es necesario definir niveles de servicio exigibles a los agregadores en materia de alertas de fraude y los tiempos de reacción esperados para el bloqueo o etiquetado de SMS fraudulentos

Al respecto, **ASOBANCARIA** identifica como un reto la necesidad de calibrar adecuadamente los sistemas de etiquetado y alerta, de manera que se minimicen los falsos positivos que puedan afectar la experiencia del usuario y la confianza en los canales de las entidades financieras. En este punto, dice **ASOBANCARIA**, resulta relevante otorgar claridad normativa respecto de que la obligación asociada a la implementación, operación y ajuste de dichos sistemas recae en los operadores de servicios móviles. En concreto, **ASOBANCARIA** considera que es necesario que la regulación contemple mecanismos expeditos de reclasificación, revisión y apelación frente a eventuales bloqueos o marcaciones erróneas de comunicaciones legítimas, así como una delimitación clara de responsabilidades entre los distintos actores de la cadena de valor. En este sentido, **ASOBANCARIA** sugiere que se definan criterios claros y homogéneos para el etiquetado de las comunicaciones, tales como las categorías de «No verificada» o «Probable fraude», asegurando que se minimicen los falsos positivos, que las alertas sean comprensibles para el usuario final y que los criterios de clasificación se encuentren homologados para todos los sectores impactados.

Sugiere que se debe exigir la autenticación del origen de los mensajes mediante mecanismos criptográficos o protocolos seguros, el filtrado y monitoreo activo del tráfico para identificar patrones anómalos como picos de envío, ráfagas de mensajes o rutas internacionales no verificadas, así como

la implementación de firewalls de señalización y el endurecimiento de protocolos para prevenir la explotación de vulnerabilidades como el SS7 Hacking. Estas medidas deberían complementarse con el bloqueo dinámico de comunicaciones clasificadas como no verificadas o de probable fraude, acompañado de procesos de revisión, trazabilidad y gestión de excepciones.

Considera necesario proteger comunicaciones sensibles mediante listas blancas de dominios de pago, deeplinks firmados, el uso exclusivo de mensajería in-app para operaciones críticas y la migración progresiva hacia soluciones que permitan el cifrado de extremo a extremo del contenido, con el fin de evitar la interceptación del mensaje en claro y proteger la confidencialidad de la información. Todas estas medidas deberían ser obligatorias, auditables y estar acompañadas de métricas de efectividad y niveles de servicio regulatorios que garanticen la resiliencia del canal SMS frente a ataques y fraudes, así como complementarse con la obligatoriedad para los operadores de implementar esquemas de monitoreo del tráfico P2P y mecanismos de reacción frente a los alertamientos generados.

SFC

Para la SFC, resulta prioritario que la implementación de esta medida contemple la adopción de esquemas de identificación verificada para el sector financiero, teniendo en cuenta que los mensajes de texto constituyen uno de los principales canales para el envío de OTP y notificaciones transaccionales.

En este sentido, un régimen de identificación robusto contribuiría a reducir los riesgos de redirección de los usuarios a sitios web fraudulentos, derivados de técnicas de smishing que suplantan la identidad de entidades financieras. Adicionalmente, considera relevante que, en el diseño de la medida, se incorporen mecanismos que permitan mitigar el riesgo de afectación al tráfico legítimo de las entidades financieras, de forma que no se impacte la continuidad y operatividad del sistema de pagos.

PTC

Frente a la trazabilidad A2P, **PTC** se inclina por una solución integral basada en recursos exclusivos de identificación (códigos cortos o numeración E.164) para marcas, por estimar que ello mejora simultáneamente la trazabilidad y la prevención del fraude. **PTC** señala que, desde el punto de vista técnico, la exclusividad permitiría identificar con claridad al originador, habilitando monitoreo más preciso y controles preventivos basados en patrones de uso. Además, ese operador sugiere incorporar medidas complementarias como categorización del contenido, consentimiento del usuario y KYC obligatorio para agregadores, buscando control a lo largo de la cadena. También plantea que esta aproximación debe articularse con registros existentes como el RNE, para evitar duplicidades y promover coherencia. En lo operativo, **PTC** estima un plazo de un año contado desde que se asigne y habilite el NDC 940, y recomienda una implementación por etapas priorizando inicialmente a las marcas con mayor volumen de tráfico A2P.

En línea con lo anterior, **PTC** desarrolla recomendaciones específicas sobre gobernanza del ecosistema A2P. Así, propone que los integradores/agregadores se clasifiquen bajo un sistema de reputación definido por la CRC, que permita consultar su confiabilidad según desempeño en detección y gestión de fraude. Añade que el proceso debe ser digital, soportado documentalmente, con vigencia temporal definida y aplicable tanto a integradores nacionales como internacionales. Asimismo, considera pertinente que exista un proceso (centralizado o distribuido) de validación que permita a la CRC conocer públicamente a los agregadores y establecer condiciones de confianza basadas en medición

de comportamiento. Estas ideas refuerzan su insistencia en que las medidas antifraude deben asignar responsabilidades y exigencias verificables a todos los actores de la cadena.

HABLAME

En relación con controles y trazabilidad, **HABLAME** sostiene que la regulación debe observar estrictamente la proporcionalidad, afirmando –con base en sus monitoreos y filtros– que el tráfico fraudulento representaría menos del 2% del total de SMS cursados, por lo cual medidas estructurales podrían poner en riesgo el 98% de tráfico legítimo y habilitar dinámicas de bloqueo masivo injustificado. En esta línea, insiste en que aproximaciones amplias o imprecisas pueden impactar negativamente el tráfico legítimo, deteriorar competitividad e introducir barreras artificiales de entrada.

Un eje central de su comentario es la oposición a habilitar, directa o indirectamente, que los operadores móviles determinen, bloqueen o filtren contenidos con base en criterios propios o reportes aislados de usuarios. **HABLAME** reporta incidentes de bloqueo de mensajes legítimos (p. ej., OTP bancarios, notificaciones médicas o educativas) y plantea que ello comprometería derechos como información, salud, educación y libre comunicación. Adicionalmente, advierte riesgos para neutralidad de red, competencia y eventuales abusos de posición dominante. Ilustra lo anterior con un caso en el que una campaña comercial legítima fue bloqueada por reporte individual, y concluye que la determinación de si un contenido es fraudulento debe recaer en un juez o autoridad competente con capacidades periciales, no en decisiones privadas discrecionales.

Como alternativa, **HABLAME** propone fortalecer un esquema de decisión centralizada e imparcial a través de COLCERT, que actuaría como autoridad técnica y articuladora (en coordinación con MinTIC y Policía), administrando un portal público de consulta, recepción de reportes, análisis técnico-jurídico, y una base de datos nacional en tiempo real de patrones (URLs, frases, fragmentos) para habilitar bloqueos automáticos inmediatos a nivel nacional, con el propósito de evitar sesgos y discrecionalidad.

Además, manifiesta estar de acuerdo con esquemas KYC/KYB, pero solicita que se reconozcan riesgos de suplantación documental y la buena fe del integrador cuando también resulta víctima del engaño. Finalmente, ratifica una propuesta técnica previa: exigir que la transmisión de SMS entre integradores tecnológicos y PRST se realice por canales punto a punto no expuestos a Internet (p. ej., enlaces dedicados o MPLS), como estándar de seguridad.

TIGO

Manifestó que las alternativas orientadas a garantizar la asignación de un identificador único por marca, ya sea a través de códigos alfanuméricos (Sender ID), códigos cortos o numeración E.164 exclusiva, tienen un potencial significativamente mayor para contener el fraude, en la medida en que fortalecen la atribución del tráfico, facilitan la trazabilidad de las campañas y reducen la posibilidad de suplantación del originador.

TIGO resaltó que la efectividad de estas medidas se incrementa cuando se complementan con obligaciones de debida diligencia (KYC) sobre las marcas y clientes, así como con la posibilidad de bloquear o restringir tráfico no verificado o que no cumpla requisitos mínimos de autenticidad. No obstante, el operador señaló que dentro de esta temática se incluye una medida relacionada con la categorización del contenido y el consentimiento del usuario, articulada con el Registro de Números

Excluidos (RNE), la cual, a su juicio, no guarda una relación directa con la prevención del fraude cibernético en su modalidad de smishing.

Sobre este punto, **TIGO** advirtió que la incorporación de nuevas obligaciones en materia de consentimiento y categorización podría implicar cargas operativas y costos relevantes, sin un impacto proporcional en la reducción del fraude. Adicionalmente, recordó que dichas materias fueron objeto de ajustes regulatorios recientes a través de la Resolución CRC 7356 de 2024, expedida en desarrollo de la Ley 2300 de 2023, por lo que introducir nuevas exigencias podría generar solapamientos normativos y exceder el alcance del proyecto regulatorio.

Frente a la Alternativa 1 (statu quo), **TIGO** consideró que mantener el esquema actual resulta insuficiente para abordar la problemática identificada, razón por la cual estimó necesario descartar esta opción.

Respecto de la Alternativa 2 (proceso de validación centralizado de originadores de contenido), el operador señaló que, para su adecuada implementación, es indispensable precisar previamente la definición y el alcance regulatorio de la figura de «agregador». En ese sentido, sostuvo que las obligaciones asociadas a la validación deben recaer expresamente sobre los asignatarios de códigos cortos, es decir, los PCA y los IT. **TIGO** reconoció que un esquema de validación centralizada podría contribuir a mejorar la trazabilidad y permitir una gestión preventiva del fraude. Sin embargo, enfatizó la necesidad de definir claramente la asignación de responsabilidades y costos, señalando que estos no deberían trasladarse a los PRST, cuyo rol se limita al transporte y terminación del tráfico. Además, realiza una distribución de responsabilidades en la que sugiere que:

- La Comisión, en calidad de Administradores de los Recursos de Identificación, este a cargo del seguimiento y control de las actividades que el validador este ejecutando.

- La CRC precise expresamente la asignación de responsabilidades sobre los costos de implementación, operación y soporte del proveedor que centralice dicha validación. En particular, indica que estos costos deberían ser asumidos por los asignatarios de los códigos cortos (PCA e IT), quienes se benefician directamente del uso del recurso y controlan la relación con la marca/campaña y en ningún caso deberían trasladarse a los PRST, que actúan como red de transporte y terminación del tráfico y que no controlan el origen comercial del mensaje.

- En lo respectivo a los PRST, su carga debería limitarse a los costos estrictamente asociados a la implementación técnica de los mecanismos necesarios para: (i) consultar o verificar el «paquete» de identificadores válidos; y (ii) ejecutar la suspensión temporal del tráfico que no incorpore dicha validación.

- El bloqueo debería realizarse en el origen de la cadena, es decir, por parte del agregador, PCA o IT, quienes deben asumir la responsabilidad por la filtración articulada y preventiva. Permitir que el PRST se convierta en el punto primario de contención incrementa cargas de trafico de red innecesarias

Considera necesario que la Comisión acompañe estas alternativas con un análisis costo–beneficio que evalúe su pertinencia, proporcionalidad y viabilidad, incluyendo costos de implementación y operación comparadas frente a las demás alternativas.

Asimismo, manifestó inquietudes sobre el esquema de supervisión del validador y los riesgos asociados a posibles manipulaciones o suplantaciones del proceso de validación, y sostuvo que el bloqueo del tráfico no validado debería realizarse preferiblemente en el origen de la cadena.

En cuanto a la Alternativa 3 (proceso de validación distribuido mediante tecnologías DLT), **TIGO** reconoció que este tipo de esquemas podría ofrecer ventajas en términos de integridad, inmutabilidad y trazabilidad de la información. No obstante, consideró indispensable que la CRC adelante un análisis costo–beneficio que evalúe su viabilidad regulatoria y operativa, teniendo en cuenta la complejidad de su gobernanza, los costos de implementación y operación, así como los impactos en tiempos de procesamiento e interoperabilidad entre actores.

Finalmente, frente a la Alternativa 4 (identificación exclusiva mediante códigos cortos, numeración E.164 o códigos alfanuméricos), **TIGO** manifestó que esta constituye la opción más adecuada para abordar la problemática de trazabilidad y prevención del fraude. El operador destacó que la asignación de un identificador único por marca permite rastrear de manera clara las campañas, facilita la identificación de responsables ante incidentes y reduce la dependencia de validadores externos, lo que se traduce en menores costos de implementación y operación, así como en una mayor agilidad para el despliegue de campañas legítimas. Adicionalmente, señaló que este esquema puede complementarse con procesos de KYC a cargo de los agregadores y con la facultad de los PRST para restringir o suspender tráfico ante indicios objetivos de fraude, siempre que existan criterios claros y verificables definidos por la Comisión y mecanismos de reacción ante reportes de los usuarios.

ASOMÓVIL

El gremio considera que fortalecer la identificación del remitente es un elemento necesario para mejorar la trazabilidad y reducir el smishing, siempre que dicha identificación esté acompañada de controles efectivos en el origen del tráfico. No obstante, enfatiza que la responsabilidad por la identificación clara y correcta del remitente debe recaer sobre los PCA e IT, quienes gestionan la relación comercial con las marcas y campañas, y no sobre los PRST, cuya función se limita al transporte del tráfico.

CLARO

Manifestó que las debilidades identificadas no obedecen a la inexistencia de herramientas regulatorias o técnicas, sino a la aplicación insuficiente y tardía de los mecanismos ya disponibles, en particular aquellos relacionados con la administración y control de los recursos de identificación.

Sostuvo que mantener el statu quo no resulta problemático en sí mismo, en la medida en que la regulación vigente ya asigna responsabilidades claras dentro de la cadena A2P, identifica al PCA o IT como el originador del contenido y faculta a los PRST para adelantar acciones de bloqueo en escenarios de fraude. En ese sentido, señaló que el operador actúa como transportador del tráfico, sin capacidad ni facultad para validar o intervenir el contenido de los mensajes, en consonancia con el principio de neutralidad de red y con lo dispuesto en la normativa sectorial.

Frente a la alternativa de establecer un proceso de validación centralizado de originadores de contenido, **CLARO** consideró que esta medida resulta innecesaria y desproporcionada, al pretender imponerse de manera generalizada a todos los actores del ecosistema cuando, según su experiencia

operativa, los incumplimientos se concentran en casos puntuales de PCA o IT reincidentes. Adicionalmente, indicó que esta alternativa desconoce el rol definido del PRST en la cadena A2P, introduce riesgos legales asociados a la posible intervención del contenido de los mensajes y enfrenta limitaciones técnicas relevantes, dada la imposibilidad de validar en tiempo real grandes volúmenes de tráfico sin afectar la calidad del servicio.

En la misma línea, **CLARO** manifestó que la alternativa de validación distribuida mediante tecnologías DLT tampoco resulta viable ni necesaria, en tanto reproduce las mismas dificultades jurídicas, técnicas, operativas y económicas del esquema centralizado, añadiendo además complejidades de gobernanza, altos costos de implementación y largos plazos de despliegue que no se compadecen con la naturaleza dinámica del fraude.

Respecto de la alternativa de identificación exclusiva mediante códigos cortos o numeración E.164, **CLARO** reconoció que la asignación de identificadores exclusivos por marca puede contribuir a mejorar la identificación del remitente y facilitar la atribución de responsabilidades en caso de fraude. No obstante, enfatizó que el control de dichos identificadores debe recaer en el agregador u originador del contenido, evitando configuraciones que permitan la generación de identificadores confusos o susceptibles de inducir a error a los usuarios. En todo caso, reiteró que esta medida no debe implicar cargas adicionales para los PRST ni desplazar responsabilidades hacia estos que corresponden al PCA y/o IT.

De manera transversal, **CLARO** insistió en que la medida más efectiva para la mitigación del fraude A2P ha sido la suspensión provisional de códigos cortos al inicio de las actuaciones administrativas, aplicada recientemente por la CRC, la cual, según su experiencia, produjo una reducción sustancial de los casos de fraude reportados. En consecuencia, el operador consideró que antes de introducir nuevas obligaciones tecnológicas o esquemas de validación complejos, resulta indispensable consolidar y fortalecer este tipo de medidas focalizadas, permitir la terminación de contratos con PCA o IT reincidentes, y evaluar cualquier intervención adicional a través de un Análisis de Impacto Normativo (AIN) que garantice proporcionalidad, necesidad y sostenibilidad económica.

TELEFÓNICA

Identifica como principal debilidad estructural la pérdida de trazabilidad del tráfico A2P, especialmente en esquemas con múltiples intermediarios y rutas internacionales. Señala que el anonimato del originador facilita el smishing y limita la imputación de responsabilidades.

Frente a las alternativas planteadas, apoya el fortalecimiento de la trazabilidad desde el origen, pero rechaza que los PRST asuman funciones de auditoría del contenido o de validación comercial, por ser técnica y jurídicamente ineficiente. Considera indispensable que las obligaciones de KYC/KYB y validación recaigan directamente sobre agregadores y PCA, quienes mantienen la relación comercial con el originador del tráfico. En su opinión, para asegurar el éxito de la iniciativa de KYC, **TELEFÓNICA** considera que es indispensable resolver previamente inquietudes operativas clave relacionadas con la disponibilidad, latencia y seguridad de la información en dicha plataforma central. Para este operador, el modelo debe diseñarse de tal forma que garantice agilidad en la consulta para no afectar el tráfico legítimo, y debe articularse estrictamente con el reordenamiento de los recursos de numeración (Sender ID únicos), asegurando que la validación administrativa se traduzca efectivamente en una limpieza técnica del ecosistema.

Asimismo, advierte que tecnologías complejas (p. ej. DLT o blockchain) deben ser evaluadas estrictamente bajo AIN, dado el riesgo de costos desproporcionados frente a la estructura económica del servicio SMS.

Respuesta de la CRC:

Frente a esta temática, **ASOBANCARIA, PTC, TELEFÓNICA, TIGO, ASOMÓVIL, CLARO** y la **SFC** señalaron que el ecosistema A2P presenta una pérdida estructural de trazabilidad extremo a extremo, particularmente en esquemas con múltiples intermediarios, lo cual dificulta identificar al responsable del contenido y favorece la reincidencia del fraude. Este señalamiento coincide plenamente con la intención original de la CRC al formular las alternativas regulatorias de esta temática, las cuales parten del reconocimiento de que el marco vigente no permite una atribución efectiva de responsabilidades teniendo en cuenta la imposibilidad de reconocer el origen del tráfico A2P.

De manera complementaria, **ASOBANCARIA, la SFC, CLARO, TELEFÓNICA** y **TIGO** indicaron que la falta de trazabilidad no solo dificulta la investigación de eventos de fraude, sino que reduce los incentivos al cumplimiento normativo y facilita la reincidencia por parte de actores maliciosos. La CRC reconoce que este efecto es consistente con el enfoque preventivo que se busca fortalecer mediante las alternativas regulatorias propuestas, particularmente aquellas relacionadas con el régimen de administración de recursos de identificación. No obstante, la reincidencia se entiende como una manifestación del problema y no como su causa estructural, por lo que este argumento se acoge como criterio relevante para evaluar la eficacia disuasiva de las alternativas asociadas a la revisión del régimen de administración de recursos de identificación bajo el enfoque de simplificación.

Por su parte, **CLARO, ASOMÓVIL** y **TELEFÓNICA** sostuvieron que el problema no radica en la ausencia de regulación, sino en la dificultad práctica para atribuir responsabilidades de manera verificable. Este planteamiento es coherente con la intención de la CRC de evitar intervenciones meramente declarativas y concentrarse en alternativas que puedan causar efectos operativos reales en cuanto a la prevención del fraude. En consecuencia, el argumento se acoge como un criterio transversal de evaluación, que orienta el análisis comparativo.

En relación con la asignación de responsabilidades, **CLARO, TELEFÓNICA, HABLAME, TIGO** y **ANDESCO** advirtieron que no debe trasladarse a los PRST la validación, auditoría o calificación del contenido de los mensajes A2P. La CRC comparte este señalamiento, dado que desde el diseño de las alternativas se ha buscado preservar la separación de roles en la cadena de valor y evitar asignar a los PRST funciones cuasi-judiciales o de control comercial. En ese sentido, este argumento no solo se acoge, sino que establece un lineamiento para la evaluación de las alternativas y la estructuración de la propuesta regulatoria.

En la misma línea, **TIGO, TELEFÓNICA, CLARO** y **ASOMÓVIL** insistieron en la necesidad de preservar la separación de roles dentro de la cadena A2P, asignando las responsabilidades al eslabón que mantiene la relación comercial con la marca. En concordancia con lo indicado frente al argumento anterior, este argumento es plenamente consistente con la intención regulatoria de la CRC, por lo que este se acoge y en consecuencia condiciona la evaluación de las alternativas a dicho criterio.

Adicionalmente, **HABLAME, CLARO, TELEFÓNICA** y **ANDESCO** advirtieron que permitir decisiones discrecionales de bloqueo o calificación del contenido por parte de los PRST podría afectar la neutralidad de red, el debido proceso y la libre competencia. La CRC considera que este argumento

refuerza la necesidad de que cualquier alternativa que contemple mecanismos de reacción frente al fraude esté basada en criterios técnicos objetivos y procedimientos verificables. En consecuencia, el argumento se acoge y se tendrá en cuenta al momento de la evaluación y de la estructuración de la propuesta regulatoria, excluyendo así esquemas discrecionales en su diseño.

Existe un consenso amplio entre **PTC, TIGO, CLARO, ASOMÓVIL, TELEFÓNICA**, **ASOBANCARIA** y la **SFC** en que la asignación de identificadores exclusivos por marca puede mejorar significativamente la trazabilidad y reducir la suplantación. Este argumento se alinea directamente con la intención de la CRC al incluir esta alternativa dentro del conjunto a evaluar. Desde el análisis preliminar, la CRC considera que este señalamiento refuerza la pertinencia de la alternativa y en consecuencia se mantiene para su correspondiente evaluación en la forma presentada.

No obstante, **PTC, TIGO, CLARO, TELEFÓNICA, ASOMÓVIL** y **HABLAME** señalaron que el control y la administración de dichos identificadores deben recaer sobre los PCA o integradores tecnológicos. La CRC insisten en que uno de los objetivos de las alternativas es reforzar la atribución de responsabilidades en el origen del tráfico. Este argumento es valioso y se tendrá en cuenta al momento de definir el alcance de la alternativa.

Por otro lado, **HABLAME** y **TELEFÓNICA** advirtieron que los identificadores exclusivos podrían generar una falsa sensación de legitimidad ante los usuarios si no se acompañan de procesos de validación robustos. Al respecto, la CRC considera que este riesgo es relevante, pero no suficiente para descartar la alternativa. Por lo tanto, el argumento se acoge como advertencia y la alternativa se mantiene, mitigando este riesgo en la especificación del proceso de validación de los clientes mediante el KYC para su evaluación posterior.

Asimismo, **ASOMÓVIL, CLARO, TELEFÓNICA** y **ANDESCO** señalaron que la implementación de identificadores exclusivos debe observar criterios de gradualidad y proporcionalidad. La CRC acoge este argumento por ser consistente con su intención de evitar cargas regulatorias excesivas. En consecuencia, la alternativa se mantiene, con la consideración de posibles ajustes de diseño e implementación que serán plasmados en la alternativa definitiva y evaluados más adelante.

En relación con los esquemas de KYC/KYB, **ASOBANCARIA, PTC, TIGO, TELEFÓNICA**, **ALDEAMO** y la **SFC** resaltaron su importancia para reducir el anonimato en el origen del tráfico. La CRC reconoce que este argumento apoya el enfoque preventivo de las alternativas planteadas, aunque se resalta también que estos mecanismos no son autosuficientes y se contemplaron desde un inicio para que actuaran como complemento de una estrategia integral que permitiera mejorar la trazabilidad de la originación del contenido en las comunicaciones A2P. Por ello, el argumento se acoge y conduce naturalmente a mantener la alternativa como medida complementaria, sujeta a evaluación sistémica más adelante.

De manera complementaria, **TELEFÓNICA, TIGO, CLARO** y **ASOMÓVIL** indicaron que las obligaciones de KYC deben recaer sobre los PCA e integradores tecnológicos. La CRC comparte este planteamiento, e indica que de ese modo quedó plasmado en el documento de formulación de alternativas regulatorias. En ese sentido, el argumento se acoge y conduce corroborar la línea ya dada al respecto en la formulación de la alternativa definitiva.

Por su parte, **HABLAME** y **ALDEAMO** advirtieron que esquemas de KYC excesivamente exigentes podrían generar barreras de entrada al mercado. Al respecto, si bien la CRC y la industria consideran

en su mayoría que estos esquemas de validación de los originadores introducen controles necesarios para garantizar la trazabilidad de los contenidos, este riesgo que se pone de presente debe ser tenido en cuenta a la hora de la evaluación y de la estructuración de la propuesta regulatoria. Por lo anterior, el argumento se acoge como advertencia, pero no conduce a modificar la alternativa, la cual se mantiene en la forma presentada para evaluación.

En esa misma línea, **HABLAME, ALDEAMO** y **TELEFÓNICA** señalaron que incluso con KYC pueden presentarse escenarios de fraude por suplantación o mala fe. La CRC coincide con este análisis cuando se realiza de manera aislada, sin embargo, resulta importante considerar que las alternativas regulatorias para esta temática se plantearon de manera sistémica contemplando varias medidas en forma de paquete articulado, y en ese sentido el comentario refuerza la idea de evaluar combinaciones de medidas y no medidas aisladas.

Respecto a los modelos de validación centralizada o distribuida, **PTC, ALDEAMO** y **HABLAME** manifestaron interés en su adopción como mecanismo para mejorar la trazabilidad. En contraste, **CLARO, TELEFÓNICA, TIGO** y **ANDESCO** advirtieron sobre los riesgos de costos, latencias operativas y concentración de funciones asociados a estos esquemas y señalaron que estos esquemas no deben adoptarse sin un Análisis de Impacto Normativo. Al respecto, la CRC acoge el argumento de los costos y las latencias operativas como un elemento significativo, lo cual eleva el umbral de justificación de esta alternativa a la hora de la evaluación de las implicaciones de los mismos en las dinámicas del mercado en el marco del AIN que se detalla más adelante en el presente documento.

Existe un consenso transversal entre **ASOBANCARIA, ANDESCO, la SFC, TIGO, CLARO, TELEFÓNICA** y **HABLAME** sobre la necesidad de contar con mecanismos de reacción frente al fraude como el bloqueo de mensajes identificados como fraude en el proceso de monitoreo. No obstante, **HABLAME, TELEFÓNICA, ASOBANCARIA** y la **SFC** advirtieron sobre el riesgo de falsos positivos derivados de bloqueos discrecionales. Asimismo, **HABLAME, TELEFÓNICA, CLARO** y **ANDESCO** propusieron que los bloqueos se basen en criterios técnicos objetivos y estandarizados. Al respecto, la CRC comparte la inquietud planteada frente a la necesidad de generar reglas claras para que el monitoreo, bloqueo y marcado de mensajes se hagan bajo criterios técnicos objetivos y estandarizados, incluyendo elementos que permitan evitar los falsos positivos y el diseño de mecanismos que permitan abordar ese tipo de situaciones cuando se presenten. En ese sentido, se harán las aclaraciones correspondientes en la descripción de la alternativa definitiva para su posterior evaluación en el marco del AIN.

En relación con la protección de tráfico crítico, ASOBANCARIA, la SFC, TELEFÓNICA y HABLAME destacaron la necesidad de proteger los mensajes OTP, las alertas financieras y los mensajes sensibles. La CRC considera este argumento plenamente consistente con su intención regulatoria y lo acoge como criterio transversal para la evaluación de las alternativas y el diseño de la propuesta regulatoria.

Por su parte, CLARO y TIGO señalaron que la suspensión provisional de recursos de identificación ha sido una herramienta eficaz y que antes de introducir nuevas obligaciones tecnológicas o esquemas de validación complejos, resulta indispensable consolidar y fortalecer este tipo de medidas focalizadas, permitir la terminación de contratos con PCA o IT reincidentes, y evaluar cualquier intervención adicional a través de un Análisis de Impacto Normativo (AIN) que garantice proporcionalidad, necesidad y sostenibilidad económica. Al respecto, es necesario mencionar que, si bien la CRC ha venido diseñando e implementando mecanismos como la recuperación de códigos cortos y la suspensión de tráfico a fin de poder mitigar el fraude, dichos mecanismos corresponden a medidas

reactivas dado que al momento de la suspensión del tráfico o la recuperación del recurso de identificación los usuarios ya han sido víctimas de las comunicaciones generadas con fines fraudulentos.

En ese sentido, aunque en el eje temático de este proyecto enfocado en la revisión del régimen de administración de recursos de identificación se abordan algunos elementos enfocados en favorecer y reforzar este tipo que mecanismos reactivos complementarios, es necesario resaltar la necesidad actual de ahondar en el desarrollo de herramientas que permitan prevenir el contacto a usuarios con fines fraudulentos, y de esa manera comenzar a recuperar de nuevo la confianza de estos en las comunicaciones remitidas mediante SMS.

Finalmente, PTC, TIGO, ASOBANCARIA y la SFC insistieron en la necesidad de evitar duplicidades con instrumentos regulatorios existentes, refiriéndose expresamente a la articulación con el RNE. Al respecto, la CRC entiende y comparte que la implementación de las últimas modificaciones del RNE a raíz de la Resolución CRC 7356 de 2024, expedida en desarrollo de la Ley 2300 de 2023, son recientes y que la incorporación de nuevas obligaciones en materia de consentimiento y categorización podría implicar cargas operativas y costos adicionales, sin un impacto directo en la reducción del fraude.

En este orden de ideas, en la eventual recategorización de los contenidos asociados a comunicaciones A2P se tendrá como lineamiento de diseño de la propuesta regulatoria el no afectar las últimas implementaciones de este mecanismo.

Por su parte, **TELEFÓNICA, CLARO** y **TIGO** reiteraron la necesidad de diferenciar el tratamiento del tráfico A2P y P2P. Al respecto, la CRC acoge plenamente el argumento y en concordancia con ello desarrolla un análisis del mercado de SMS, en la segunda fase del presente proyecto regulatorio, en donde se reconocen los segmentos de mensajes cortos de texto P2P y A2P con las implicaciones de mercado que eso conlleva.

En cuanto a la proporcionalidad, **HABLAME, CLARO, TELEFÓNICA, ALDEAMO** y **ANDESCO** enfatizaron la necesidad de costo-eficiencia para considerar las alternativas. La CRC acoge este argumento como principio rector del proceso de evaluación de las alternativas planteadas, y confirma que ninguna será adoptada sin una evaluación integral posterior, manteniéndose así todas las alternativas planteadas inicialmente para esta temática, con las variaciones y adiciones indicadas anteriormente, como objeto de análisis en las secciones siguientes del presente documento.

8.2.3.4 Subtemática 3: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

ALDEAMO

Considera que existen diferentes herramientas en el mercado para controlar los mensajes SMS P2P que han sido implementadas por muchos operadores en varios países. Señala que la razón principal por la que no se ha implementado en Colombia es el costo. Así mismo, propone que se elimine la regulación que controla el precio de los mensajes de texto, para que se generen los recursos necesarios para esta implementación.

CLARO

Reconoce que el tráfico SMS P2P puede ser utilizado con fines fraudulentos, particularmente mediante el abuso de planes ilimitados. En este sentido, considera viable la implementación de controles de patrones atípicos, aun cuando reconoce que estos pueden generar un margen reducido de error que eventualmente afecte mensajes legítimos.

No obstante, se opone de manera expresa a la imposición regulatoria de límites máximos de SMS P2P por usuario, al considerar que esta medida es técnica y jurídicamente desproporcionada, vulnera principios de neutralidad tecnológica, intervención mínima y protección de los derechos de los usuarios, y genera costos operativos elevados sin evidencia suficiente de eficacia.

En adición, señala que obligar a los proveedores a adoptar configuraciones específicas de red y control de tráfico no responden a la arquitectura ni a la evolución natural de sus plataformas, limitando la libertad para gestionar sus redes de manera eficiente, y no se demuestra que sea el mecanismo menos intrusivo ni el más eficaz para mitigar el fraude.

HABLAME

Plantea que la CRC debe evitar trasladar al A2P las lógicas del P2P, pues el mercado A2P tiene flujos, relaciones contractuales y tiempos distintos. En consecuencia, sostiene que cualquier medida que pretenda reforzar controles debería partir de una segmentación adecuada por tipo de tráfico para no afectar desproporcionadamente comunicaciones legítimas.

PTC

Estima que, conforme a disposiciones regulatorias, se necesitaría alrededor de un (1) año para implementar los mecanismos de detección y análisis de tráfico que requieren ajustes en función de las disposiciones de fraude que sean indicadas.

Adicionalmente, resalta la necesidad de mantener modelos dinámicos de detección para evitar afectaciones al usuario legítimo. Como criterio operacional, sugiere fortalecer controles existentes e incrementar gradualmente umbrales de detección, permitiendo adaptación progresiva y resultados tempranos.

TELEFÓNICA

Telefónica reconoce el riesgo asociado al uso fraudulento de planes con SMS ilimitados (granjas de SIM), y considera viable la detección de patrones atípicos basada en analítica de tráfico (volumen, velocidad, dispersión de destinos, correlación IMEI/IMSI).

Sin embargo, se opone a la imposición de límites rígidos definidos regulatoriamente, y propone que la regulación faculte a los operadores para definir umbrales dinámicos dentro de sus políticas de uso justo, acompañados de esquemas de suspensión temporal y mecanismos de autenticación reforzada para evitar afectaciones a usuarios legítimos.

TIGO

Manifiesta que la regulación vigente ya faculta a los operadores para implementar herramientas tecnológicas de prevención del fraude, también en el tráfico P2P, por lo que no comparte el diagnóstico según el cual no existirían controles sobre este tipo de tráfico.

En consecuencia, descarta las alternativas regulatorias que proponen controles adicionales o límites máximos de SMS P2P por usuario, al considerarlas innecesarias y potencialmente lesivas para los derechos de los usuarios legítimos. A su juicio, la imposición de topes rígidos podría afectar la experiencia del servicio contratado y no constituye el mecanismo menos intrusivo ni más eficaz para mitigar el fraude.

Respuesta de la CRC:

En relación con el comentario de **ALDEAMO**, en donde manifiesta que el costo es la razón principal de la ausencia de herramientas para el control para el tráfico de mensajes SMS P2P en Colombia y además propone como alternativa eliminar de la regulación del precio establecido para la remuneración de los mensajes de texto, esta Comisión considera pertinente realizar las siguientes precisiones.

En primer lugar, mediante la Resolución CRC 7007 de 2022 se introdujo el esquema de remuneración *Senders Keeps All* (SKA) para la terminación de SMS en redes móviles. Luego, mediante la Resolución CRC 7753 de 2025 se estableció un umbral de tolerancia más o menos el 5% para el balance de tráfico móvil entre operadores, en los mismos términos en los que fue establecido para compensar los desbalances del tráfico de terminación de llamadas en redes móviles.

Este esquema busca promover el uso eficiente de la red y evitar distorsiones en los incentivos de intercambio de tráfico entre operadores. En este contexto, no se identifican elementos que indiquen que el esquema de remuneración vigente impida o desincentive la adopción de herramientas tecnológicas para la detección de comportamientos anómalos en el tráfico SMS P2P.

Segundo lugar, de acuerdo con la información recopilada por esta Comisión mediante requerimiento de información dirigidos a los operadores móviles[36], estos ya cuentan con diversas herramientas para la gestión y monitoreo del tráfico de SMS P2P, tales como sistemas de análisis de patrones de tráfico, controles de envío masivo desde terminales y mecanismos de detección de comportamientos atípicos asociados a posibles esquemas de fraude. La descripción sobre estas herramientas se presenta en la sección 6.3 que trata sobre la «**Caracterización del comportamiento del servicio de voz y SMS**» en este documento. Si bien estas herramientas pueden presentar distintos niveles de sofisticación entre operadores, su existencia demuestra que el despliegue de mecanismos de control no depende exclusivamente de modificaciones en el régimen tarifario.

De igual forma, es importante señalar que la regulación asociada a la remuneración del servicio de SMS ha sido objeto de revisión reciente en el marco del proyecto regulatorio «Esquemas de

[36] CRC. Radicado de salida 202600188. Asunto: Requerimiento de información No. 2026-010. Información relacionada con la implementación de las medidas para mitigar el fraude cibernético por medio de servicios de telecomunicaciones móviles

Remuneración Mayorista de Redes Móviles[37]», en los cuales se evaluaron las condiciones tarifarias de este servicio a partir del enfoque de costos eficientes que se deriva a partir del Modelo de Empresa Móvil. Tras realizar el análisis de los comentarios recibidos, en el citado proyecto regulatorio se encontró pertinente trasladar la temática de remuneración del servicio de SMS para comunicaciones A2P al presente proyecto la cual es objeto de análisis en la sección 8.3 del presente documento «Comentarios del sector a las alternativas sobre remuneración de mensajes cortos de texto en comunicaciones A2P», con el propósito de articular su análisis e impacto a la luz de la implementación de las alternativas regulatorias orientadas a mitigar el contacto a usuarios con fines fraudulentos.

Frente al comentario de **CLARO**, relacionado con la alternativa que propone la adopción de límites máximos para el envío de SMS P2P por usuario, se hace necesario tener en cuenta que cualquier medida regulatoria que incida sobre el uso de servicios de comunicaciones debe observar los principios de proporcionalidad, necesidad, intervención mínima y protección de los derechos de los usuarios, en concordancia con el marco constitucional y legal aplicable al sector TIC.

En este sentido, es importante precisar que las alternativas regulatorias asociadas al establecimiento de parámetros o límites sobre el tráfico SMS P2P no constituyen decisiones adoptadas, sino hipótesis regulatorias sometidas a evaluación dentro del proceso de AIN. En este sentido, la evaluación de estas alternativas no parte de la intención de imponer restricciones indiscriminadas al uso legítimo del servicio, sino de valorar herramientas que permitan gestionar riesgos específicos asociados al uso irregular del servicio de SMS P2P con fines fraudulentos.

Como se señaló en la respuesta brindada en la sección de Comentarios generales en el contexto de las medidas asociadas al servicio SMS, es importante considerar que el AIN contempla la evaluación de los impactos económicos asociados a cada alternativa, sin embargo, también debe considerarse que la ausencia de mecanismos eficaces de control puede generar externalidades negativas en el ecosistema de comunicaciones, tales como pérdida de confianza de los usuarios, incremento de costos asociados a la gestión de fraudes y afectaciones reputacionales para el sector.

En este sentido, la Comisión reconoce las preocupaciones planteadas por **CLARO** respecto a la proporcionalidad, costos operativos y protección de los usuarios. No obstante, considera necesario evaluar si la adopción de medidas adicionales podría contribuir a mitigar riesgos asociados al uso indebido del tráfico SMS P2P, garantizando que cualquier intervención regulatoria sea proporcional, minimice cargas, respete la neutralidad tecnológica de los operadores y proteja el uso legítimo del servicio de mensajería por parte de los usuarios.

Con respecto a la observación de **HABLAME** en donde indica que se debe evitar trasladar al A2P las lógicas del P2P, esta Comisión coincide en que la cadena de valor del servicio de SMS A2P presenta características estructurales significativamente distintas a las del servicio de SMS P2P. Mientras que el tráfico P2P corresponde principalmente a comunicaciones interpersonales originadas desde terminales móviles, el tráfico A2P se desarrolla en un ecosistema más complejo que involucra múltiples actores, tales como marcas u originadores de contenido, proveedores de contenidos y aplicaciones (PCA), integradores tecnológicos (IT), agregadores y proveedores de redes y servicios de telecomunicaciones (PRST). Esta arquitectura de intermediación implica dinámicas operativas, contractuales y económicas diferenciadas que deben ser consideradas en el diseño de cualquier medida regulatoria.

[37] Comisión de Regulación de Comunicaciones (CRC). Esquemas de Remuneración Mayorista de Redes Móviles. 2026. Disponible en: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-41-7-9

Precisamente por esta razón, el análisis desarrollado por esta Comisión reconoce la necesidad de abordar de manera diferenciada las problemáticas asociadas al tráfico A2P y al tráfico P2P. Sin embargo, es importante precisar que las alternativas regulatorias identificadas en esta materia serán sujeto de análisis en la segunda fase del presente proyecto, en donde se realizará un enfoque de manera separada para cada uno de estos segmentos, de tal manera que se puedan integrar sus especificidades técnicas, sus distintos esquemas de intermediación y los riesgos específicos asociados a cada modalidad de tráfico.

Respecto a los comentarios de **PTC** y **TELEFÓNICA**, en los cuales se señala la necesidad de adoptar modelos dinámicos para la detección de comportamientos irregulares con fines de fraude, esta Comisión reconoce que la eficacia de los mecanismos antifraude se construye a partir de procesos de calibración continua, más que mediante reglas estáticas que pueden incrementar la probabilidad de falsos positivos.

En este sentido, resulta necesario que las herramientas y medidas adoptadas cuenten con la flexibilidad suficiente para evolucionar y adaptarse a los nuevos retos asociados a este tipo de conductas. Así mismo, en línea con la recomendación presentada por **PTC**, la Comisión considera pertinente contemplar periodos de transición para la implementación y puesta en marcha de algunas de las medidas identificadas como posibles soluciones al problema analizado. Por esta razón, la propuesta regulatoria que acompaña el presente proyecto incorpora de manera expresa los plazos previstos para la entrada en vigor de cada una de las medidas que eventualmente se adopten.

Respecto al comentario de **TIGO**, en el cual se señala que la regulación vigente ya faculta a los operadores para implementar herramientas tecnológicas de prevención del fraude, incluyendo aquellas aplicables al tráfico SMS P2P, es importante señalar que, a pesar de que el marco regulatorio vigente contempla disposiciones generales en materia de seguridad, prevención del fraude y gestión del tráfico, el análisis adelantado demuestra que persisten vulnerabilidades tanto en el ecosistema de los servicios SMS como en el llamadas de voz, para la ejecución de acciones irregulares con fines de fraude. Lo anterior sugiere que la mera habilitación regulatoria para implementar controles no necesariamente garantiza su adopción homogénea ni su efectividad sistémica.

En este contexto, las alternativas regulatorias que contemplan mecanismos adicionales de control se plantean como hipótesis regulatorias orientadas a fortalecer las capacidades de detección y prevención del fraude. Estas alternativas no parten de la premisa de que actualmente no existan controles, sino de la necesidad de evaluar si la adopción de medidas adicionales puede contribuir a fortalecer la gestión de riesgos en el tráfico SMS P2P, garantizando en todo caso que cualquier intervención regulatoria respete los principios de proporcionalidad, eficiencia y protección del usuario.

8.2.4 Respuesta a las preguntas de la consulta frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

- *¿Qué retos y beneficios identifica en la implementación de un proceso obligatorio de conocimiento del cliente (KYC) para agregadores de SMS? ¿Qué criterios mínimos considera indispensables para que este proceso sea efectivo y no excluyente?*

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ASOBANCARIA

En su opinión, la implementación de un proceso obligatorio KYC para los agregadores de SMS presenta beneficios relevantes en la mitigación del fraude, al constituirse como el primer control para prevenir la dispersión de mensajes fraudulentos. Así, dice, este mecanismo fortalece la trazabilidad y reduce el riesgo de suplantación o uso indebido del canal SMS. Sin embargo, **ASOBANCARIA** advierte que el principal reto consiste en definir un nivel de KYC suficientemente robusto para identificar empresas legítimas y verificar la coherencia entre su actividad comercial y el contenido de los mensajes enviados, sin generar barreras de entrada ni afectar la competencia. Añade que resulta indispensable establecer criterios mínimos claros y proporcionales, así como implementar procesos periódicos de actualización del KYC que permitan un seguimiento continuo al uso adecuado del canal.

CLARO

Señala que, en su caso, anualmente realzan evaluaciones de sus clientes desde el punto de vista jurídico, financiero y otros, y que en muchos casos se obtienen resultados negativos, no obstante, la regulación obliga a mantener las relaciones de acceso con estos PCA. Y que el efecto de esta medida solo se recoge teniendo en cuenta los resultados negativos de las evaluaciones, y la consecuencia de terminar contratos.

Considera que son retos los costos, agregadores pequeños que pueden enfrentarse a dificultades para cumplir con procesos robustos de verificación, la protección de datos personales, evasión mediante el uso de intermediarios, actores fraudulentos que usen terceros para eludir controles, establecer criterios uniformes entre operadores, PCA e integradores para evitar brechas, y los tiempos de implementación.

PTC

Propone como criterio mínimo que los integradores tecnológicos se clasifiquen mediante un sistema de reputación establecido por la CRC, que permita consultar el nivel de confiabilidad del agregador según su comportamiento y su implementación/detección/gestión del fraude. Indica que el proceso debe ser digital, con soportes, por un tiempo determinado, y aplicable a integradores nacionales e internacionales.

TELEFÓNICA

Considera que el principal beneficio es la trazabilidad, ya que permite vincular un mensaje fraudulento con una persona jurídica o natural real, desincentivando el anonimato. Sin embargo, este agente advierte sobre dos retos. El primer reto es el alcance extraterritorial, ya que muchos agregadores o clientes finales son empresas extranjeras, lo que dificulta la validación de documentos de constitución y representación legal bajo estándares locales. El segundo reto es el costo de implementación, ya que a su juicio la verificación exhaustiva manual es costosa y lenta.

En opinión de **TELEFÓNICA**, se deben tener en cuenta los siguientes criterios mínimos para que el proceso sea efectivo: (i) verificación de la existencia legal de la empresa y del representante legal; (ii) validación de la titularidad de la marca que se pretende usar en el sender ID (identificador de remitente); y (iii) registro de casos de uso (para qué se usará la mensajería).

Finalmente, para **TELEFÓNICA** es importante precisar que la responsabilidad de ejecutar este KYC recae sobre el agregador o integrador que tiene la relación comercial con el cliente, y no sobre el operador de red móvil, quien actúa como transportador.

TIGO

Señala que esta medida debe articularse con las entidades de vigilancia y control para hacer efectivo su cumplimiento. Dentro de los criterios mínimos este proceso debe contener:

- Verificación de identidad.
- Perfilamiento y evaluación del riesgo.
- Monitoreo continuo.

RESPUESTA CRC:

ASOBANCARIA, **CLARO**, **PTC**, **TELEFÓNICA** y **TIGO** coincidieron en que la implementación de un proceso obligatorio de conocimiento del cliente (KYC) para agregadores de SMS genera beneficios relevantes en la mitigación del fraude, al constituirse como una barrera preventiva inicial que reduce el anonimato en el origen del tráfico y fortalece la trazabilidad. Este planteamiento es plenamente consistente con la intención de la CRC al incorporar el KYC como una de las medidas consideradas dentro de las alternativas regulatorias, particularmente como requisito previo para el acceso al canal de envío de mensajes A2P. En consecuencia, este argumento se acoge y conduce a mantener la alternativa de KYC obligatorio para su evaluación posterior.

No obstante, **ASOBANCARIA** y **PTC** advirtieron que uno de los principales retos del KYC obligatorio consiste en definir un nivel de exigencia suficientemente robusto para identificar empresas legítimas y verificar la coherencia entre su actividad comercial y el contenido de los mensajes, sin generar barreras de entrada ni afectar la competencia. La **CRC** considera que este argumento es consistente con el principio de proporcionalidad que orienta el diseño regulatorio y, en consecuencia, se acoge como criterio para la especificación y evaluación del diseño del KYC.

De manera complementaria, **ASOBANCARIA** y **TELEFÓNICA** señalaron que el KYC no debe concebirse como un proceso estático, sino que debe incluir actualizaciones periódicas que permitan un seguimiento continuo del uso del canal. La CRC acoge este planteamiento, dado que la intención regulatoria no es establecer controles meramente formales, sino mecanismos efectivos y sostenibles en el tiempo. Este argumento conduce a mantener la alternativa, incorporando este elemento como criterio de diseño a evaluar.

Por su parte, **CLARO** indicó que, aunque actualmente realiza evaluaciones a sus clientes, estas carecen de efectos prácticos debido a la imposibilidad regulatoria de terminar relaciones de acceso frente a resultados negativos. Este argumento evidencia una limitación del esquema vigente y no cuestiona la pertinencia del KYC, sino su eficacia sin consecuencias asociadas. En consecuencia, la CRC acoge este argumento como insumo para el análisis de las alternativas, precisando que esta temática se aborda de manera específica en la sección asociada con la revisión del régimen de administración de administración de recursos de identificación.

PTC propuso complementar el KYC con un sistema de reputación de agregadores administrado por la CRC. La Comisión reconoce que este planteamiento apunta a reforzar la transparencia del ecosistema, sin embargo, considera que implica desafíos relevantes en términos de gobernanza y costos. En consecuencia, este argumento se acoge como insumo para la evaluación de la alternativa, sin adoptar de manera anticipada dicho esquema.

Finalmente, **TELEFÓNICA** y **TIGO** enfatizaron que la responsabilidad de ejecutar el KYC debe recaer en los agregadores o integradores tecnológicos, y no en los operadores de red móvil. La CRC considera que este argumento es coherente con el enfoque de responsabilidad en el origen y con la separación de roles en la cadena de valor. En consecuencia, este criterio se acoge y condiciona el diseño de la alternativa.

- *Teniendo en cuenta que los agregadores pueden actuar tanto en acuerdos directos (normalmente clientes nacionales como bancos, comercios, entidades de salud o aerolíneas, etc), como en esquemas donde funcionan como parte de una cadena para terminar tráfico de otros agregadores (normalmente tráfico internacional). ¿Qué diferencias, riesgos u oportunidades identifica entre estos dos tipos de tráfico en cuanto al establecimiento de medidas regulatorias para la prevención del fraude? ¿Considera pertinente establecer medidas diferenciadas para cada caso? ¿Qué criterios o mecanismos recomendaría para gestionar de manera más efectiva el tráfico proveniente de cadenas internacionales, especialmente en lo relacionado con la trazabilidad, el monitoreo y la validación de los originadores de contenido?*

ASOBANCARIA

Considera necesario establecer controles generales que sean aplicables tanto al tráfico nacional como al internacional, con el fin de garantizar un nivel mínimo homogéneo de protección frente al fraude. Sin embargo, **ASOBANCARIA** cree que, dadas las particularidades del tráfico internacional, especialmente cuando se estructura a través de esquemas en cadena, resulta pertinente que ciertos controles sean más estrictos en estos casos. A su juicio, la diferenciación regulatoria representa una oportunidad para fortalecer los esquemas de control, priorizando exigencias adicionales para el tráfico internacional, tales como mayores estándares de identificación del origen, monitoreo reforzado y mecanismos preventivos más robustos. Concluye que este enfoque permitiría mitigar los riesgos asociados sin afectar de manera innecesaria el tráfico legítimo, promoviendo un uso más seguro y confiable de los servicios móviles.

CLARO

Señala que es pertinente establecer medidas para diferenciar entre acuerdos directos e internacionales, debido a los riesgos y capacidad de control que operan de forma diferente:

En cuanto al tráfico nacional:

• Trazabilidad: exigir que cada intermediario revele el origen real del mensaje o llamada.
• Monitoreo: usar alertas por volúmenes anormales y patrones sospechosos.
• Validación: implementar procesos de registro y verificación para los originadores antes de permitir el envío.
• Cooperación: Una vez realizada denuncia por estos hechos, es necesario que la CRC actúe con rapidez, para evitar que la situación se siga presentando

En el tráfico internacional, recomienda exigir validación del originador por parte del primer agregador que entrega tráfico al país, trazabilidad obligatoria de toda la cadena y monitoreo reforzado de patrones. Adicionalmente, que se imponga la medida obligatoria a todos los PRSTM de bloquear tráfico con numeración enmascarada.

TELEFÓNICA

A su juicio, el tráfico internacional que pasa por múltiples saltos (hops) presenta el mayor riesgo de pérdida de trazabilidad y manipulación de cabeceras. **TELEFÓNICA** considera que es un riesgo crítico el «blanqueo» de tráfico, donde un mensaje fraudulento entra a través de una ruta legítima. De manera concreta, este operador no recomienda medidas diferenciadas que relajen controles, sino un estándar único de entrada a la red nacional.

Frente a la responsabilidad del último eslabón, **TELEFÓNICA** propone que el agregador o carrier que entrega el tráfico directamente a **TELEFÓNICA** debe ser contractual y legalmente responsable por el contenido que cursa, independientemente de cuántos intermediarios hubo antes. En relación con los identificadores inalterables, **TELEFÓNICA** propone que el sender ID o código corto no sea modificado en el tránsito. Finalmente, **TELEFÓNICA** propone que, si el agregador no puede certificar el origen del tráfico, el operador debe tener la facultad expresa de rechazar dichos mensajes sin sanciones regulatorias.

TIGO

Sugiere que, para el tráfico internacional, también podría contemplarse la asignación de un código corto único por cliente. En la resolución de asignación de un código corto la Comisión debería designar si el código fue asignado para uso de un cliente local o si es para el uso de un cliente internacional. Señala que con esta caracterización se podría validar el establecimiento de reglas diferenciales que debe implementar el asignatario del código corto como la validación mencionada de URLs para el tráfico local. Aclara que en el tráfico internacional no es posible determinar cuál es el cliente que origina el mensaje, debido a que un mensaje puede tener varios saltos antes de llegar al proveedor en Colombia.

Adicionalmente, indica que cuando se detecten patrones o señales objetivas compatibles con campañas asociadas a fraude, debería preverse un marco que habilite, la suspensión temporal y preventiva de la numeración asociada con dicho tráfico, tanto por parte del agregador como del PRST.

RESPUESTA CRC:

La CRC observa que los aportes de **ASOBANCARIA**, **CLARO**, **TELEFÓNICA** y **TIGO** coinciden en que el tráfico internacional cursado a través de esquemas en cadena presenta mayores riesgos estructurales que el tráfico originado en acuerdos directos con clientes nacionales, particularmente en términos de pérdida de trazabilidad, opacidad del origen y dificultad para imputar responsabilidades. Este diagnóstico es consistente con la identificación previa del problema regulatorio y refuerza la necesidad de analizar medidas específicas para este tipo de tráfico.

En relación con la pertinencia de establecer medidas diferenciadas, la CRC identifica una convergencia parcial: mientras **ASOBANCARIA** y **CLARO** consideran razonable introducir controles más estrictos para tráfico internacional, **TELEFÓNICA** advierte que no deben flexibilizarse los estándares, proponiendo en cambio un criterio uniforme de entrada a la red nacional, con responsabilidades claramente asignadas al último eslabón que entrega el tráfico. La Comisión considera que ambos enfoques no son contradictorios, sino complementarios, y en esa medida constituyen insumos válidos para la evaluación regulatoria posterior.

Respecto a los criterios y mecanismos para gestionar tráfico internacional, la CRC identifica como elementos recurrentes en los comentarios: (i) la necesidad de trazabilidad obligatoria de toda la cadena, (ii) la asignación clara de responsabilidad al agregador o carrier que entrega el tráfico a la red nacional, (iii) la implementación de monitoreo reforzado de patrones, y (iv) la posibilidad de rechazo o suspensión preventiva del tráfico cuando no se pueda certificar el origen o existan señales objetivas de fraude. Estos elementos se alinean con el enfoque de gestión del riesgo distribuido que orienta el diseño de las alternativas regulatorias del proyecto.

En consecuencia, la CRC considera que los comentarios recibidos no conducen a descartar ni a modificar una alternativa específica, sino que refuerzan la pertinencia de evaluar esquemas diferenciados o reforzados para tráfico internacional, manteniendo principios de proporcionalidad, trazabilidad y responsabilidad en el origen. Estas consideraciones serán incorporadas como criterios de evaluación en el marco del AIN.

- *¿Considera pertinente la implementación de un proceso centralizado o distribuido para la validación de agregadores, marcas y campañas antes de cursar tráfico A2P?*

ASOBANCARIA

Opina que ambas alternativas contribuyen a la mitigación del fraude en el tráfico A2P, en la medida en que fortalecen los mecanismos de validación previa de agregadores, marcas y campañas antes de cursar el tráfico. Sin embargo, **ASOBANCARIA** sostiene que se considera más conveniente optar por un proceso centralizado. Al respecto, indica que un esquema centralizado permitiría aplicar criterios homogéneos de validación, reducir asimetrías entre actores, facilitar la supervisión regulatoria y mejorar la trazabilidad del origen del tráfico y de las campañas autorizadas. Adicionalmente, **ASOBANCARIA** señala que este enfoque favorece una identificación más clara de responsabilidades frente a eventuales incidentes de fraude, así como una respuesta más ágil y coordinada ante comportamientos irregulares.

CLARO

No considera acertada la propuesta sin analizar previamente si las medidas actualmente disponibles son suficientes para atender la problemática. En particular, señala que debe evaluarse el efecto de la suspensión provisional mientras se adelanta la actuación administrativa de recuperación del código corto por uso indebido, así como otras alternativas como el bloqueo por parte de los PRSTM cuando, mediante herramientas tecnológicas, se evidencie el envío de SMS con contenido fraudulento, y la terminación de contratos con PCA/IT como última instancia.

Indica que, una vez se conozcan los resultados de la aplicación de estas medidas, podría analizarse la necesidad de eventuales ajustes regulatorios adicionales.

Finalmente, **CLARO** sostiene que la regulación debe aplicarse de manera proporcional y únicamente cuando sea necesaria para corregir fallas de mercado, proteger a los usuarios o garantizar condiciones de competencia. Advierte que una intervención excesiva o injustificada puede generar cargas adicionales para los agentes, distorsionar el funcionamiento del mercado y limitar la innovación.

PTC

Sugiere un proceso que permita conocer a los agregadores de manera pública y por parte de la CRC, para establecer confianza a partir de la medición del comportamiento en detección de fraude. Reitera que debe ser digital, con soportes, por un tiempo determinado y sin limitarse por nacionalidad (nacional/internacional).

TELEFÓNICA

Sostiene que es pertinente establecer mecanismos robustos de validación (KYC) para agregadores, marcas y campañas, reconociendo que unificar estos criterios es un paso positivo para sanear el ecosistema. De manera concreta, para **TELEFÓNICA** es importante asegurar que la arquitectura elegida no introduzca latencias o puntos únicos de falla que puedan impactar la experiencia del usuario final o la seguridad de la información transaccional.

Respecto a la alternativa de implementación distribuida (basada en tecnologías como DLT o Blockchain), a **TELEFÓNICA** le preocupa el hecho de que podría implicar costos de inversión y operación desproporcionados frente a la estructura económica actual del servicio de SMS. En consecuencia, este operador sugiere que se prioricen modelos que sean costo-eficientes y sostenibles en el tiempo. En resumen, **TELEFÓNICA** considera que los costos de implementación, gestión y consulta de estas plataformas no deben ser trasladados a los Proveedores de Redes (PRSTM), dado que, a su juicio, no son los generadores del contenido ni quienes gestionan la relación comercial con las marcas. Al respecto, **TELEFÓNICA** insiste en que la responsabilidad operativa de realizar la validación y mantener la información actualizada debe recaer en los Agregadores y PCAs, quienes tienen el vínculo directo con el cliente final.

TIGO

Considera que esta alternativa podría implicar costos elevados de implementación y sostenimiento. Agrega que, dado el carácter dinámico del fraude, existe un riesgo significativo de que los actores fraudulentos adapten rápidamente sus tácticas, reduciendo la efectividad de la medida en el corto plazo y obligando a incurrir en nuevas inversiones para mantener su utilidad.

Estima más pertinente priorizar la asignación única por marca de códigos cortos o numeración E.164, en la medida en que simplifica el ecosistema de envío, facilita la trazabilidad y el control, y permite una implementación más directa y costo-eficiente.

RESPUESTA CRC:

La CRC observa que los comentarios de **ASOBANCARIA**, **CLARO**, **PTC**, **TELEFÓNICA** y **TIGO** reflejan posiciones diferenciadas respecto a la conveniencia y arquitectura de un proceso de validación

previa de agregadores, marcas y campañas antes de cursar tráfico A2P. No obstante, existe coincidencia en que el fortalecimiento de la validación previa es un elemento relevante para la mitigación del fraude, particularmente en lo relacionado con la reducción del anonimato y la mejora de la trazabilidad.

En particular, **ASOBANCARIA** destaca las ventajas de un esquema centralizado, enfatizando la homogeneidad de criterios, la reducción de asimetrías y la facilidad de supervisión. La CRC reconoce que estos atributos son consistentes con la intención regulatoria de fortalecer la trazabilidad y la imputación de responsabilidades, sin que ello implique una decisión anticipada sobre la adopción de dicho esquema.

Por su parte, **CLARO** plantea que no resulta procedente adoptar nuevas plataformas sin antes evaluar la efectividad de las herramientas actualmente vigentes, como la suspensión provisional del tráfico y las medidas frente a reincidencia. La CRC considera que este argumento es consistente con los principios de necesidad y proporcionalidad regulatoria, y lo acoge como criterio metodológico para la evaluación de alternativas, sin embargo, no descarta las opciones de validación centralizada o distribuida y por lo que procederá con su evaluación, así como, se analizará lo correspondiente en la sección 8.2.7 visto desde el enfoque de simplificación la suspensión provisional del tráfico y las medidas frente a la reincidencia.

TELEFÓNICA y **TIGO** advierten sobre los riesgos económicos, operativos y de gobernanza asociados tanto a modelos centralizados como distribuidos, particularmente en lo relativo a costos, latencias y sostenibilidad del sistema. La CRC reconoce estos riesgos como elementos relevantes que elevan el umbral de justificación de estas alternativas y refuerzan la necesidad de evaluarlas cuidadosamente en el marco del AIN.

En consecuencia, la CRC concluye que los aportes recibidos no conducen a descartar ni a adoptar de manera anticipada un proceso centralizado o distribuido de validación. Por el contrario, se mantienen ambas alternativas como hipótesis regulatorias, sujetas a evaluación integral en el AIN, considerando criterios de proporcionalidad, costos, viabilidad técnica, gobernanza y alineación con las herramientas ya existentes.

- *¿Cuáles serían, a su juicio, los principales desafíos técnicos, económicos, operativos y de gobernanza para un sistema centralizado de validación de remitentes y campañas? ¿Qué mecanismos de transparencia y auditoría considera necesarios?*

ASOBANCARIA

En su sentir, el principal desafío de un sistema centralizado de validación de remitentes y campañas es diseñar un proceso de inscripción y validación que articule de forma coherente la verificación de agregadores, remitentes y campañas, garantizando la legitimidad y consistencia del objetivo de los mensajes. Adiciona que el sistema debe equilibrar la robustez de los controles con la eficiencia operativa y la diversidad de modelos del ecosistema. Sugiere que resulta pertinente compartir de manera periódica resultados agregados del proceso con los principales actores, como insumo para la mejora continua de los controles.

CLARO

Considera que la propuesta es innecesaria y que su implementación implicaría importantes desafíos técnicos, económicos, operativos y de gobernanza, lo que la convertiría en una medida costosa y de largo plazo. Señala que, en un entorno donde las modalidades de fraude evolucionan rápidamente, este tipo de medidas no garantizan resultados y pueden generar cargas significativas para los agentes.

Entre los principales retos se encuentran la validación de un alto volumen de campañas en tiempo real sin afectar la entrega del tráfico, la integración con múltiples operadores y plataformas, la seguridad y protección de datos, los altos costos de infraestructura y operación, así como riesgos de exclusión para actores con menor capacidad. También advierte dificultades operativas asociadas a la gestión de picos de tráfico, la necesidad de atención permanente y la definición de un esquema claro de administración y supervisión de la plataforma.

En ese contexto, **CLARO** solicita a la CRC que, antes de adoptar una medida de este tipo, evalúe formalmente la efectividad de la suspensión provisional y determine si persiste un problema residual; fortalezca los procesos de recuperación y la articulación sectorial; y realice un análisis de impacto normativo (AIN). A su juicio, solo si dicho análisis demuestra que el fraude no puede ser contenido con las herramientas actuales tendría sentido considerar nuevos desarrollos técnicos.

Finalmente, concluye que la medida propuesta no resulta viable para atender la problemática, especialmente considerando que esta se ha mitigado en gran medida con la suspensión provisional aplicada por la CRC al iniciar actuaciones administrativas.

TELEFÓNICA

Identificó un desafío económico correspondiente a que los márgenes del servicio de SMS son estrechos. A su juicio, crear una entidad centralizada implica costos de administración que no pueden ser trasladados a los operadores de red, cuyas tarifas de acceso ya son bajas. Además, advirtió sobre la latencia como un desafío operativo, ya que consultar una base de datos central por cada envío masivo (millones de transacciones) puede degradar la calidad del servicio y afectar la entrega de mensajes críticos (como OTPs bancarios). Finalmente, **TELEFÓNICA** advirtió sobre la existencia de un desafío de gobernanza al momento de definir quién responde cuando el validador central comete un error (falso positivo) y bloquea una campaña legítima de un banco o entidad de salud.

Este operador propone un mecanismo de auditoría en tiempo real y un SLA (acuerdo de nivel de servicio) estricto, donde el administrador central asuma la responsabilidad por fallas en la validación.

RESPUESTA CRC:

La CRC observa que los comentarios de **ASOBANCARIA**, **CLARO** y **TELEFÓNICA** coinciden en que un sistema centralizado de validación de remitentes y campañas plantea desafíos relevantes en múltiples dimensiones, particularmente en términos técnicos, económicos, operativos y de gobernanza. Estos aportes confirman que se trata de una alternativa de alta complejidad, cuyo diseño y eventual implementación exige un análisis riguroso y proporcional.

En el plano técnico y operativo, la Comisión identifica como desafíos recurrentes la capacidad de validar grandes volúmenes de campañas en tiempo real, la integración con múltiples plataformas y actores del ecosistema, y el riesgo de latencias operativas que puedan afectar la continuidad de

servicios críticos. La CRC reconoce que estos elementos son especialmente sensibles en el contexto del tráfico A2P, donde la oportunidad en la entrega del mensaje es un atributo esencial.

Desde la dimensión económica, la CRC recoge las preocupaciones asociadas a los costos de implementación, operación y sostenimiento de una entidad centralizada, particularmente en un mercado caracterizado por bajos márgenes en el servicio SMS. En este sentido, la Comisión considera que estos factores elevan el umbral de justificación de la alternativa y refuerzan la necesidad de evaluarla estrictamente bajo la metodología del AIN.

En materia de gobernanza, la CRC identifica como aspecto crítico la asignación de responsabilidades frente a errores del sistema, tales como bloqueos indebidos o falsos positivos. Al respecto, la Comisión reconoce la pertinencia de los planteamientos orientados a establecer mecanismos claros de auditoría, transparencia y niveles de servicio, como condición mínima para cualquier esquema de validación centralizada.

En consecuencia, la CRC concluye que los comentarios recibidos aportan criterios esenciales para su evaluación y eventual desarrollo en la propuesta regulatoria, en particular en lo relacionado con:

- La necesidad de mecanismos de transparencia y auditoría verificables.
- La definición clara de responsabilidades del administrador del sistema.
- La evaluación de costos, latencias y riesgos de exclusión.

Estos elementos serán considerados como insumos técnicos clave.

- *¿Qué ventajas y desafíos técnicos, económicos, operativos o de gobernanza identifica en un modelo distribuido de validación basado en DLT? ¿Qué elementos deberían definirse para asegurar la interoperabilidad y la confianza entre los distintos actores?*

ASOBANCARIA

Indica que los principales retos se concentran en los aspectos técnicos y de gobernanza, particularmente en la delimitación de responsabilidades frente a eventos de fraude. Añade que resulta necesario garantizar una adecuada experiencia de usuario, mediante la detección y bloqueo efectivo de SMS fraudulentos, manteniendo bajos niveles de falsos positivos.

CLARO

Expone que la propuesta es inviable, pues implicaría altos costos, una implementación prolongada y múltiples desafíos técnicos, económicos, operativos y de gobernanza. Señala que, en un contexto donde el fraude evoluciona rápidamente, este tipo de medidas de largo plazo no garantiza resultados y puede generar cargas significativas para los actores, además de dificultades para alinear responsabilidades entre los participantes del ecosistema.

Entre los principales retos menciona la validación de grandes volúmenes de campañas sin afectar el tráfico A2P, la integración entre operadores y plataformas, la protección de datos, los costos de implementación y mantenimiento, la definición de la administración de la plataforma y la necesidad de reglas claras de acceso, seguridad e interoperabilidad.

En ese sentido, solicita a la CRC que antes de adoptar la medida evalúe la efectividad de la suspensión provisional y determine si existe un problema residual, fortalezca los procesos de recuperación y la articulación sectorial, y realice un análisis de impacto normativo (AIN). A su juicio, solo si dicho análisis demuestra que las herramientas actuales no son suficientes tendría sentido considerar nuevos desarrollos técnicos. Finalmente, concluye que la medida no resulta necesaria, especialmente considerando que la problemática se ha mitigado en gran parte con la suspensión provisional aplicada por la CRC al iniciar actuaciones administrativas.

TELEFÓNICA

Opina que la inmutabilidad de los registros y trazabilidad descentralizada es una ventaja teórica.

Por su parte, **TELEFÓNICA** considera que los costos y tiempos de transacción son desafíos reales, ya que las tecnologías DLT (blockchain) suelen tener costos de escritura y lectura que harían inviable el modelo de negocio del SMS A2P, además de tiempos de confirmación que no se ajustan a la inmediatez requerida.

De manera concreta, **TELEFÓNICA** resume su posición en el sentido de advertir que imponer tecnologías complejas como DLT sin un Análisis de Impacto Normativo (AIN) previo que demuestre que el beneficio en reducción de fraude supera los altos costos de implementación (CAPEX/OPEX), podría encarecer el servicio al punto de desplazar el tráfico hacia canales OTT no regulados, anulando el propósito de la medida.

RESPUESTA CRC:

La CRC observa que los comentarios de **ASOBANCARIA**, **CLARO** y **TELEFÓNICA** coinciden en que un modelo distribuido de validación basado en DLT presenta desafíos significativos en términos técnicos, económicos, operativos y de gobernanza, que superan ampliamente los beneficios potenciales identificados hasta el momento.

En el plano técnico y operativo, la Comisión identifica como obstáculos relevantes la capacidad de procesar grandes volúmenes de validaciones en tiempo real, los tiempos de confirmación propios de las tecnologías DLT, y la complejidad de integrar múltiples actores bajo un esquema distribuido sin afectar la entrega oportuna del tráfico A2P. La CRC reconoce que estos elementos son críticos en un servicio donde la latencia y la continuidad son atributos esenciales.

Desde la dimensión económica, la CRC recoge la preocupación reiterada sobre los altos costos de implementación y operación de soluciones basadas en DLT, así como el riesgo de que dichos costos resulten desproporcionados frente a la estructura económica actual del servicio de SMS. En este sentido, la Comisión considera que estos factores elevan de manera significativa el umbral de justificación de esta alternativa y refuerzan la necesidad de una evaluación rigurosa en el marco del AIN.

En materia de gobernanza, la CRC identifica como desafío central la definición de responsabilidades entre los distintos participantes del modelo distribuido, particularmente frente a errores, fallas del sistema o eventos de fraude. Asimismo, se reconoce que asegurar la interoperabilidad y la confianza

entre actores requeriría reglas claras de participación, estándares técnicos comunes y mecanismos de supervisión, cuya complejidad no ha sido resuelta en el contexto actual del ecosistema A2P.

En consecuencia, la CRC concluye que los aportes recibidos añaden elementos de análisis para la evaluación de la alternativa y la posible estructuración como propuesta regulatoria. En este sentido, la alternativa se mantiene únicamente como hipótesis regulatoria, sujeta a evaluación estricta dentro del AIN, con un umbral de justificación elevado dada su complejidad, costos y riesgos asociados.

- *¿Qué requerimientos funcionales considera que una solución tecnológica debe tener en cuenta para llevar a cabo de manera efectiva la validación de autenticidad de las URL en el evento que el mensaje corto de texto las contenga?*

ASOBANCARIA

Sugiere que una solución para validar la autenticidad de las URL contenidas en SMS debería integrar mecanismos de evaluación conjunta del contenido del mensaje, la URL incluida y el nivel de riesgo asociado, considerando variables técnicas como el dominio u host, la reputación de la URL y la validez de los certificados SSL. A su juicio, esto permitiría detectar oportunamente enlaces maliciosos y mitigar la distribución de phishing, reduciendo la exposición de los usuarios a fraudes.

CLARO

Expone que en un contexto donde el fraude evoluciona rápidamente, medidas de largo plazo no garantizan resultados y pueden generar cargas significativas para el sector.

Además, que cuando los mensajes incluyan URL, corresponde al dueño del contenido garantizar su verificación en tiempo real, incluyendo la validación del dominio (seguro y que no esté en listas negras), la seguridad del certificado, la reputación del sitio y la confirmación del titular de la marca, asegurando también su adecuada integración con los sistemas de los PRST.

En ese sentido, se solicita a la CRC que, antes de adoptar la medida, evalúe la efectividad de la suspensión provisional, fortalezca los procesos de recuperación y la articulación sectorial, y realice un Análisis de Impacto Normativo (AIN). Solo si dicho análisis demuestra que las herramientas actuales no son suficientes tendría sentido considerar nuevos desarrollos técnicos. En todo caso, se considera que la medida no resulta viable, especialmente considerando que la problemática se ha mitigado en gran medida con la suspensión provisional aplicada por la CRC.

TELEFÓNICA

Considera que la implementación técnica, sin vulnerar la privacidad, requeriría: (i) Que la validación se realice contra una «lista blanca» de dominios pre-registrados por el cliente corporativo al momento de contratar la campaña; (ii) Que el sistema sea automatizado (sin intervención humana); y (iii) Que exista una exención de responsabilidad legal para el operador por el tratamiento de estos datos con fines de ciberseguridad.

TIGO

Considera que con la asignación de un único código corto o numeración E.164 por marca, se refuerza la trazabilidad del tráfico y la asociación unívoca entre el identificador utilizado para el envío y el titular responsable del contenido. Señala que, bajo este esquema, el agregador contaría con un parámetro objetivo para la debida diligencia de sus clientes. Indica que en este contexto el agregador podría incorporar reglas de validación y gestión del tráfico (firewalls) en sus plataformas para detectar y bloquear mensajes que incluyan enlaces distintos a los previamente registrados y autorizados por el titular de la marca, en tanto tales desviaciones constituyen un indicador de riesgo de suplantación o de campañas de smishing.

RESPUESTA CRC:

La CRC observa que los aportes de **ASOBANCARIA**, **CLARO, TELEFÓNICA** y **TIGO** convergen en que la validación de autenticidad de URL incluidas en mensajes SMS debe sustentarse en criterios técnicos objetivos, orientados a reducir el riesgo de phishing y smishing, sin afectar la continuidad del tráfico legítimo.

De manera transversal, la Comisión identifica coincidencias en torno a la necesidad de que las soluciones tecnológicas contemplen:

- la verificación del dominio y la reputación de la URL
- la validación de la titularidad de la marca
- el uso de listas blancas previamente registradas
- la automatización del proceso, evitando intervenciones manuales que introduzcan latencias o riesgos operativos.

Asimismo, la CRC reconoce que varios agentes enfatizan la importancia de asignar responsabilidades claras en la cadena de valor, particularmente en cabeza del agregador u originador del contenido, y no de los PRST, así como la necesidad de que cualquier esquema de validación se integre adecuadamente con los sistemas existentes y respete los principios de protección de datos personales. En consecuencia, la Comisión considera que los requerimientos funcionales identificados constituyen insumos técnicos relevantes para la evaluación de las alternativas regulatorias asociadas a la mitigación del fraude mediante SMS A2P, y para la eventual formulación de este elemento en la propuesta regulatoria.

- *¿Qué impactos positivos y negativos prevé en la obligación de bloquear o marcar mensajes que no cuenten con identificadores validados? ¿Cómo se podría garantizar que no se afecte la entrega de mensajes legítimos?*

ASOBANCARIA

Considera que la obligación de bloquear o marcar mensajes sin identificadores validados puede tener un impacto en la mitigación del fraude, al limitar la suplantación de identidad. Sugiere que, para evitar afectaciones al tráfico legítimo, resulta necesario establecer un proceso de transición gradual y un mecanismo de registro sencillo y estandarizado de los mensajes, que permita a los actores adaptarse sin afectar la entrega de comunicaciones legítimas.

CLARO

Considera que, si en el proceso previo al envío de mensajes, se realiza correctamente, y que en sus remitentes cumplieran con la regulación existente, no debería tener afectación asociada a los mensajes legítimos, Señala que, en todo caso pueden haber impactos positivos tal como la protección al usuario, reducción de campañas fraudulentas y fortalecimiento de trazabilidad del tráfico A2P; en impactos negativos señalar que pueden presentarse bloqueos de mensajes legítimos por errores de validación o fallas en el registro de originadores.

SFC

Comenta que la obligación de bloqueo o alerta sobre los mensajes con alta sospecha de ser fraude puede constituir una verdadera protección para los consumidores. Ahora bien, añade que es importante que la eventual normatividad asigne esta obligación a los operadores, y no a las entidades o comercios que hacen uso legítimo del canal SMS. La claridad sobre el sujeto obligado a operar el bloqueo o la alerta puede reducir indebidas interpretaciones normativas, y evitar una afectación al uso adecuado del canal.

Igualmente, añade que, con el objetivo de facilitar la aplicación práctica de esta obligación, es recomendable que existan canales de coordinación entre los operadores y los usuarios masivos del canal SMS, con el fin de evitar bloqueos indebidos a mensajes relevantes. Es importante que los usuarios del canal SMS tengan alternativas para informar a los operadores las condiciones de uso masivo del canal, con el fin de evitar bloqueos que no sean procedentes.

TELEFÓNICA

Identificó la limpieza inmediata del ecosistema y reducción drástica del smishing como positivo.

Por su parte, calificó como negativo el riesgo de bloquear notificaciones críticas (salud, banca, emergencias) si el proceso de validación falla o es lento.

En cuanto a la forma de garantizar que no se afecte la entrega de mensajes legítimos, TELEFÓNICA propone una implementación gradual con «listas de confianza» para actores críticos y un canal de soporte 24/7 exclusivo para reactivación de tráfico legítimo bloqueado erróneamente.

TIGO

Señala que con la alternativa más pertinente de implementación es la asignación de un único código corto o numeración E.164 por marca. Con este mecanismo no se materializaría el riesgo asociado a la no entrega de mensajes legítimos que no cuenten con identificadores validados.

RESPUESTA CRC:

La CRC observa que los comentarios de **ASOBANCARIA**, **CLARO**, **SFC**, **TELEFÓNICA** y **TIGO** coinciden en que la obligación de bloquear o marcar mensajes que no cuenten con identificadores validados puede generar impactos positivos relevantes en la mitigación del fraude, particularmente al reducir la suplantación de identidad y fortalecer la trazabilidad del tráfico A2P. Este enfoque es

consistente con la intención regulatoria de limitar el anonimato en el origen del tráfico y proteger a los usuarios finales.

No obstante, la Comisión también identifica una convergencia clara en torno a los riesgos asociados a bloqueos indebidos, especialmente cuando se trata de mensajes legítimos y críticos, como aquellos relacionados con servicios financieros, salud o emergencias. La CRC reconoce que estos riesgos podrían afectar la confianza en el canal SMS y generar externalidades negativas si no se diseñan salvaguardas adecuadas.

En este contexto, la CRC acoge como criterios relevantes para el diseño de la alternativa, los siguientes:

- la gradualidad en la implementación
- la definición de mecanismos de registro claros y estandarizados
- la habilitación de canales de coordinación y soporte para la gestión de bloqueos erróneos
- la asignación clara de responsabilidades dentro de la cadena de valor

En consecuencia, la CRC concluye que los aportes recibidos condicionan la evaluación de la alternativa en cuanto a la incorporación de salvaguardas operativas y procedimentales que permitan maximizar los beneficios antifraude sin afectar la entrega de mensajes de texto (SMS) legítimos, así como la eventual estructuración de una propuesta regulatoria al respecto.

- *¿Qué ventajas y riesgos observa en la clasificación obligatoria de los mensajes por tipo de contenido y la articulación con el consentimiento del usuario mediante el RNE? ¿Cómo podría mejorarse la protección de los derechos del usuario a decidir el tipo de contenido que desea recibir? ¿Considera pertinente una clasificación de tipos de contenido distinta a la propuesta?*

ASOBANCARIA

Sostiene que las principales ventajas se relacionan con el uso adecuado del consentimiento del usuario y la priorización de mensajes críticos, como alertas de seguridad, OTP o notificaciones financieras. Precisa que el principal riesgo radica en garantizar una correcta categorización que evite que mensajes fraudulentos sean clasificados como prioritarios.

CLARO

Expone que una medida como la propuesta genera altas cargas y costos operativos, y que puede afectar la experiencia del usuario, si se etiqueta incorrectamente los mensajes legítimos, y en consecuencia se bloquea una campaña legitima tal como de salud, bancos, y/o desastres naturales.

Asimismo, señala que solo es pertinente si mejora la diferenciación entre mensajes transaccionales, informativos y promocionales sin generar complejidad innecesaria, en razón a ello, solicita a la CRC antes de implementar una medida como la propuesta (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos.

Concluye en todo caso, que no es una medida viable para la solución de la problemática, dado que a su juicio el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando da inicio una actuación administrativa.

TELEFÓNICA

Considera como ventaja la capacidad de empoderar al usuario para filtrar selectivamente el tráfico, permitiendo, por ejemplo, bloquear comunicaciones comerciales sin impedir la recepción de mensajes críticos como OTPs o notificaciones bancarias. Sin embargo, **TELEFÓNICA** considera que existe un desafío técnico y operativo relacionado en garantizar la veracidad de dicha clasificación. Concretamente, dice, existe un riesgo latente de que los originadores etiqueten erróneamente mensajes publicitarios como «transaccionales» o «de servicio» para evadir bloqueos. Ante lo anterior, **TELEFÓNICA** propone una clasificación simplificada (por ejemplo, limitándose a «Comercial/Publicitario» y «Servicio/Transaccional») que facilitaría la gestión y reduciría las zonas grises, siempre bajo la premisa de que la responsabilidad por el correcto etiquetado recae en el Agregador y no en el operador de red.

Frente al Registro de Números Excluidos (RNE), **TELEFÓNICA** considera que la protección de los derechos del usuario mejora si se establece la obligación estricta para el Agregador o PCA de consultar y depurar sus bases de datos contra el RNE antes de inyectar el tráfico en la red. En todo caso, **TELEFÓNICA** considera que el RNE ha mostrado limitaciones en su eficacia, pues los usuarios inscritos continúan recibiendo tráfico no deseado, por lo que sugiere la implementación de mecanismos de vigilancia y sanción efectivos por parte de las autoridades competentes (SIC/CRC).

TIGO

Considera pertinente recordar que recientemente se adelantó la implementación de la Resolución CRC 7356 de 2024 «Por la cual se modifican disposiciones sobre el Registro de Números Excluidos contenidas el Capítulo 1 del Título II de la Resolución CRC número 5050 de 2016 y se dictan otras disposiciones.», cambio motivado por las disposiciones contenidas en la Ley 2300 de 2023 conocida como la Ley «Dejen de fregar». Así las cosas, señala que introducir nuevas obligaciones regulatorias sobre consentimiento y
categorización, podría desbordar el alcance del proyecto, generar solapamientos normativos y elevar la complejidad de articulación con una norma de jerarquía superior ya vigente e implementada, sin aportar una solución real y proporcional al núcleo del problema.

RESPUESTA CRC:

La CRC observa que los comentarios de **ASOBANCARIA**, **CLARO**, **TELEFÓNICA** y **TIGO** evidencian posiciones divergentes respecto a la conveniencia y alcance de la clasificación obligatoria de mensajes por tipo de contenido y su articulación con el consentimiento del usuario mediante el RNE. No obstante, existe coincidencia en que la clasificación puede ofrecer beneficios potenciales en términos de protección del usuario, siempre que se diseñe con criterios de proporcionalidad y correcta implementación.

En particular, la Comisión identifica como ventaja reconocida la posibilidad de priorizar mensajes críticos y de empoderar al usuario para decidir el tipo de contenido que desea recibir. Sin embargo, la CRC también recoge de manera consistente los riesgos asociados a la clasificación incorrecta, la generación de falsos positivos, y la afectación indebida de comunicaciones legítimas, lo cual podría erosionar la confianza en el canal SMS.

Respecto a la articulación con el RNE, la CRC reconoce los argumentos que advierten sobre la reciente implementación normativa de este mecanismo y el riesgo de duplicidad regulatoria. En este sentido, la Comisión considera pertinente evitar solapamientos normativos y evaluar cuidadosamente la temática para evitar que nuevas obligaciones de categorización generen cambios a las recientes implementaciones en el marco del RNE.

- *¿Qué capacidades o características mínimas debería tener el sistema de monitoreo de tráfico por parte de los agregadores para detectar patrones anómalos o sospechosos? ¿Qué salvaguardas deberían definirse para evitar bloqueos injustificados?*

ASOBANCARIA

Expone que el sistema de monitoreo de tráfico de los agregadores debe contar con un motor de evaluación de riesgo en tiempo real, detección de patrones anómalos, reglas de control parametrizables y análisis de URLs. Adiciona que se deben incorporar mecanismos de retroalimentación continúa basados en reportes de fraude, asegurar la trazabilidad de las acciones ejecutadas y generar reportes estandarizados que faciliten la supervisión y la mejora continua.

CLARO

Considera que como mínimo debería contar con capacidad para analizar volúmenes y frecuencias de envío, identificar variaciones atípicas, detectar remitentes irregulares y validar coincidencias con las listas de riesgo.

PTC

Señala que el sistema debe poder procesar el total de SMS enviados y recibidos, operar de manera automática y autónoma, y ser masivo (no basado en filtrado manual o búsquedas puntuales). Indica que el software debe estimar la mayor probabilidad de fraude. Frente a bloqueos injustificados, afirma que ocurrirán y deben desbloquearse en el menor tiempo posible, con análisis posterior y decisión manual de aprobación o rechazo.

TELEFÓNICA

Opina que los sistemas de monitoreo de los agregadores deben tener como mínimo: (i) Detección de volumen inusual (rate-limiting) correspondientes a alertas por picos de tráfico no programados; (ii) Análisis de contenido repetitivo en términos de detección de campañas idénticas enviadas desde múltiples orígenes; y (iii) Validación de sender ID para asegurar que el remitente alfanumérico corresponda al autorizado.

Frente a las salvaguardas, **TELEFÓNICA** enfatiza la necesidad de protocolos claros de «notificación y defensa» post-bloqueo, permitiendo al operador actuar primero para proteger al usuario y revisar después.

RESPUESTA CRC:

En términos generales, los comentarios recibidos evidencian coincidencias relevantes entre los agentes respecto a las capacidades técnicas mínimas que deberían integrar los sistemas de monitoreo de tráfico asociados a la provisión de servicios de mensajería móvil, particularmente en el ámbito A2P y en los eslabones de agregación e intermediación. De manera transversal, se resalta la necesidad de incorporar herramientas automatizadas de análisis masivo que permitan detectar patrones anómalos de tráfico, variaciones atípicas de volumen y frecuencia de envío, validaciones de identidad del remitente, análisis de contenido repetitivo y mecanismos de evaluación probabilística de riesgo de fraude.

Asimismo, varios operadores destacan la importancia de que estos sistemas cuenten con motores de detección en tiempo real, reglas parametrizables, validación contra listas de riesgo, análisis de URLs, trazabilidad de las acciones ejecutadas y generación de reportes estandarizados que faciliten la supervisión regulatoria. De igual forma, se subraya la necesidad de integrar esquemas de retroalimentación continúa basados en reportes de fraude y protocolos claros para la gestión de falsos positivos, incluyendo mecanismos de desbloqueo oportuno y revisión posterior bajo criterios objetivos.

Estos aportes son considerados por la CRC como insumos técnicos relevantes para la estructuración de la temática correspondiente que aborda la «Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude» que se encuentra descrita en la sección 9.2.1.2. del presente documento. En específico, para la construcción de la alternativa 2, la cual está asociada con la adopción de herramientas para el monitoreo y gestión de riesgos por parte de los actores que intervienen en la cadena de provisión del servicio. En consecuencia, dichos elementos serán considerados dentro del análisis técnico que se desarrolla en el marco del Análisis de Impacto Normativo (AIN).

- ¿Qué beneficios y limitaciones identifica en la alternativa de asignación de códigos alfanuméricos, códigos cortos o números E.164 exclusivos para cada marca? ¿Cómo podría impactar esto en la trazabilidad y la experiencia del usuario?

ASOBANCARIA

Indica que los beneficios dependen de la veracidad de la marca asociada a cada identificador, dado el riesgo de suplantación. En términos de trazabilidad, **ASOBANCARIA** añade que los beneficios serían mayores en la medida en que existan acciones efectivas frente a los agregadores y las marcas involucradas.

CLARO

Expone como cierto que los usuarios normalmente no revisan bien el origen del mensaje, situación que le baja eficacia a la propuesta, no obstante, el hecho que se asigne un código exclusivo a cada

marca permite identificar plenamente al remitente de la información, y señalarlo cuando la misma es fraudulenta.

SFC

Menciona que esta alternativa elimina la ambigüedad en las comunicaciones al asignar un recurso único a cada entidad financiera, lo que reduce el riesgo de suplantación asociado a números compartidos y permite a los usuarios identificar con mayor certeza los mensajes oficiales.

No obstante, la SFC observa que esta medida se enfoca en la identificación del remitente, pero no en el contenido del mensaje, por lo que, si no se acompaña de controles sobre las plantillas autorizadas, el riesgo de fraude se mantiene. Adicionalmente, asegura que su efectividad puede verse limitada en teléfonos más antiguos o cuando el mecanismo depende de que el usuario recuerde códigos. En términos de trazabilidad, la medida facilita significativamente la investigación y asignación de responsabilidades, y desde la perspectiva del usuario contribuye a restablecer la confianza en el canal y a reducir la exposición a fraudes.

TELEFÓNICA

Subraya como beneficio el incremento sustancial en la trazabilidad y la confianza del usuario, ya que la asignación exclusiva elimina la ambigüedad que hoy existe con los códigos cortos compartidos, donde un mismo número es utilizado por múltiples empresas, dificultando distinguir una comunicación legítima de una fraudulenta. En su opinión, el uso de identificadores alfanuméricos (sender ID) exclusivos refuerza la identidad de marca y facilita al ciudadano reconocer quién le escribe.

A pesar de lo anterior, **TELEFÓNICA** advierte sobre limitaciones técnicas y operativas importantes. En concreto, este operador sostiene que la migración masiva a numeración E.164 para aplicaciones comerciales requeriría ajustes profundos en los sistemas de enrutamiento y señalización de las redes móviles, así como en las plataformas de los agregadores. Adicionalmente, TELEFÓNICA considera que, si la asignación no se gestiona con agilidad, podría generar barreras de entrada para pequeñas empresas. Añade que, en términos de experiencia de usuario, aunque el código alfanumérico es preferible por claridad, este no permite una respuesta directa (doble vía) en la mayoría de los terminales, lo cual limita casos de uso interactivos. Por todo lo anterior, **TELEFÓNICA** sugiere un esquema híbrido donde la exclusividad sea la norma, pero se permitan modelos compartidos estrictamente controlados para empresas de menor tamaño, siempre bajo la responsabilidad del agregador.

TIGO

Considera que esta alternativa es la más propicia para mitigar el fraude a través de mensajes de texto. Entre los beneficios indica que:

- Permite identificar claramente el agregador (asignatario del código) y la marca que está lanzando cada campaña.
- El agregador podría implementar firewall para bloquear tráfico que no corresponda con la URL reportada por la marca a la que le pertenecería el código corto o numeración E.164.
- Se puede implementar la obligación KYC a los agregadores.

- No requiere establecer un acuerdo contractual con un tercero para la validación de los mensajes, evitando costos por este concepto.
- Como se daría continuidad a la metodología de configuración de recursos de red actual, su implementación no sugiere complejidades técnicas.
- Este tipo de numeración permite configurar texto para que el usuario pueda identificar su remitente.
- Se podría habilitar a los PRST la suspensión temporal del código corto con tráfico sospechoso.

RESPUESTA CRC:

De los comentarios recibidos se observa un consenso en que la asignación exclusiva de recursos de identificación por marca fortalece significativamente la trazabilidad del tráfico SMS A2P, al permitir una atribución más clara del originador, facilitar la investigación de eventos fraudulentos y eliminar la ambigüedad derivada del uso compartido de códigos. Asimismo, se reconoce su potencial para reforzar la confianza de los usuarios en el canal y mejorar el reconocimiento de marca.

No obstante, los operadores coinciden en señalar que esta medida no constituye un mecanismo antifraude autónomo, en la medida en que su efectividad depende de la existencia de procesos robustos de validación del asignatario, controles sobre el uso del recurso, acciones correctivas frente a incumplimientos y mecanismos complementarios de monitoreo del contenido y del comportamiento del tráfico. En ausencia de estos elementos, la exclusividad podría generar una falsa sensación de seguridad sin mitigar plenamente el riesgo de suplantación.

Desde el punto de vista técnico y competitivo, algunos agentes advierten que la migración hacia esquemas de exclusividad podría implicar ajustes operativos relevantes en redes y plataformas, así como eventuales barreras de entrada para empresas de menor tamaño si los procesos de asignación no son ágiles y proporcionales. También se identifican limitaciones funcionales asociadas a ciertos identificadores, como restricciones en comunicaciones bidireccionales.

En este sentido, la CRC considera que los aportes recibidos constituyen insumos relevantes para evaluar, en el marco del Análisis de Impacto Normativo, la proporcionalidad de esta alternativa, su complementariedad con otras medidas de control y trazabilidad, y la necesidad de diseñar esquemas de implementación que mitiguen riesgos competitivos y operativos.

- *¿Qué efectividad considera que tendría la obligatoriedad de usar identificadores alfanuméricos únicos (Sender ID) en todos los mensajes de texto que reciban los usuarios, de cara a la confianza en el canal y la prevención del fraude?*

ASOBANCARIA

Advierte que la obligatoriedad de usar Sender ID únicos puede contribuir a reducir la suplantación y fortalecer la confianza en el canal SMS, siempre que se implemente de forma articulada con los demás controles propuestos. Sostiene que, de manera aislada, su efectividad sería limitada, por lo que resulta más adecuada como parte de un enfoque integral de mitigación del fraude.

CLARO

Considera que pueda que tenga una baja efectividad, pero podría mejorar la transparencia y la trazabilidad del origen, y la percepción de seguridad en el canal A2P, No obstante, expone que deber ser necesaria hacer una evaluación de impacto normativo para validar si es viable, y que en todo caso debe establecerse en la regulación que el encargado de cumplir con el requerimiento es el PCA/IT, quien es el dueño del código corto, y por ende el que conoce el contenido del mensaje que se va remitir.

Insiste, en que antes de implementar una medida (i) evalúe formalmente la efectividad de la suspensión provisional y determine si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia. Destaca que el problema se solucionó con la suspensión provisional por parte de la CRC cuando inicia una actuación administrativa.

TELEFÓNICA

Opina que la medida sería altamente efectiva para mitigar la suplantación de identidad (spoofing) en el canal de mensajería empresarial. E su opinión, el hecho de estandarizar el uso de sender ID únicos y validados reduce drásticamente la superficie de ataque para los delincuentes que aprovechan la falta de estandarización para hacerse pasar por entidades bancarias o gubernamentales. No obstante, **TELEFÓNICA** advierte que la medida debe ir acompañada de procesos de validación rigurosos en el origen (a cargo de los agregadores) que impidan que un actor no autorizado registre un identificador similar al de una marca reconocida.

TIGO

Señala que Esta identificación del remitente si bien puede generar confianza en el usuario, también se corre el riesgo de una falsa sensación de legitimidad. Por ello, se sugiere que esta medida este acompañada de la medida de asignación de un único código corto o numeración E.164 por marca para que pueda tener efectos positivos en la prevención del fraude.

RESPUESTA CRC:

De los comentarios recibidos se evidencia un consenso general en que la obligatoriedad de utilizar identificadores alfanuméricos únicos (Sender ID) puede contribuir positivamente a fortalecer la confianza de los usuarios en el canal SMS y a mejorar la trazabilidad del originador del mensaje, en la medida en que facilita la identificación visible de la entidad emisora y reduce escenarios de ambigüedad propios del uso de identificadores compartidos. En particular, varios agentes coinciden en que esta medida puede limitar prácticas de suplantación de identidad (spoofing), mejorar la transparencia del canal A2P y reforzar la percepción de seguridad por parte de los usuarios.

No obstante, también se observa una coincidencia relevante en que la medida, aplicada de manera aislada, tendría una efectividad limitada frente al fenómeno del fraude. En efecto, los comentarios señalan que el uso obligatorio de Sender ID únicos no elimina por sí mismo el riesgo de suplantación

si no se acompaña de mecanismos robustos de validación del titular del identificador, controles sobre el registro de marcas similares, esquemas de trazabilidad integral del tráfico y medidas correctivas frente al uso indebido, lo cual también se identificó en el uso exclusivo de códigos cortos o numeración E.164 como recurso de identificación para el envío de SMS A2P. Asimismo, se advierte que podría generarse una falsa sensación de legitimidad en los usuarios si no existen controles complementarios que garanticen la autenticidad del remitente.

Desde el punto de vista operativo y regulatorio, algunos agentes destacan la necesidad de que cualquier obligación en esta materia delimite claramente el sujeto responsable de su implementación, particularmente PCA e integradores tecnológicos como titulares del recurso de identificación, y que su adopción esté precedida por un análisis de impacto normativo que evalúe su proporcionalidad, costos y beneficios frente a las herramientas actualmente vigentes. En este sentido, en la respuesta a la consulta se resalta la importancia de evaluar la eficacia de medidas existentes de control y suspensión de recursos antes de introducir nuevas cargas regulatorias.

En consideración de lo anterior, la CRC reconoce que la obligatoriedad del uso de Sender ID únicos constituye un mecanismo que puede aportar a la gobernanza del recurso de identificación y a la mejora de la trazabilidad del tráfico A2P, pero cuya efectividad como herramienta antifraude depende de su articulación con otras medidas técnicas, operativas y de supervisión. Por tanto, su pertinencia será evaluada de manera integral en el marco del AIN, considerando criterios de proporcionalidad, complementariedad regulatoria, cargas operativas y efectos sobre la competencia y la innovación.

- *¿Considera que una eventual limitación del uso de Sender ID alfanumérico a mensajes transaccionales reduciría costos de implementación, o por el contrario contribuiría a desaprovechar la posibilidad de poder generar un mecanismo en el que los usuarios puedan identificar a todos los originadores de contenidos de manera clara?*

ASOBANCARIA

Considera pertinente que el uso de Sender ID aplique a todas las categorías de mensajes SMS y no solo a los transaccionales, dado que los mayores niveles de fraude se concentran actualmente en mensajes comerciales o publicitarios. Sostiene que limitarlo únicamente a mensajes transaccionales podría generar brechas que faciliten prácticas fraudulentas, mientras que su aplicación transversal fortalecería la identificación del remitente, la trazabilidad y la protección del usuario.

CLARO

Expone que existen medidas que son de más bajo costo en la implementación, que logran mejores resultados frente al problema, no obstante, reconoce que podría mejorar la transparencia y la trazabilidad de origen, y la percepción de seguridad del canal A2P.

Recalca que, en ese escenario, el encargado de cumplir con el requerimiento debe ser el PCA/IT, quien es el dueño del código corto, y que conoce el contenido que se va a remitir.

Solicita a la CRC que, antes de implementar la medida propuesta, evalúe formalmente la efectividad de la suspensión provisional y compruebe si queda un problema residual; fortalezca procesos de recuperación ágiles, reglas claras sobre reincidencia y mayor articulación sectorial; y realice un AIN para confirmar que persiste un nivel de fraude que no puede controlarse con las herramientas actuales.

Solo si el AIN lo demuestra tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Concluyen que, por los retos y el tiempo requerido, la medida no es viable ahora, especialmente porque la suspensión provisional ya ha resuelto gran parte del problema

PTC

Indica que el código corto debe ser único para cada marca, como mecanismo para ayudar a los usuarios a identificar a los originadores de manera clara.

TELEFÓNICA

Considera que limitar el uso de identificadores alfanuméricos exclusivamente a mensajes transaccionales sería contraproducente. En concreto, opina que esa fragmentación podría generar confusión en el usuario, quien tendría que aprender a interactuar con dos estándares distintos (alfanuméricos para bancos, numéricos para promociones) dentro de su misma bandeja de entrada. Añade que restringir esta funcionalidad podría desincentivar el uso del canal SMS legítimo frente a aplicaciones OTT, donde la identificación de marca es estándar. Por lo anterior, sugiere que la estrategia más efectiva es permitir y promover el uso generalizado de identificadores claros para todo tipo de tráfico A2P, asegurando que el costo de dicha implementación sea asumido por el mercado corporativo que se beneficia de la identidad de marca, y no subsidiado por los operadores de red.

TIGO

Sugiere no implementar desarrollos para la inclusión de los mecanismos de validación por el uso de un Sender ID.

RESPUESTA CRC:

De los comentarios recibidos se identifican posturas divergentes respecto a la conveniencia de limitar el uso de identificadores alfanuméricos (Sender ID) únicamente a mensajes transaccionales. Por una parte, algunos agentes señalan que la aplicación transversal del Sender ID a todas las categorías de mensajes permitiría fortalecer la identificación clara de los originadores, mejorar la trazabilidad del tráfico A2P y reducir espacios de suplantación, especialmente considerando que una proporción significativa del fraude se concentra en mensajes promocionales o comerciales. Asimismo, se advierte que la coexistencia de esquemas diferenciados de identificación podría generar confusión en los usuarios y debilitar el efecto de señalización del remitente, además de restar competitividad al canal SMS frente a servicios OTT donde la identificación de marca es uniforme.

Por otra parte, algunos operadores indican que la implementación generalizada de esta medida implicaría costos técnicos y operativos relevantes, por lo que sugieren priorizar herramientas de menor costo que puedan generar impactos equivalentes en la mitigación del fraude. En este sentido, se resalta la necesidad de que cualquier obligación regulatoria esté precedida por la evaluación de la eficacia de mecanismos actualmente vigentes, particularmente las medidas de suspensión provisional de recursos de identificación, así como por un análisis de impacto normativo que permita determinar la existencia de un problema residual que justifique nuevas cargas regulatorias. Al respecto, es importante señalar que este tema fue abordado en la respuesta brindada por esta Comisión en la sección 8.2.3, específicamente en lo relacionado a la subtemática 3. De igual forma, se enfatiza que,

en caso de adoptarse obligaciones asociadas al uso de Sender ID, la responsabilidad de su implementación debería recaer en los PCA e integradores tecnológicos, en su calidad de titulares y administradores del contenido de los mensajes.

En atención a lo anterior, la CRC observa que la decisión entre un esquema limitado a mensajes transaccionales y uno de aplicación general implica un balance regulatorio entre eficiencia económica, simplicidad operativa y efectividad en términos de señalización al usuario y trazabilidad del tráfico. Mientras un esquema limitado podría reducir cargas de implementación, también podría fragmentar la experiencia del usuario y mantener espacios de riesgo en segmentos relevantes del tráfico; en contraste, un esquema generalizado podría fortalecer la coherencia del sistema de identificación, aunque con mayores costos y exigencias operativas.

En este sentido, la CRC considera que los aportes recibidos constituyen insumos relevantes para evaluar, en el marco del AIN, la proporcionalidad de la medida, su alcance óptimo de aplicación, los costos diferenciales entre esquemas regulatorios y su complementariedad con otros mecanismos de prevención y control del fraude. Por tanto, la pertinencia de limitar o generalizar el uso del Sender ID será valorada integralmente bajo criterios de eficiencia regulatoria, impacto competitivo, experiencia de usuario y efectividad antifraude.

- *¿Qué criterios considera relevantes para definir patrones atípicos en el tráfico SMS P2P? ¿Cómo se podría evitar afectar a usuarios legítimos?*

ASOBANCARIA

Opina que, para identificar patrones atípicos en el tráfico SMS P2P, son relevantes variables como la velocidad y frecuencia de envío, el volumen y número de destinatarios, la presencia y características de URLs, la repetición de contenidos, la antigüedad de la línea o código originador y el nivel de confianza del originador. A su juicio, la evaluación conjunta de estos criterios permite detectar usos indebidos del canal sin generar impactos significativos sobre los usuarios legítimos.

CLARO

Expone como criterios para identificar patrones atípicos incluyen la detección de volúmenes inusuales por unidad de tiempo, un número elevado de mensajes enviados por línea en intervalos cortos, y distribuciones geográficas anómalas. También se consideran indicativos de comportamiento atípico los envíos masivos hacia destinos internacionales no habituales para el usuario o, en el caso de mensajes entrantes, provenientes de destinos internacionales. Otros factores incluyen un alto número de destinatarios únicos en periodos breves, la actividad en horarios no convencionales y la aparición de picos de envío en horas atípicas.

TELEFÓNICA

Sostiene que los criterios técnicos más relevantes para detectar tráfico atípico o granjas de SIM (SIM farms) incluyen:

(i) la dispersión de destinatarios (un solo número enviando a cientos de destinos únicos en un periodo corto);
(ii) la velocidad de envío (rate limit) superior a la capacidad humana de digitación;

(iii) el uso de dispositivos con IMEI estáticos asociados a múltiples IMSI (rotación de tarjetas SIM); y
(iv) la ubicación fija en celdas con comportamiento de tráfico inusual.

Añade que, para evitar afectar a usuarios legítimos, es fundamental establecer umbrales dinámicos que se adapten a los perfiles de consumo promedio y no aplicar bloqueos definitivos inmediatos. Al respecto, propone un esquema de suspensión temporal con redirección a un portal cautivo o envío de un mensaje de advertencia, permitiendo al usuario legítimo validar su identidad y reactivar su servicio mediante un proceso de autenticación reforzada.

TIGO

Señala que los criterios atípicos a un uso habitual de una persona podrían tipificarse en estas dos modalidades:

- Criterios por dispersión: cuando un mismo usuario origina una cantidad inusualmente alta de mensajes dirigidos a múltiples destinatarios distintos
- Criterios por ventada de tiempo: cuando se registran volúmenes elevados de envíos concentrados en una ventana temporal corta

RESPUESTA CRC:

A partir de los comentarios recibidos se observa una convergencia técnica significativa respecto a los criterios que permitirían identificar patrones atípicos en el tráfico SMS P2P, orientados a distinguir usos legítimos de posibles comportamientos automatizados o fraudulentos. De manera transversal, los agentes coinciden en que el análisis debe basarse en variables de comportamiento asociadas a volumen, frecuencia, dispersión de destinatarios y temporalidad de los envíos, destacándose elementos como: tasas de envío superiores a patrones humanos normales, concentración de mensajes en ventanas de tiempo reducidas, envío masivo a múltiples destinatarios únicos, actividad en horarios atípicos, distribuciones geográficas inusuales y picos de tráfico inconsistentes con el perfil histórico del usuario.

Adicionalmente, algunos operadores resaltan criterios técnicos avanzados que permiten identificar esquemas organizados de fraude, como la rotación de tarjetas SIM asociadas a un mismo dispositivo (SIM farms), el uso de equipos con identificadores estáticos (IMEI) vinculados a múltiples líneas, y patrones de localización celular que evidencian comportamientos automatizados. Otros agentes subrayan la relevancia de evaluar elementos de contenido como la inclusión de URLs sospechosas, la repetición sistemática de mensajes y el nivel de confianza asociado al originador.

En cuanto a la protección de usuarios legítimos, existe coincidencia en que la aplicación de controles debe sustentarse en enfoques de análisis probabilístico y umbrales dinámicos ajustados a los perfiles normales de consumo, evitando bloqueos definitivos inmediatos. En este sentido, se proponen mecanismos de gestión gradual del riesgo tales como suspensiones temporales, notificaciones preventivas, autenticación reforzada del usuario y validaciones posteriores que permitan restablecer el servicio cuando se trate de actividades legítimas.

Con base en lo anterior, la CRC identifica que los aportes recibidos proporcionan criterios técnicos relevantes para estructurar esquemas de monitoreo de tráfico P2P basados en analítica de comportamiento, gestión del riesgo y medidas proporcionales de control, los cuales serán considerados para la estructuración y el análisis de alternativas regulatoria descritas en la sección 9.2.1.3 más adelante que trata sobre la subtemática asociada a la «Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados».

- *¿Qué ventajas y desventajas identifica en la imposición de un límite máximo de SMS P2P por usuario? ¿Qué umbrales serían razonables?*

ASOBANCARIA

Indica que la principal ventaja es garantizar el uso legítimo del canal y mitigar el fraude. Añade que los umbrales específicos podrían definirse por los PRST, considerando los usos habituales del servicio.

CLARO

Expone que esta medida es técnicamente y jurídicamente desproporcionada, vulnera la neutralidad tecnológica al imponer configuraciones de red que limitan la gestión eficiente de las plataformas; afecta la intervención mínima y la regulación eficiente al aplicar restricciones generalizadas que impactan a todos los usuarios sin ser el mecanismo más eficaz; deteriora los derechos de los usuarios al generar bloqueos automáticos en servicios ilimitados; y desalienta la inversión e innovación al exigir desarrollos técnicos costosos que desvían recursos de soluciones más focalizadas y efectivas contra el fraude, comprometiendo la eficiencia y sostenibilidad del sector TIC prevista en la Ley 1341.

TELEFÓNICA

Comenta que la principal ventaja de establecer límites técnicos es la contención inmediata del abuso de planes ilimitados para fines comerciales o fraudulentos, protegiendo la integridad de la red y el modelo económico del servicio. Por su parte, advierte que la desventaja radica en la posible afectación a usuarios con patrones de uso intensivo pero legítimo.

Frente a los umbrales, opina que estos no deben ser fijados de manera rígida por la regulación, ya que los patrones de consumo evolucionan. Por lo tanto, sugiere que la norma faculte a los operadores para definir y actualizar estos límites en sus políticas de uso justo (fair use policy), comunicándolos transparentemente en los contratos. Concretamente, dice que en umbral razonable debería estar basado en el análisis estadístico del percentil 95 o 99 del tráfico de usuarios residenciales, garantizando que la inmensa mayoría de los clientes no se vea impactada.

TIGO

Señala que la regulación vigente ya habilita a los PRST para implementar herramientas tecnológicas orientadas a la prevención del fraude. En ese sentido, consideramos que la medida debería propender por reconocer de manera expresa en el marco regulatorio la facultad de bloquear numeración que evidencie patrones de uso compatibles con conductas asociadas a actividades fraudulentas.

RESPUESTA CRC:

De los comentarios recibidos se identifican posiciones diferenciadas frente a la imposición de límites máximos de SMS P2P por usuario, las cuales permiten evidenciar un debate regulatorio entre la necesidad de prevenir usos indebidos del canal y la protección de los derechos de los usuarios legítimos.

Por una parte, algunos agentes reconocen que la fijación de límites técnicos puede contribuir a mitigar el uso abusivo de planes ilimitados con fines comerciales o fraudulentos, al introducir un mecanismo de contención inmediata frente a comportamientos atípicos que afectan la integridad de la red y el modelo económico del servicio. Asimismo, se plantea que la definición de umbrales podría basarse en criterios estadísticos asociados a patrones reales de consumo, de modo que se preserve el uso legítimo del canal por parte de la gran mayoría de los usuarios.

No obstante, otros operadores advierten que la imposición regulatoria de límites rígidos podría generar efectos adversos relevantes. En particular, se señala que una restricción generalizada puede resultar desproporcionada frente al objetivo perseguido, afectar la experiencia de usuarios con patrones intensivos legítimos, interferir en la gestión técnica eficiente de las redes y desincentivar inversiones en soluciones tecnológicas más focalizadas. Asimismo, se resalta que este tipo de medidas podría implicar desarrollos técnicos costosos y trasladar cargas regulatorias innecesarias cuando ya existen facultades para gestionar riesgos mediante herramientas de monitoreo y control basadas en analítica de comportamiento.

En cuanto a la definición de umbrales, se observa coincidencia en que estos no deberían establecerse de manera estática o uniforme en la regulación, dado que los patrones de consumo evolucionan y varían entre segmentos de usuarios. En este sentido, se propone que los operadores puedan definir límites dinámicos sustentados en análisis estadísticos del comportamiento del tráfico, incorporándolos en sus políticas de uso justo y comunicándolos de manera transparente a los usuarios.

Adicionalmente, algunos comentarios resaltan que el marco regulatorio vigente ya contempla herramientas que permiten bloquear tráfico asociado a patrones compatibles con actividades fraudulentas, por lo que la discusión regulatoria podría orientarse a reforzar el reconocimiento expreso de dichas facultades en lugar de imponer topes cuantitativos generalizados.

En consideración de lo anterior, la CRC identifica que los aportes recibidos constituyen insumos relevantes para el proceso de evaluación de alternativas, tales como la proporcionalidad, eficacia y necesidad de eventuales límites regulatorios al tráfico SMS P2P, así como para analizar alternativas basadas en enfoques de gestión del riesgo más flexibles y focalizados, como el monitoreo de tráfico.

En este sentido, estas consideraciones se encuentran reflejadas tanto en la descripción de alternativas regulatorias contenidas más adelante en la sección 9.2.1.3 más adelanteque trata sobre la subtemática asociada a la «Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados», como en su respectiva evaluación, contenida en la sección 9.2.1.3.4.

- *¿Qué mecanismos de colaboración entre agregadores, operadores y autoridades considera que pueden implementarse para que la detección, prevención y judicialización de fraudes sea más efectiva?*

ASOBANCARIA

Indica que, para una detección y judicialización más efectiva del fraude, se requieren mecanismos de colaboración intersectorial que articulen a agregadores, operadores, entidades financieras y conglomerados comerciales. Adiciona que estos esquemas deben operar bajo una gobernanza clara, liderada por la autoridad regulatoria nacional, que facilite el intercambio de información, la identificación de patrones y la coordinación con las autoridades competentes para la investigación y sanción de las conductas fraudulentas.

CLARO

Propone que la validación en tiempo real referente al contenido del mensaje, como procedimiento a aplicar, que cuando un sistema tecnológico evidencie un posible mensaje fraudulento, solicite la validación del mismo con su remitente, y ponga en copia a la CRC, con el fin de que esta esta alerta a la respuesta del PCA o IT y, en caso de que no se presente una respuesta oportuna, dentro de las dos (2) horas siguientes a la validación de la veracidad del contenido, sugiere que se permita el bloqueo del mismo, y que la CRC inicie actuación administrativa de recuperación del código, con la orden de suspensión provisional del mismo.

PTC

Propone un esquema de colaboración basado en una plataforma de intercambio de información en tiempo real con base de datos compartida para reportar fraudes, alertas tempranas automatizadas, protocolos unificados de respuesta, procedimientos estandarizados para bloqueo, suspensión y notificación a usuarios, manuales operativos comunes, una mesa técnica interinstitucional y reuniones periódicas para análisis y actualización. Adicionalmente, plantea integrar entes judiciales y organismos de control con mecanismos de comunicación clara y efectiva, y apoyo coordinado entre áreas antifraude.

TELEFÓNICA

Opina que la colaboración debe centrarse en el intercambio ágil de inteligencia de amenazas y no en la centralización burocrática de procesos. Propone la creación de mesas de trabajo operativas permanentes donde se compartan, mediante protocolos seguros y automatizados (APIs), los listados de sender IDs, URLs y patrones de tráfico identificados como maliciosos. Para este operador es importante un marco que permita a los operadores compartir evidencias técnicas con las autoridades judiciales (Fiscalía y Policía) de manera expedita para soportar investigaciones penales, sin infringir las normas de protección de datos personales. En su opinión, la efectividad de la judicialización depende de que la evidencia técnica preservada por los operadores pueda ser entregada y procesada con celeridad por los entes investigadores.

TIGO

Resalta que se debe priorizar la educación y sensibilización de la ciudadanía, de manera que los usuarios cuenten con criterios claros para identificar y evitar campañas de smishing. Agrega que, a partir de las denuncias y reportes, incluidos aquellos presentados por los PRST, las autoridades competentes y, en el marco de sus funciones, la CRC, promuevan procedimientos más expeditos y coordinados que permitan adelantar las investigaciones y adoptar medidas oportunas en los menores tiempos posibles.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

RESPUESTA CRC:

De los comentarios recibidos se identifica una tendencia en las observaciones que considera que la mitigación efectiva del fraude requiere esquemas de colaboración articulados entre agregadores, operadores, autoridades regulatorias, entidades judiciales y otros actores relevantes del ecosistema digital. En particular, los aportes destacan la necesidad de fortalecer el intercambio oportuno de información sobre eventos de fraude, patrones de comportamiento malicioso y señales de alerta temprana, así como de establecer protocolos coordinados de respuesta que permitan actuar de manera rápida y proporcional frente a incidentes identificados.

Algunos agentes resaltan la conveniencia de desarrollar plataformas compartidas o mecanismos interoperables que faciliten el reporte en tiempo real de campañas fraudulentas, el intercambio de bases de datos sobre identificadores comprometidos, URLs maliciosas y patrones de tráfico sospechoso, así como la estandarización de procedimientos operativos para el bloqueo preventivo de comunicaciones y la notificación a usuarios potencialmente afectados. De igual forma, se propone la creación de espacios técnicos permanentes de coordinación interinstitucional que permitan el análisis conjunto de comportamientos irregulares, la actualización de tipologías de fraude y la mejora continua de los protocolos de actuación.

Adicionalmente, varios comentarios subrayan la importancia de fortalecer la articulación con las autoridades judiciales y de control, mediante mecanismos que faciliten el suministro expedito de evidencia técnica preservada por los operadores, garantizando simultáneamente el cumplimiento de las normas de protección de datos personales. En este sentido, se reconoce que la eficacia de la judicialización depende no sólo de la detección oportuna del fraude, sino también de la trazabilidad de la evidencia y de la capacidad de las autoridades para procesarla de manera ágil.

Por otra parte, algunos actores enfatizan que la colaboración debe incluir mecanismos preventivos orientados a la educación y sensibilización de los usuarios, de modo que estos puedan identificar señales de riesgo y reducir su exposición a esquemas de fraude, complementando así las acciones tecnológicas y de supervisión institucional.

En consideración de lo anterior, la CRC observa que los aportes recibidos convergen en la necesidad de adoptar esquemas de cooperación interinstitucional que prioricen el intercambio ágil de información, la coordinación operativa y la estandarización de protocolos de respuesta, evitando cargas administrativas innecesarias y promoviendo una gestión del riesgo basada en evidencia.

8.2.5 Sobre las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

8.2.5.1 Comentarios generales en el contexto de las medidas asociadas al servicio tradicional de voz móvil

ANDI

La agremiación advierte que las medidas tecnológicas propuestas para mitigar el contacto fraudulento por voz hacen parte de un paquete de obligaciones potencialmente costosas y complejas, cuya conveniencia no puede asumirse sin una evaluación formal. En esa medida, la **ANDI** insiste en que el AIN debe determinar, para el conjunto de medidas asociadas a la mitigación del fraude por voz, si son técnica y económicamente viables, si resultan realmente necesarias frente a herramientas ya existentes, y si su diseño cumple criterios de proporcionalidad y eficiencia. Complementariamente, reitera la conveniencia de contar con una habilitación clara para bloquear llamadas, incluidas nacionales e internacionales, cuando se evidencie posible fraude, como mecanismo preventivo orientado a proteger al usuario mientras se esclarecen los hechos.

CCIT

Indica que, dentro del diseño regulatorio, debería permitirse el bloqueo preventivo de llamadas (nacionales e internacionales) cuando existan indicios de posible fraude. La **CCIT** presenta esta solicitud como parte de un paquete de herramientas preventivas que deberían poder activarse para proteger a los usuarios, en paralelo a la evaluación de medidas más estructurales y costosas que puedan requerir implementación sectorial y coordinación técnica compleja.

Respuesta de la CRC:

Con respecto a la observación presentada por la **ANDI** acerca de obligaciones potencialmente costosas y complejas, o cuya viabilidad técnica y económica debe ser revisada, en la nueva versión de las alternativas regulatorias para las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz se ha tomado en consideración dicha observación, incluyendo el costo de implementación o el nivel de complejidad técnica, en función del grado actual de evolución tecnológica de las interconexiones nacionales e internacionales de los servicios de voz en el país, como elementos fundamentales para la evaluación de las alternativas regulatorias.

En cuanto a la observación de la **ANDI** y la **CCIT** respecto al bloqueo preventivo de llamadas nacionales e internacionales, cuando se evidencie posible fraude, en esta nueva propuesta se ha mejorado la redacción en la reformulación de las alternativas, para indicar los casos y las circunstancias en los cuales los PRST tendrán la posibilidad de bloquear llamadas nacionales e internacionales, cuando se evidencie posible fraude.

8.2.5.2 Subtemática 1: Mecanismos de verificación, autenticación e identificación del originador de la llamada de voz, o limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)

ANDESCO

Destaca las consideraciones de viabilidad técnica sobre la alternativa de implementación de STIR/SHAKEN/RCD. Señala que no se trata de una simple actualización de software y que su efectividad depende de que las redes e interconexiones operen de forma 100% IP (SIP), ya que en interconexiones TDM la «firma» puede perderse, haciendo ineficaz la inversión si no hay una migración tecnológica previa y coordinada. En ese sentido, solicita que el AIN incorpore explícitamente estos

condicionantes de red, para evitar mandatos que resulten incompletos o no ejecutables de manera interoperable a nivel sectorial, especialmente cuando se pretendan soluciones que descansen en autenticación técnica del identificador de llamada.

Adicionalmente, **ANDESCO** enfatiza que, cuando las alternativas contemplen bloqueo, marcación o etiquetado de llamadas (p. ej., advertencias al usuario como o «probable fraude»), la CRC debería definir criterios claros y verificables que habiliten estas acciones de mitigación sin dejar espacio a discrecionalidad abierta o a algoritmos no homologados, por los riesgos de reclamos masivos y afectaciones a comunicaciones legítimas. De manera convergente con lo anterior, **ANDESCO** solicita una facultad expresa y un «puerto seguro» regulatorio para que los PRST puedan bloquear preventivamente numeración, códigos o incluso tráfico de voz internacional (LDI) cuando existan patrones técnicos o reportes consistentes de fraude, sin que ello sea interpretado como obstrucción o denegación indebida del servicio, priorizando la protección inmediata del usuario mientras se surten verificaciones y/o actuaciones posteriores.

ASOBANCARIA

Identifica un riesgo estructural elevado en el canal de voz, asociado a la suplantación, el enmascaramiento de numeración y el uso creciente de inteligencia artificial generativa para la clonación o imitación de voz.

En este contexto, considera necesario que las alternativas regulatorias incluyan mecanismos técnicos obligatorios de autenticación del origen, tales como STIR/SHAKEN complementados con Rich Call Data, así como la creación de registros de numeración autorizada para llamadas asociadas a servicios financieros.

No obstante, advierte que la autenticación del CLI, por sí sola, no resulta suficiente, dado que el fraude puede ser ejecutado por usuarios legítimos con intenciones fraudulentas. Por ello, propone complementar estos mecanismos con análisis de comportamiento del tráfico de voz, detección de patrones anómalos y uso de herramientas basadas en inteligencia artificial.

De igual forma, **ASOBANCARIA** resalta la importancia de fortalecer la resiliencia frente a ataques asociados a la explotación de protocolos de señalización, mediante la implementación de firewalls especializados para SS7/SIGTRAN, reglas de filtrado, rate limiting, validación de Global Title, auditorías periódicas y pruebas de penetración sobre interconexiones internacionales, con el fin de mitigar riesgos sistémicos asociados al fraude por voz. La adopción conjunta de estos controles técnicos con acciones orientadas a la educación del usuario, en opinión de **ASOBANCARIA**, puede contribuir a una mayor comprensión y efectividad de los cambios regulatorios propuestos.

ASOMÓVIL

Identifica el spoofing de la identidad de la línea llamante como una de las principales fuentes de fraude en el canal de voz, especialmente a través de tráfico internacional que aparenta ser de origen nacional. En este contexto, si bien reconoce la relevancia de alternativas como STIR/SHAKEN, advierte que su implementación implica altos costos de inversión y operación, y que su efectividad depende de condiciones técnicas que actualmente no están dadas de forma generalizada en Colombia ni en la cadena internacional de interconexión. En consecuencia, considera que imponer estas obligaciones sin un AIN previo puede generar cargas desproporcionadas para los PRST.

CLARO

Identifica el spoofing de numeración como una de las principales fuentes de fraude en el canal de voz, especialmente mediante llamadas internacionales que utilizan CLI nacional. En este contexto, apoya la prohibición del uso de numeración nacional en llamadas internacionales, con excepción de escenarios legítimos como el roaming.

El operador considera que esta medida es técnicamente viable y de rápida implementación, siempre que se exija a los operadores de LDI y carriers internacionales el cumplimiento estricto de los estándares UIT E.164, y se establezcan consecuencias regulatorias para quienes permitan el enmascaramiento.

Frente a la alternativa de etiquetado de llamadas como «no verificadas» o «probable fraude», **CLARO** manifiesta que su efectividad es limitada, pues los usuarios tienden a ignorar las alertas y persiste el riesgo de falsos positivos que afectan la experiencia del servicio.

Respecto a STIR/SHAKEN y RCD, el operador considera que su implementación no es viable en el corto plazo, debido a la complejidad de interoperabilidad, los altos costos y la coexistencia de redes no IP.

HABLAME

Reconoce el spoofing dentro de las modalidades de fraude observadas en el ecosistema y acepta que el fenómeno también se materializa por voz, sin embargo sostiene que es necesario prevenir que el diseño regulatorio derive en habilitaciones para que agentes privados filtren o bloqueen comunicaciones con criterios subjetivos, por lo que sugiere privilegiar un enfoque de articulación institucional y decisión imparcial (como el modelo propuesto con COLCERT) para minimizar errores y abusos, protegiendo tanto al usuario como la legitimidad del mercado.

PTC

Respalda la prohibición total del enmascaramiento del CLI, especialmente para llamadas internacionales entrantes que presenten numeración nacional, al considerarla una medida técnicamente efectiva y necesaria para reducir suplantación de identidad y modalidades como el vishing. Desde la perspectiva de red, plantea que el control se puede materializar mediante reglas claras de enrutamiento y validación de señalización, introduciendo únicamente excepciones controladas en escenarios legítimos (por ejemplo, roaming internacional). En términos de implementación, estima un plazo de seis (6) meses, al tratarse principalmente de ajustes en reglas de enrutamiento y validación.

Complementariamente, al referirse a la prohibición de CLI nacional en llamadas internacionales, **PTC** sugiere que un mecanismo práctico –para no perder capacidad de identificación– es el uso de máscaras o prefijos que permitan reconocer llamadas LDI entrantes cuando, por alguna razón operativa, se presenten con numeración local. Con ello, su preocupación operativa parece orientada a que la red y el usuario cuenten con señales suficientes para discriminar origen y reducir exposición a fraude, sin afectar comunicaciones legítimas por falta de diferenciación.

SFC.

Favorecen autenticación progresiva (STIR/SHAKEN + RCD) con controles complementarios, destacando riesgos de suplantación bancaria y necesidad de interoperabilidad y pilotos

SSC

Plantea que el fraude en llamadas de voz no se origina en la numeración ni en la simple presentación del CLI, sino en la dificultad para identificar y rastrear el origen técnico real de las llamadas, especialmente cuando estas atraviesan múltiples redes, plataformas y operadores.

Con base en su experiencia operativa, **SSC** identifica tres fuentes funcionales de tráfico de voz, cada una con perfiles de riesgo y capacidades de control diferenciadas:

1. Tráfico directo nacional:

Corresponde a llamadas en las que el PRST que presta efectivamente el servicio controla el establecimiento, enrutamiento y terminación de la llamada. En estos escenarios existe plena trazabilidad, bajo riesgo y alta capacidad de auditoría, suspensión y judicialización.

2. Tráfico originado en plataformas OTT / CPaaS:

Incluye llamadas legítimas cursadas desde plataformas globales (contact center y servicios en la nube) que presentan CLI nacional asignado a clientes empresariales, aunque el origen técnico se encuentre en infraestructura internacional. Este tráfico presenta un riesgo intermedio y gestionable, derivado de la disociación entre numeración y origen técnico, pero no debe equipararse automáticamente a fraude.

3. Tráfico internacional en cadena de intermediarios:

Corresponde a llamadas que atraviesan múltiples carriers y redes internacionales, con alta opacidad del origen real, lo que limita la capacidad de los PRST para identificar responsabilidades y aplicar controles directos. Este es el escenario de mayor riesgo.

SSC considera que prohibir de forma generalizada las llamadas internacionales con CLI nacional no resulta eficaz, pues no aborda la causa estructural del fraude y puede bloquear comunicaciones empresariales legítimas, mientras que los actores fraudulentos podrían adaptarse utilizando CLI internacional.

TELEFÓNICA

Respalda el objetivo de erradicar el CLI spoofing, pero advierte que la adopción obligatoria de STIR/SHAKEN y RCD enfrenta limitaciones técnicas estructurales, dado que estos protocolos requieren interconexión IP extremo a extremo (SIP), condición que no se cumple de forma generalizada en Colombia ni en las rutas internacionales.

Solicita que cualquier obligación en esta materia esté condicionada a un análisis de factibilidad técnica real, a un plan sectorial de migración a redes *All-IP* y a un cronograma de transición. Imponer estas

tecnologías sin resolver la brecha de infraestructura implicaría inversiones ineficientes que no se traducirían en protección efectiva al usuario.

TIGO

Identifica el spoofing de numeración como una de las principales modalidades de fraude en el canal de voz, particularmente a través de tráfico internacional que se presenta ante el usuario como numeración nacional. No obstante, advierte que varias de las alternativas propuestas enfrentan limitaciones técnicas relevantes.

Este operador llama la atención enfoque de asignación de responsabilidades a los PRST, sin contemplar la responsabilidad de los carrier en la gestión y control del tráfico que originan, e incluso de establecer para ellos sanciones que motiven la verificación del tráfico que gestionan.

Adicionalmente, señala que resulta técnicamente complejo, costoso o incluso inviable detectar el enmascaramiento de la identidad de la línea llamante en tiempo real, dado que la red recibe la información de terceros que pueden modificar los encabezados de señalización sin que ello sea detectable mediante mecanismos estándar.

Frente a la implementación de STIR/SHAKEN y RCD, **TIGO** reconoce que podrían ser viables en el largo plazo, pero insiste en que su adopción es altamente costosa, depende de la migración generalizada a redes IP y de acuerdos internacionales, y no puede imponerse como una solución inmediata ni universal, ni generar obligaciones exclusivas para los PRST.

U. EXTERNADO

Menciona que la CRC debería fomentar (aunque sin imponer de manera inmediata) la adopción progresiva de STIR/SHAKEN en tramos IP y su extensión Out-of-Band en presencia de segmentos no-IP, de forma coordinada con los operadores y con pruebas piloto sobre roaming, OTT interconectado y call centers. La estandarización 3GPP y ATIS ya contempla APIs y perfiles operativos que facilitan interoperabilidad internacional, reduciendo el spoofing y elevando el grado de atestación. En paralelo, considera que debe mantenerse la armonización con ITU E.164 para integridad del plan de numeración, así como con recomendaciones ITU/ECC contra spoofing que habilitan acciones nacional-internacional.

ZANYA PINEDA

Sostiene que el fraude en servicios de voz no se puede determinar ex ante sin vulnerar privacidad y, por tanto, el reporte del usuario resulta clave. Considera que prohibición absoluta del enmascaramiento puede excluir tráfico legítimo transfronterizo y concentrar el control, por lo que propone el etiquetado informativo y la trazabilidad incremental con responsabilidades distribuidas.

Respuesta de la CRC:

En los comentarios de **ANDESCO**, **CLARO**, **TELEFÓNICA**, **TIGO** y **ASOMÓVIL** se indica que las alternativas relacionadas con la implementación de STIR/SHAKEN/RCD dependen para su efectividad de que las redes e interconexiones operen con base en el protocolo SIP de manera que se cuente con

una interconexión IP extremo a extremo. También señalan que en Colombia todavía existen interconexiones TDM que operan mediante el sistema de señalización SS7 y que una medida orientada al uso de STIR/SHAKEN/RCD, sin que previamente se dé una migración tecnológica coordinada, implicaría inversiones ineficientes que no se traducirían en una protección efectiva al usuario, por lo que su implementación no es viable en el corto plazo.

Al respecto, la investigación realizada por la CRC tanto de las experiencias internacionales, como mediante consultas con fabricantes, coinciden con las observaciones previamente anotadas de los gremios y de los PRST respecto a que la implementación de STIR/SHAKEN/RCD es nativa para redes e interconexiones que operan bajo protocolo SIP con interconexión IP extremo a extremo. En ese orden de ideas, si bien la proporción de las redes móviles que hoy funcionan bajo tecnología IP es sustancialmente mayor a la que funciona bajo tecnologías TDM, también es cierto que todavía existen en la red nacional interconexiones TDM bajo protocolo SS7.

Por su parte, se identificaron también iniciativas técnicas para el uso de *Out of Band* SHAKEN (OOB SHAKEN) para la implementación de STIR/SHAKEN en redes interconectadas bajo SS7, sin embargo, estas actualmente no cuentan con un marco definido de estandarización. Por esa razón, la Comisión considera procedente incluir como elemento fundamental el criterio de costo y el de nivel viabilidad de implementación como elementos críticos en la evaluación de la alternativa STIR/SHAKEN/RCD frente a las demás alternativas regulatorias, entendiendo que su implementación requiere un estado del arte de las redes distinto al actual.

En relación con el comentario de la **U. EXTERNADO** según el cual la CRC debería fomentar la adopción progresiva de estándares como STIR/SHAKEN, incluyendo esquemas Out-of-Band en presencia de segmentos no IP, y coordinar su implementación con operadores mediante pilotos y pruebas de interoperabilidad, esta Comisión se permite señalar que, en consistencia con lo expresado en la sección que trata sobre los «Comentarios generales en el contexto de las medidas asociadas al servicio SMS», se reconoce la utilidad de dichos estándares como marco de referencia técnico, especialmente para el análisis de mecanismos de autenticación de llamadas y de fortalecimiento de la trazabilidad del originador. No obstante, la eventual adopción de este tipo de soluciones debe evaluarse considerando las condiciones técnicas, económicas y regulatorias del entorno nacional, así como la arquitectura actual de las redes, la coexistencia de segmentos IP y no-IP, los requisitos de interoperabilidad internacional y los costos de transición asociados.

Por otra parte, **ANDESCO** presentó comentarios donde solicitan que la propuesta regulatoria defina criterios claros y verificables para las alternativas que contemplen bloqueo, marcación o etiquetado de llamadas. En la misma línea, **HÁBLAME** reconoció el spoofing dentro de las modalidades de fraude observadas en el ecosistema de voz, pero comentó respecto a la necesidad de evitar criterios subjetivos en el filtrado de comunicaciones. **ZANYA PINEDA** indicó que debe evitarse la exclusión de tráfico legítimo transfronterizo.

Al respecto, la CRC está de acuerdo en que los criterios finales de las alternativas regulatorias deben ser claros y objetivos para la determinación de los casos donde se puedan aplicar bloqueos o marcación de llamadas. Esto, con el objetivo de disminuir la probabilidad de cualquier afectación sobre el tráfico de voz legítimo, pero manteniendo el propósito de la intervención regulatoria de mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En tal sentido el comentario de **CLARO**, en el que propone que se dé cumplimiento estricto del estándar UIT-T E.164[38] que establece el plan internacional de numeración de telecomunicaciones públicas, es un buen ejemplo de un criterio claro y objetivo que será utilizado en la definición de las alternativas regulatorias.

Adicionalmente, existe coincidencia en los comentarios de **PTC, CLARO**, **TELEFÓNICA**, **TIGO**, **ASOMÓVIL** y **ASOBANCARIA**, respecto a que modalidades de fraude como spoofing y vishing se dan especialmente en llamadas internacionales entrantes que presentan enmascaramiento del número que realmente originó la llamada mediante el uso de un identificador de línea llamante (CLI) con numeración nacional. En esa medida, se observa que existe acuerdo entre los operadores y el gremio **ASOMÓVIL** respecto a la necesidad de la prohibición total del enmascaramiento del CLI en llamadas internacionales, y la prohibición del uso de numeración nacional como identificación de origen de llamada, salvo en casos legítimos como los de usuarios de servicios móviles en Roaming internacional. La CRC está de acuerdo en la conveniencia de incluir entre las alternativas regulatorias una regla en dicho sentido.

Por su parte, **SSC** identificó tres fuentes funcionales de tráfico de voz.

La primera, asociada con tráfico directo nacional, del cual dijo que corresponde a un escenario donde existe plena trazabilidad, bajo riesgo y alta capacidad de auditoría, suspensión y judicialización. La CRC considera que efectivamente el tráfico de origen nacional dispone de un mayor número de mecanismos de control vistos desde un enfoque reactivo no preventivo que permita evitar el contacto a usuarios con fines fraudulentos en llamadas de voz.

La tercera fuente la denomina SSC tráfico internacional en cadena de intermediarios e indica que puede presentar alta opacidad del origen real. La CRC considera que, efectivamente, es necesario establecer alternativas regulatorias que permitan contar con mejores herramientas para mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz para este tipo de tráfico.

Y en cuanto a la segunda fuente, **SSC** hace referencia a lo que denomina como tráfico originado en plataformas OTT/CPaaS y dice que corresponde a tráfico de voz cursado desde plataformas globales (tales como contact center y servicios en la nube) que hace uso de numeración nacional asignado a clientes empresariales en Colombia. A partir de esa descripción, **SSC** considera que prohibir de forma generalizada las llamadas internacionales con CLI nacional puede bloquear comunicaciones empresariales legítimas.

Al respecto, es importante recordar que, de conformidad con el Decreto 25 de 2002[39], el cual fue compilado en el Decreto Único Reglamentario 1078 de 2015, la CRC es el Administrador del Plan Nacional de Numeración[40] y, en el marco de esa competencia, la asignación de numeración se realiza

[38] Recomendación UIT-T E.164 Plan internacional de numeración de telecomunicaciones públicas (11/2010)
[39] Decreto 25 de 2002 "Por el cual se adoptan los Planes Técnicos Básicos y se dictan otras disposiciones". Ministerio de Comunicaciones.
[40] Artículo 2.2.12.1.2.5. del Decreto 1078 de 2015: **ARTÍCULO 2.2.12.1.2.5. NATURALEZA DE LA NUMERACIÓN.** Los números, bloques de numeración, códigos, prefijos, entre otros, son recursos públicos y pertenecen al Estado, el cual puede asignarlos a los proveedores de redes y servicios de telecomunicaciones y recuperarlos cuando se den las condiciones que

a operadores legalmente habilitados, siendo para el servicio de voz la numeración E.164 el recurso público que pertenece al Estado, definido a partir del estándar internacional establecido por la UIT, con el objetivo primordial de proveer el recurso numérico necesario para acceder unívocamente a todo usuario.

Ahora bien, con respecto a la numeración E.164, esta se clasifica en Colombia como geográfica y no geográfica, estando en esta última categoría la numeración de redes y la numeración de servicios.

El uso de numeración E.164 geográfica tiene como propósito la prestación de servicios en regiones geográficas específicas y el uso de numeración E.164 no geográfica de servicios hace referencia al conjunto de los números asociados a categorías de servicios tales como cobro revertido o tarifa con prima.

A su vez, el uso de numeración E.164 no geográfica de redes constituye el conjunto de los números nacionales (significativos) conformados por indicativos nacionales de destino asociados a redes, por ejemplo, a las redes móviles. En esa medida, las referencias utilizadas por **SSC** respecto a la portabilidad numérica móvil no desvirtúan ni el objetivo ni el propósito del uso de la numeración no geográfica, que es el de proveer el recurso numérico nacional significativo necesario para acceder unívocamente a todo usuario.

Adicionalmente en portabilidad numérica móvil no existe ningún reto de trazabilidad ni tampoco disociación entre numeración y origen técnico de la llamada, dado que se cuenta con una base de datos central de números portados, por lo que siempre se conoce el origen técnico de cualquier numeración no geográfica dentro de la red nacional, lo que facilita el enrutamiento adecuado y contribuye a la trazabilidad regulatoria.

En esa medida, el uso de numeración nacional geográfica o no geográfica de redes o de servicios asignada a Proveedores de Redes y Servicios de Telecomunicaciones legalmente constituidos en Colombia desde plataformas globales, no cumple de antemano con las asignaciones ni con los objetivos dispuestos para el plan nacional de numeración. Lo anterior está dispuesto expresamente en el parágrafo[41] del artículo 6.1.1.5 de la Resolución CRC 5050 de 2016, en el que se establece como una disposición general para los recursos de identificación que los mismos no pueden ser cedidos o transferidos sin una autorización previa y expresa de la CRC. Por tal motivo, la razón expuesta por **SSC** no puede ser invocada como una motivación para evitar el establecimiento de la alternativa regulatoria de bloqueo de llamadas internacionales con CLI que utiliza numeración nacional.

Por otra parte, **SSC** indica que prohibir de forma generalizada las llamadas internacionales con CLI nacional no resulta eficaz, pues no aborda la causa estructural del fraude. A su vez, **ASOBANCARIA**

---

determine la Comisión de Regulación de Comunicaciones para la recuperación de éstos. La asignación de dichos recursos a los operadores no les otorga derecho de propiedad alguno sobre ellos.
Los recursos asignados no podrán ser transferidos por los proveedores de redes y servicios de telecomunicaciones, sin la autorización de la Comisión de Regulación de Comunicaciones.

[41] El parágrafo indicado establece expresamente lo siguiente:
«**PARÁGRAFO.** Los recursos de identificación no pueden ser objeto de venta o comercialización. Tampoco pueden ser cedidos o transferidos, excepto cuando el Administrador de los Recursos de Identificación lo autorice de manera expresa, de oficio o a solicitud de parte, para lo cual el nuevo asignatario deberá cumplir los requisitos de asignación correspondientes.
En el caso de emitirse una autorización expresa de cesión o transferencia de los derechos de uso de los recursos de identificación, el nuevo asignatario adquiere todas las obligaciones sobre los recursos de identificación cedidos o transferidos.»

advierte que la autenticación del CLI, por sí sola, no resulta suficiente, dado que el fraude puede ser ejecutado por usuarios legítimos con intenciones fraudulentas que pueden usar herramientas sofisticadas como la Inteligencia Artificial generativa. La CRC considera que efectivamente pueden darse comportamientos delictivos desde numeración legítima, asunto que debe ser investigado por las autoridades competentes, pero insiste en que el propósito de la medida regulatoria es de mitigación para disminuir las probabilidades del contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz, por medio de medidas técnicas realistas.

A su turno, la CRC coincide con **ASOBANCARIA** en el sentido de indicar que es necesario el fortalecimiento de la resiliencia frente a ataques asociados a la explotación de protocolos de señalización. Lo anterior se logra, entre otros aspectos, mediante las medidas de carácter técnico que la Comisión ha propuesto en el documento de Alternativas Regulatorias, así como con las precisiones que están siendo analizadas en este documento, con el fin de mitigar riesgos sistémicos asociados al fraude por voz. Sin embargo, es importante precisar que, si bien se cuentan con múltiples herramientas para enfrentar este fenómeno, se hace relevante contar con medidas proporcionales que ponderen el beneficio generado por las medidas en su conjunto, así como los costos de implementación que perciben los sujetos obligados a dar respectivo cumplimiento. Adicionalmente, la Comisión advierte que, en línea con lo comentado por **ASOBANCARIA**, en este documento también se analizan una serie de medidas o acciones orientadas a la educación del usuario, que ciertamente contribuyen a una mayor comprensión y efectividad de los cambios regulatorios propuestos.

Frente al comentario de **CLARO** respecto a la posible efectividad limitada de la alternativa de etiquetado de llamadas como «no verificadas» o «probable fraude», la CRC considera que los méritos que pueda tener este comentario deben quedar evidenciados como parte de la evaluación de las alternativas regulatorias.

8.2.5.3 Subtemática 2: Falta de aplicación coordinada de métodos preventivos de filtrado de tráfico de voz

ASOMÓVIL

El gremio sostiene que la mayor parte del riesgo en el canal de voz proviene del tráfico internacional, por lo que cualquier estrategia regulatoria debe incorporar obligaciones claras para los carriers internacionales y operadores de tránsito.

ASOMÓVIL considera que imponer plataformas centralizadas de monitoreo o esquemas complejos de coordinación puede resultar ineficiente, y propone que la regulación enfatice la corresponsabilidad en la cadena internacional, lo que incluya exigencias de verificación de procedencia, pues de otro modo las cargas derivadas de la regulación podrían recaer en forma desproporcionada en los PRSTM, sin que ellos tengan el control sobre el origen de ese tipo de comunicaciones.

CLARO

Sostiene que no es necesaria la creación de plataformas centralizadas de monitoreo o intercambio de alertas. A su juicio, cada operador de LDI puede gestionar localmente sus mecanismos de detección y, cuando sea necesario, coordinarse con otros operadores mediante esquemas ya existentes.

Advierte que imponer plataformas centralizadas incrementa costos, complejiza la operación y no garantiza una reducción efectiva del fraude si no se asignan responsabilidades claras a los operadores de tránsito internacional.

PTC

Plantea elementos de coordinación para elevar efectividad. En particular, propone mecanismos como alertas tempranas automatizadas, protocolos unificados de respuesta y procedimientos estandarizados para bloqueo o suspensión y notificación, junto con manuales operativos comunes. Adicionalmente, sugiere una mesa técnica interinstitucional con reuniones periódicas para análisis de casos y actualización, y la participación de entes judiciales y organismos de control con integración en tiempo real y comunicación efectiva, apoyada por áreas antifraude de las compañías. Este enfoque refleja una preferencia por esquemas de cooperación operativa que permitan reaccionar con rapidez y coherencia frente a tendencias de fraude.

En la misma línea de gestión diferenciada del riesgo, PTC distingue entre tráfico de voz originado por acuerdos directos con clientes nacionales (bancos, comercios, salud, aerolíneas) y tráfico internacional que llega por cadenas de intermediación. Para gestionar esa diferencia, propone que las entidades legítimas cuenten con una numeración única o máscara que identifique su origen «legal», y que todo lo que quede fuera de ese rango sea marcado como spam o fraude, dejando al usuario la decisión de bloquear. Si bien el planteamiento es sintético, apunta a un criterio de segmentación por «listas de confianza» y una administración del riesgo apoyada en identificación consistente del originador.

SSC

Expone que actualmente aplica mecanismos de monitoreo continúo basados en comportamiento (volúmenes, patrones horarios, destinos y rutas), complementados con coordinación interoperatorial. Ante notificaciones de tráfico anómalo, implementa bloqueos focalizados sobre números o flujos específicos, evitando acciones generalizadas.

Afirma que estas medidas han mostrado una efectividad media a alta, especialmente cuando existe cooperación entre operadores, aunque su alcance se ve limitado por la trazabilidad disponible en tráfico internacional en cadena. En este contexto, SSC considera que los esquemas de filtrado deben priorizar la evidencia técnica, la focalización y la proporcionalidad, reduciendo falsos positivos y preservando servicios legítimos.

TELEFÓNICA

El operador reconoce la utilidad de los esquemas de monitoreo y filtrado basados en métricas de red (CSR, ACD, picos de tráfico), pero enfatiza que una parte significativa del riesgo proviene de tráfico internacional.

Por ello, propone incorporar un enfoque de corresponsabilidad internacional, exigiendo a *carriers* de tránsito y operadores LDI certificar la autenticidad del CLI del tráfico entrante. Afirma que, sin este componente, la carga operativa recaería de manera desproporcionada sobre los PRST nacionales.

TIGO

El operador considera que la imposición de esquemas de monitoreo y filtrado en tiempo real, basados en patrones estadísticos, resulta técnicamente compleja y costosa, y puede perder efectividad rápidamente frente a la adaptación de las modalidades de fraude.

Adicionalmente, resalta que, en el contexto del Statu Quo, la CRC no ha habilitado de manera suficiente a los PRST para ejecutar acciones autónomas de bloqueo o contención, lo que limita la eficacia de los mecanismos de detección existentes. En este sentido, sugiere que esta Comisión debería ampliar en este escenario la posibilidad de los PRSTs de tomar medidas que permitan contener los eventos de fraude.

Solicita el retiro de las medidas propuestas en esta temática, dado que a su parecer ninguna tendría un impacto directo y definitivo en el fin propuesto que es mitigar el fraude cibernético mediante llamadas de voz.

U. EXTERNADO

Menciona que el bloqueo selectivo de tráfico con tasa de establecimiento y distribución de prefijos anómala debe basarse en reglas auditables, listas de reputación dinámicas y mecanismos de traceback; ello exige compartición segura de indicadores (con granularidad adecuada) y regímenes de exención para casos legítimos (por ejemplo, centros de contacto verificados). Las guías ITU/GSMA recomiendan contar con equipos antifraude con capacidad de análisis en tiempo real, y la normativa comparada (FCC) refuerza exigencias de autenticación/registro para proveedores que tercerizan el firmado de llamadas.

ZANYA PINEDA

Exige que cualquier filtrado sea gradual, auditado, con debido proceso y sin inspección de contenido.

Respuesta de la CRC:

En los comentarios de **PTC** se resalta la conveniencia de contar con una entidad de coordinación para elevar la efectividad de las medidas antifraude y en los comentarios de **SSC** se indica que existe mayor efectividad cuando hay cooperación entre los operadores. Ahora bien, sobre ese mismo tema de coordinación y respecto del uso de plataformas centralizadas de monitoreo, tanto **ASOMÓVIL** como **CLARO** plantean que esto no es necesario o incluso que puede resultar ineficiente; y específicamente **CLARO** propone que cuando sea necesario se puede realizar una coordinación con otros operadores mediante esquemas ya existentes.
Por otra parte, **SSC** y **TELEFÓNICA** mencionan la posibilidad técnica de utilización de mecanismos de monitoreo y filtrado de tráfico basados en observación de comportamiento o mediante el uso de métricas de red. Sobre este mismo asunto, **ZANYA PINEDA** resalta que cualquier filtrado que llegue a darse debe ser sin inspección de contenido.

La CRC, una vez analizados estos comentarios, considera que la temática 2 original debe separarse en dos temáticas distintas en aras de aportar claridad a la hora de proceder con la evaluación. La primera que se denominará: «Subtemática 2: Falta de una instancia de coordinación para la articulación y el intercambio de alertas» y la segunda, que se llamará «Subemática 3: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas».

En la nueva temática 2 se incluirá, como parte de las alternativas regulatorias, la posibilidad de contar con una plataforma nacional de alertas centralizada para generar notificaciones en tiempo real a todos los PRST y entidades conectadas, o bien de establecer mecanismos formales de coordinación entre los PRST, agentes en general y la CRC, así como otras entidades (no necesariamente mediante una plataforma).

En la nueva temática 3 se analizarán las alternativas regulatorias para la definición o no de lineamientos para monitoreo y etiquetado de tráfico mediante la identificación de patrones sospechosos. Ahora bien, en cuanto a la nueva temática 3, la CRC considera que el monitoreo y etiquetado de tráfico deben ser incluidos como parte de la evaluación de las alternativas regulatorias, y está de acuerdo en que ningún mecanismo de monitoreo de voz debe basarse en inspección de contenido, lo cual además está en línea con el propósito de mitigar el contacto a usuarios finales con fines fraudulentos mediante los servicios tradicionales de voz, resaltando que esto último implica que los mecanismos de monitoreo y etiquetado se dan antes del establecimiento de la llamada y por tanto en ningún caso implican la inspección del contenido de la comunicación.

TIGO, por su parte, considera que las medidas de monitoreo y filtrado en tiempo real resultan técnicamente complejas y costosas. Al respecto, las alternativas regulatorias que serán estudiadas por la CRC incluirán medidas que habiliten a los PRST para tomar medidas autónomas de bloqueo y contención mediante dos tipos de mecanismos claramente diferenciados: (i) reglas directas y objetivas para los casos donde los PRST podrán hacer bloqueo de llamadas, por ejemplo, mediante el uso de base de datos de DNO (Do Not Originate) como por uso de CLI nacional en llamadas internacionales para casos distintos a Roaming Internacional y la obligación de cumplimiento de la Recomendación UIT-T E.164 para el tráfico internacional entrante; y (ii) reglas de monitoreo y filtrado con propósitos de identificación y etiquetado de llamadas («Alerta de llamada sospechosa» o «Alerta de probable fraude»), usando criterios técnicos como los sugeridos por TIGO y TELEFÓNICA en sus comentarios, por ejemplo: volumen de llamadas por CLI + relación origen – destino o métricas de llamadas que permitan determinar duración promedio de llamadas para identificación de llamadas cortas y repetitivas tales como análisis de ASR (Answer Seizure Rate) + ACD (Average Call Duration). En estos casos se pueden usar umbrales de detección dinámicos que usen técnicas de aprendizaje de máquina.

En el caso de reglas de monitoreo y filtrado con propósitos de etiquetado, se requiere primero de la construcción de una base estadística que permita la formación de un juicio bajo reglas objetivas para después sí proceder con el etiquetado en tiempo real, el cual debe ser confirmado antes de aplicarse y debe ser reversible cuando la evidencia así lo indique.

En otros temas mencionadas en las observaciones, **TELEFÓNICA**, **TIGO** y **ASOMÓVIL** proponen incorporar un enfoque de corresponsabilidad internacional, en el que los *carriers* de tránsito y los operadores de LDI certifiquen la autenticidad del CLI del tráfico entrante. Al respecto, las alternativas regulatorias propuestas por la CRC sólo pueden estar acordes con sus competencias, las cuales tienen

un ámbito de aplicación de orden nacional, o con el uso de estándares en la interconexión entre los PRST nacionales con los *carriers* internacionales.

Frente al comentario realizado por la **U. EXTERNADO,** en donde recomienda algunos mecanismos de bloqueo selectivo de tráfico basados en patrones anómalos, como tasas de establecimiento inusuales o distribuciones atípicas de prefijos, e indica que deberían sustentarse en reglas auditables, listas de reputación dinámicas y mecanismos de traceback, esta Comisión considera pertinente señalar que si bien estas técnicas de detección de fraude son relevantes, su eventual incorporación en el marco regulatorio está sujeta a los resultados del debido proceso de evaluación de alternativas, el cual debe considerar su viabilidad técnica, su proporcionalidad y su compatibilidad con las competencias regulatorias de la Comisión.

Finalmente, en cuanto a los comentarios de **PTC** acerca del uso de numeración única que identifique el origen «legal» del tráfico este asunto se aborda más adelante en la siguiente sección de respuesta a comentarios.

8.2.5.4 Subtemática 3: Ausencia de diferenciación en rangos de numeración para comunicaciones personales, comerciales y publicitarias

CLARO

El operador considera que la creación de rangos exclusivos para llamadas comerciales y publicitarias no resulta eficaz, dado que los usuarios no identifican los indicativos de numeración y la medida no impide el spoofing. A su juicio, esta alternativa introduce cargas regulatorias y operativas sin atacar el problema estructural del fraude y la suplantación.

PTC

Sobre medidas basadas en diferenciación por numeración, **PTC** estima que, una vez creados y definidos rangos específicos E.164, se requerirá aproximadamente un (1) año para una implementación completa. Advierte que la transición implica ajustes en sistemas de tarificación, enrutamiento y señalización, y procesos de migración ordenada de actores que hoy usan numeración no diferenciada. Por ello, ese operador recomienda un esquema de migración gradual, iniciando con nuevos asignatarios y permitiendo un periodo de convivencia con la numeración actual. Este comentario se alinea con la necesidad de implementar cambios de identificación sin generar disrupciones abruptas en operación ni en continuidad del servicio.

SSC

Analiza la creación de rangos exclusivos para llamadas comerciales y publicitarias y concluye que, si bien esta medida puede aportar claridad informativa parcial al usuario, presenta limitaciones estructurales:

- Riesgo de bloqueo generalizado de rangos completos por parte de los usuarios.
- Incentivos a la evasión por parte de actores fraudulentos.

- Costos operativos y de migración para servicios existentes.
- Baja efectividad frente a fraude sofisticado basado en suplantación.

Por lo anterior, SSC considera que la diferenciación de rangos no constituye una solución suficiente ni determinante, y que su eventual adopción solo tendría sentido como medida complementaria dentro de un enfoque integral.

TELEFÓNICA

Considera que la creación de rangos exclusivos para llamadas comerciales presenta beneficios limitados y altos costos de migración, además de no resolver el problema del *spoofing*. Sostiene que resulta más eficaz autenticar quién llama que segmentar la numeración utilizada.

TIGO

Considera que la diferenciación de rangos de numeración para llamadas personales y comerciales sí podría ser técnicamente viable en el mediano plazo y aportar beneficios en términos de experiencia del usuario, trazabilidad y análisis estadístico del tráfico comercial.

No obstante, aclara que esta medida no constituye por sí sola una solución definitiva al fraude, y que su efectividad dependería de su articulación con campañas educativas y de la capacidad de los usuarios para reconocer y comprender dicha diferenciación.

ZANYA PINEDA.

Considera que aporta valor marginal y es evadible, por lo que debe ser una medida complementaria y requiere pedagogía para evitar confusión o fatiga de los usuarios.

Respuesta de la CRC:

TIGO considera que la diferenciación de rangos exclusivos de numeración para llamadas comerciales y publicitarias sí podría ser técnicamente viable y útil para la diferenciación del tráfico, pero aclara que esta medida por sí sola no sería efectiva porque también se requeriría de campañas educativas que les permitan a los usuarios reconocer y entender la diferenciación en el uso de la numeración. A su vez **PTC** recomienda una migración gradual.

Por su parte **SSC, CLARO, TELEFÓNICA** y **ZANYA PINEDA** consideran que la medida no es eficaz y exponen diversos argumentos, por ejemplo, que implica altos costos, puede generar bloqueo generalizado de rangos completos de numeración o migración de los actores fraudulentos hacia otras modalidades de fraude.

En atención a estos comentarios, y dadas las medidas pedagógicas y educativas que se proponen en el numeral 8.2.6 para el servicio de voz y SMS, la CRC considera que la alternativa regulatoria planteada debe ser evaluada incorporando los posibles costos y externalidades señaladas por la industria como criterio fundamental para la valoración de la adopción de la alternativa relacionada con la diferenciación de rangos de numeración para llamadas comerciales y publicitarias.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

8.2.5.5 Subtemática 4: Falta de estandarización en la aplicación de listas de no originación (DNO)

ASOBANCARIA

Señala que se requiere control transversal y coordinado para proteger números que no deben originar llamadas.

CLARO

Considera viable que cada PRST mantenga sus propias listas DNO bajo un estándar mínimo obligatorio definido por la CRC, siempre que estas listas sean manejables, no excesivamente extensas y no requieran actualizaciones dinámicas complejas que afecten el desempeño de las redes.

Se opone a la creación de un registro DNO nacional único, al considerar que añadir consultas a fuentes externas puede ralentizar la detección y el control del fraude.

PTC

Apoya la creación de un registro DNO nacional único administrado por la CRC, al considerarlo el esquema más eficiente y coherente: una fuente centralizada, actualizada en tiempo real, permitiría una aplicación uniforme de bloqueos en todas las redes, reduciendo errores y asimetrías operativas y simplificando la integración de sistemas con un repositorio oficial. También destaca que este registro fortalecería el rol coordinador de la CRC y garantizaría condiciones homogéneas de cumplimiento en beneficio de la eficacia antifraude. Para su integración completa con sistemas de red, estima un plazo de un (1) año desde la puesta en operación, señalando como retos la integración técnica y los mecanismos de actualización en tiempo real; como transición, propone iniciar con una versión mínima viable y ampliar progresivamente alcance y funcionalidades.

SSC

El operador analiza de manera detallada dos alternativas:

Registro nacional único de DNO:

Reconoce beneficios potenciales (homogeneidad y referencia compartida), pero advierte riesgos significativos de falsos positivos sistémicos, rigidez operativa, concentración de responsabilidades y evasión por parte de actores fraudulentos. Considera que este esquema solo sería viable con criterios estrictos de inclusión, evidencia técnica verificable, revisión periódica, expiración automática y fuertes salvaguardas de gobernanza y protección de datos.

Listas DNO administradas por cada PRST bajo un estándar mínimo obligatorio:

SSC considera esta alternativa más flexible, proporcional y operativamente viable, al permitir respuestas ágiles y focalizadas, reducir riesgos sistémicos y alinearse con la realidad operativa de cada red. No obstante, enfatiza la necesidad de lineamientos regulatorios claros para evitar asimetrías de

mercado, usos desproporcionados o distorsiones competitivas, especialmente por parte de PRST con alta participación de mercado.

TELEFÓNICA

El operador valora las listas DNO como una herramienta complementaria, especialmente para proteger numeración institucional que no debe originar llamadas. Considera que un esquema donde cada PRST gestiona su propia lista de DNO bajo estándares mínimos ofrece la ventaja de la agilidad y la autonomía en la gestión de riesgos de su propia red, pero que debe existir un mecanismo de intercambio o consulta para que el bloqueo de no-originación sea respetado por todas las redes interconectadas.

No obstante, considera que STIR/SHAKEN no sustituye estas listas de DNO y que su gestión debe garantizar actualización en tiempo real, validación estricta del asignatario y mecanismos ágiles de consulta, evitando bloqueos erróneos.

TIGO

Manifiesta reservas frente a la efectividad de las listas DNO como mecanismo de mitigación del fraude, al considerar que los actores fraudulentos pueden sustituir rápidamente la numeración bloqueada. Asimismo, advierte que la centralización de estas listas podría generar ineficiencias, mayores costos operativos y un uso menos eficiente de un recurso escaso como la numeración.

En este contexto, considera viable mantener el statu quo, con ajustes puntuales para evitar bloqueos indebidos asociados a procesos como la portabilidad y el reciclaje de numeración. Además, solicita que se ajuste el proceso de bloqueo de los números portados, pues cuando estas líneas DNO son recicladas por parte del operador de origen pueden aparecer bloqueadas en las listas del operador a las que en algún momento se portaron y se detectó el fraude.

Por otro lado, considera que la alternativa 3 concentra nuevamente las obligaciones, y seguramente las responsabilidades por la ocurrencia de fraudes en los PRSTs. Mientras que la alternativa 4 No es una alternativa que se pueda aplicar de modo universal, además que no reconoce la participación y responsabilidades de otros agentes como los Carrier internacionales, los MVNO, e incluso las OTT.

ZANYA PINEDA

Manifiesta su preferencia frente a las listas por PRST bajo estándar mínimo, por agilidad y reducción de riesgo sistémico de falsos positivos, exigiendo coherencia inter-operador, gobernanza y depuración.

Respuesta de la CRC:

Respecto de la creación de un registro DNO nacional único administrado por la CRC, se observan comentarios a favor por parte de **PTC**, que consideran que una fuente centralizada y actualizada en tiempo real permitiría una aplicación uniforme de bloqueos en todas las redes.

En cambio, **TELEFÓNICA** considera que puede resultar más efectivo un esquema donde cada PRST gestiona su propia lista de DNO bajo estándares mínimos, pero con mecanismos de intercambio o consulta y **SSC** también considera esta alternativa más flexible, proporcional y operativamente viable.

A su vez **CLARO** favorece listas DNO propias bajo un estándar mínimo obligatorio y **ASOBANCARIA** enfatiza la necesidad de un control transversal de las listas. Por su parte **TIGO** cuestiona la efectividad de las listas DNO como mecanismo de mitigación del fraude e indica que la centralización puede implicar ineficiencias y mayores costos operativos.

Analizados los comentarios, la CRC considera que es importante mantener la temática de falta de estandarización en la aplicación de las listas de no originación, de manera que permita evaluar las alternativas regulatorias de las listas de DNO y contrastarlas con el statu quo. Sin embargo, el enfoque de la alternativa regulatoria estará basado en el mantenimiento de listas propias DNO gestionadas directamente por cada PRST con base en reglas objetivas definidas por la CRC, tales como: la protección de numeración institucional que no origina llamadas, y la numeración E.164 no atribuida, asignada o adjudicada de acuerdo con la información del Sistema de Información y Gestión de Recursos de Identificación (SIGRI) de la CRC y la información de gestión interna de los PRST.

Bajo este contexto, se descarta la alternativa regulatoria de un registro DNO nacional único administrado por la CRC porque, como lo anotan las observaciones, puede generar ineficiencias en los mecanismos de consultas e incrementar los costos operativos sin que se evidencie una ventaja distintiva obvia que favorezca su inclusión como alternativa regulatoria frente al uso de reglas simples y objetivas.

No obstante, y con el fin de complementar el análisis regulatorio frente al statu quo y a la alternativa basada en reglas objetivas definidas por la CRC, se considera pertinente incorporar una nueva alternativa que contemple un esquema dinámico y colaborativo, es decir, que no parta de una definición regulatoria en materia técnica ni de listas de no originación (DNO) base, sino que la misma sea definida de común acuerdo por PRSTM en función de la efectividad del mecanismo que propone.

La inclusión de esta alternativa responde a la necesidad de contar con un escenario de referencia que permita contrastar los beneficios y limitaciones de un enfoque completamente descentralizado, en el cual no exista intervención regulatoria en la definición de criterios técnicos, operativos o de gestión de las listas DNO. Esto resulta relevante en la medida en que algunos agentes del sector han manifestado que esquemas con mayor flexibilidad podrían reducir cargas operativas y facilitar la adaptación a dinámicas cambiantes de fraude.

De esta manera, la incorporación de esta nueva alternativa permitirá enriquecer el análisis comparativo entre distintos grados de intervención regulatoria, así como evaluar si la ausencia de estandarización puede generar eficiencias operativas sin comprometer los objetivos de mitigación del fraude y protección de los usuarios, frente a esquemas con reglas mínimas comunes o mayores niveles de centralización.

8.2.5.6 Respuesta a las preguntas de la consulta frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

- *En el servicio de llamadas de voz, los operadores pueden gestionar tanto tráfico originado por acuerdos directos con clientes nacionales (por ejemplo, bancos, comercios, entidades de salud, aerolíneas), como tráfico internacional que llega a través de cadenas de intermediarios, donde el originador de la llamada no siempre es certificado o plenamente identificable. ¿Qué*

diferencias, riesgos y oportunidades observa entre estos dos tipos de tráfico en relación con la prevención y mitigación del fraude? ¿Qué criterios, mecanismos o medidas considera relevantes para gestionar de manera diferenciada el tráfico directo y el tráfico en cadena, especialmente en lo relacionado con la trazabilidad, autenticación, control de llamadas sospechosas y judicialización?

ASOBANCARIA

Sostiene que el tráfico internacional presenta mayores riesgos debido a limitaciones en la trazabilidad y en la efectividad de las medidas correctivas. En este contexto, **ASOBANCARIA** opina que es necesario establecer controles diferenciados, con reglas más estrictas para el tráfico internacional, sin perjuicio de aplicar de manera integral las temáticas propuestas para mitigar el fraude en llamadas nacionales.

CLARO

Expone que el principal problema se centra en el tráfico internacional entrante, ya que no existe una norma clara que lo obligue a cumplir el plan de numeración, lo que permite la manipulación del CLI para actividades fraudulentas. Se propone primero regular el cumplimiento del plan de numeración nacional e internacional para llamadas entrantes, incluyendo aquellas con country code 57 o de otros países con fines fraudulentos, y como consecuencia, establecer la obligación de bloquear de inmediato las rutas que no cumplan autenticación o trazabilidad. En contraste, el tráfico nacional es más fácil de identificar y rastrear, por lo que la mayor preocupación radica en el tráfico internacional.

PTC

Plantea que las llamadas provenientes de bancos, comercios, salud, aerolíneas, etc., deberían contar con numeración única o máscara que permita identificar el origen y reconocer que es una llamada legítima, de modo que todo lo que esté por fuera de ese rango debe marcarse como spam o fraude, y que el cliente pueda decidir si bloquea o no.

SSC

Al respecto SSC no identifica únicamente dos tipos de tráfico, sino tres fuentes funcionales de origen claramente diferenciadas, cada una con perfiles de riesgo, capacidades de control y oportunidades de mitigación distintas frente al fraude. Menciona que reconocer esta diferenciación resulta esencial para el diseño de medidas regulatorias efectivas, proporcionales y técnicamente viables.

El primer tipo de tráfico que menciona es el directo nacional, en el que el elemento determinante no es el PRST al que se le asignó originalmente la numeración sino el PRST que presta efectivamente el servicio y controla el origen técnico de la llamada, por lo que el PRST provee el acceso a la red al cliente y gestiona el establecimiento, enrutamiento y terminación de la llamada dentro de su propia infraestructura. El recurso de numeración utilizado (CLI nacional) puede haber sido asignado al mismo PRST que provee el acceso o a otro PRST que fue el asignatario original del número, sin que ello afecte la legitimidad del servicio.

Indica que, en escenarios plenamente legítimos como la portabilidad numérica, se produce una separación entre el PRST asignatario original del número y el PRST que presta efectivamente el servicio. En estos casos, es el operador receptor quien cursa técnicamente la llamada y mantiene el control y la trazabilidad del tráfico, de conformidad con los mecanismos vigentes de gestión y administración de la numeración. En este esquema el PRST que presta el servicio pone a disposición del cliente numeración, ya sea asignada directamente o heredada mediante portabilidad, y provee el acceso a la red controlando el establecimiento, enrutamiento y terminación de la llamada.

Asegura que existe coincidencia entre el titular legítimo del CLI nacional, el origen técnico de la llamada y el operador que gestiona efectivamente el tráfico, independientemente de cuál PRST haya sido el asignatario original del recurso de numeración. Por esa razón el riesgo es bajo y controlable porque el operador cuenta con visibilidad completa del tráfico, capacidad de auditoría, suspensión inmediata ante comportamientos irregulares y soporte efectivo para procesos de investigación y judicialización.

Adicionalmente, agrega que existe una base de datos centralizada de numeración, que permite identificar de manera precisa el PRST que presta efectivamente el servicio asociado a cada CLI nacional, reforzando la trazabilidad del origen y la asignación de responsabilidades en este tipo de tráfico. Como oportunidades de mitigación del riesgo para este tipo de tráfico menciona que pueden tenerse controles contractuales y técnicos, trazabilidad completa del origen y evidencia técnica sólida para acciones correctivas y judiciales.

El segundo tipo de tráfico que indica es el que se genera desde Plataformas OTT / CPaaS. Menciona frente al mismo que se trata de llamadas plenamente legítimas originadas en plataformas tecnológicas globales, que no cuentan con red propia en todos los países y que, por tanto, utilizan carriers internacionales como medio de transporte para cursar sus comunicaciones.

Asegura que, en estos esquemas, la plataforma no es titular de la numeración, sino que presenta numeración asignada por PRST locales a sus clientes empresariales, quienes contratan dichos números para realizar comunicaciones salientes. Este modelo genera una separación entre la asignación del recurso de numeración y el origen técnico de la llamada, análoga a lo que ocurre en la portabilidad numérica, con la diferencia de que dicha separación no se materializa en otro operador de red, sino en infraestructura de plataforma basada en la nube.

Indica que, como resultado, las llamadas pueden presentar un CLI nacional aun cuando su origen técnico se encuentre en infraestructura internacional de la plataforma, como ocurre con Google (servicios de voz integrados a Google Cloud y soluciones empresariales), Amazon (servicios de voz prestados a través de Amazon Connect), Microsoft (servicios empresariales sobre Teams Phone), Twilio (servicios CPaaS y contact center en la nube), Genesys Cloud, y otras plataformas IP similares que dependen de carriers internacionales para cursar llamadas hacia las redes nacionales.

Asegura que este tipo de tráfico representa actualmente un porcentaje mayoritario del tráfico de larga distancia internacional (LDI), estimado en alrededor del 80 %, y corresponde principalmente a comunicaciones empresariales, transaccionales, de atención al cliente y cobranzas (no publicitarias o de ventas). En cuanto al tráfico de cobranzas, indica que este se enmarca en relaciones contractuales preexistentes y cuenta con autorización previa del usuario, por lo que no deben equipararse a llamadas comerciales o publicitarias.

Frente a los riesgos de este tipo de tráfico, manifiesta que presenta un riesgo intermedio, superior al del tráfico directo nacional, pero inferior al del tráfico internacional en cadena no identificado, debido a que se trata mayoritariamente de servicios empresariales legítimos, aunque con limitaciones estructurales de trazabilidad.

Este riesgo lo explica principalmente por disociación entre numeración y origen técnico de la llamada, teniendo en cuenta que la originación se da en infraestructura de plataforma basada en la nube, mientras que el CLI nacional corresponde a numeración asignada a un cliente empresarial, lo que introduce un reto de trazabilidad similar al observado en la portabilidad, pero sin una base centralizada equivalente que identifique al originador técnico del servicio.

Manifiesta que también cuenta con dependencia de carriers internacionales para el transporte, ya que las plataformas dependen de carriers internacionales al no contar con red propia en todos los países, y eso limita la visibilidad directa del PRST colombiano sobre el origen final del tráfico y puede retrasar la aplicación de medidas correctivas.

Igualmente, indica que hay un posible aprovechamiento de este tipo de tráfico por actores maliciosos, teniendo en cuenta que, aunque el modelo OTT /CPaaS es predominantemente legítimo, puede ser utilizado de forma indebida por terceros para ocultar su origen técnico y presentar CLI nacional válido, cuando no existen mecanismos adecuados de identificación y trazabilidad aguas arriba.

No obstante, manifiesta que este riesgo no se deriva del uso de CLI nacional ni de la naturaleza de la plataforma, sino de la ausencia de mecanismos estandarizados de trazabilidad y asignación clara de responsabilidades a lo largo de la cadena de prestación del servicio.

Desde la perspectiva operativa de SSC, considera que el tráfico originado en plataformas OTT / CPaaS presenta un riesgo medio y gestionable, por lo cual las medidas de mitigación deben ser proporcionales, técnicas y focalizadas, en concordancia con las alternativas regulatorias analizadas por la CRC, evitando enfoques de bloqueo generalizado que afecten tráfico empresarial legítimo.

En este contexto, se identifican como oportunidades de mitigación el fortalecimiento de la trazabilidad técnica del tráfico y el etiquetado informativo y señalización al usuario final por niveles de confianza, considerando etiquetas positivas con alto nivel de confianza (empresa verificada, origen empresarial identificado, llamada autenticada), etiquetas neutrales o informativas con confianza intermedia (llamada no verificada, origen internacional, origen no autenticado) y etiquetas de advertencia con uso restringido y focalizado (posible fraude, riesgo elevado).

El tercer tipo de tráfico que identifica es el internacional en cadena, el cual corresponde a llamadas que ingresan al país a través de uno o varios operadores internacionales de larga distancia (carriers), en las cuales el PRST colombiano mantiene relación contractual y técnica únicamente con el operador inmediato anterior, sin vínculo directo con el originador real de la llamada. Durante su tránsito, estas llamadas atraviesan múltiples redes, agregadores y plataformas, lo que reduce la trazabilidad sobre el origen técnico y el cliente final, y permite que un mismo carrier transporte simultáneamente llamadas personales desde el exterior, tráfico de roaming internacional, comunicaciones empresariales legítimas, tráfico originado en plataformas OTT / CPaaS y, en menor proporción, tráfico abusivo, en un contexto en el que la adopción masiva de aplicaciones OTT ha desplazado las llamadas conversacionales tradicionales y ha hecho que el tráfico LDI actual esté compuesto mayoritariamente

por comunicaciones empresariales legítimas cursadas a través de plataformas IP y carriers internacionales.

Indica que este tipo de tráfico presenta un riesgo elevado debido a la limitada trazabilidad del originador real de la llamada, como resultado de la multiplicidad de intermediarios (carriers, agregadores y plataformas) involucrados en su transporte. Esta situación genera una disociación entre el CLI presentado y el origen técnico efectivo, aun en escenarios de tráfico legítimo, lo que reduce la capacidad del PRST colombiano para identificar responsabilidades, aplicar controles directos y reaccionar oportunamente ante eventos de fraude. En este contexto, el riesgo no se encuentra en la numeración ni en la ruta internacional en sí mismas, sino en la opacidad del origen específico del tráfico.

Con base en su experiencia operativa en la gestión de tráfico de voz, SSC considera que la mitigación efectiva del fraude debe fundamentarse en medidas proporcionales, técnicas y focalizadas, alineadas con la complejidad del ecosistema actual. En este sentido, SSC prioriza el monitoreo y gestión de riesgo basada en comportamiento, el etiquetado informativo y señalización al usuario final y la Cooperación interoperatorial e intercambio de alertas.

TELEFÓNICA

Advierte sobre la existencia de una diferencia estructural crítica según la cual, en el tráfico nacional directo, el operador tiene control contractual sobre el origen y puede aplicar medidas de validación inmediata, por lo que el riesgo es bajo y la oportunidad de control es alta mediante cláusulas contractuales. Sin embargo, dice, el tráfico internacional que llega en cadena presenta el mayor riesgo de fraude y spoofing (suplantación), pues la trazabilidad se pierde entre múltiples intermediarios y no existe una relación contractual con el originador real. En virtud de lo anterior, **TELEFÓNICA** sugiere la aplicación de medidas diferenciadas, en virtud de las cuales para el tráfico nacional se debe fortalecer la validación contractual y, por su parte, para el tráfico internacional en cadena es indispensable exigir que el operador de larga distancia internacional (LDI) que entrega la llamada a la red nacional asuma la responsabilidad de garantizar que el CLI (identificador de llamada) no ha sido alterado. En ese marco, **TELEFÓNICA** concluye que, si el carrier internacional no puede certificar el origen, el operador nacional debe estar facultado para rechazar dicho tráfico o etiquetarlo como «no verificado».

TIGO

Señala que en el caso del tráfico originado a través de acuerdos directos existe un escenario de mayor control, que permite la identificación de alguna debilidad y su mitigación. Sin embargo, el tráfico internacional que llega a través de cadenas de intermediarios; si el origen no cuenta con firmas certificadas, el control y la identificación de los eventos de fraude resulta complejo y altamente costoso.

Este operador manifiesta que la obligación de control no puede recargarse en el último eslabón de la cadena, principalmente en los PRST's, y además las acciones de control no pueden limitarse a la detección, o prevención, sino que deben articularse mecanismos de sanción lo suficientemente justos y robustos que desincentiven la generación de eventos de fraude.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

RESPUESTA CRC:

Frente a esta pregunta, la mayoría de los agentes coinciden en señalar que el riesgo de fraude asociado a las llamadas de voz no es homogéneo, sino que depende principalmente del tipo del tráfico y grado de control que los operadores tengan sobre el origen de las comunicaciones. En este sentido **ASOBANCARIA** señala que el tráfico internacional presenta mayores riesgos debido a las limitaciones de trazabilidad y en la aplicación de medidas correctivas. De igual, **CLARO** destaca que el problema se concentra en el tráfico internacional entrante debido a que no se disponen de reglas suficientemente claras que obliguen a garantizar el cumplimiento del plan de numeración en este tipo de tráfico, facilitando la manipulación del identificador de llamadas (CLI), y como consecuencia la realización de actividades fraudulentas, a diferencia del tráfico nacional, que resulta más fácil de rastrear.

En el mismo sentido, **TELEFÓNICA** y **TIGO** destacan que existe una diferencia estructural entre el tráfico nacional directo y el tráfico internacional que ingresa al país a través de cadenas de intermediarios. Según **TELEFÓNICA**, en el tráfico nacional el operador cuenta con control contractual sobre el origen de la comunicación y puede aplicar medidas de validación inmediata, lo que reduce el nivel de riesgo. Por el contrario, el tráfico internacional en cadena presenta mayores riesgos de fraude y suplantación, debido a que la trazabilidad del origen de la llamada se diluye entre múltiples operadores y agregadores internacionales, con los cuales el operador nacional no necesariamente mantiene una relación contractual directa. De manera similar, **TIGO** señala que cuando el tráfico se cursa a través de acuerdos directos existe mayor capacidad para identificar debilidades y adoptar medidas de mitigación, mientras que el tráfico internacional que transita por múltiples intermediarios dificulta la identificación de eventos de fraude y aumenta los costos asociados a su control, particularmente cuando el origen no cuenta con mecanismos de autenticación o certificación.

Por su parte, **SSC** propone una aproximación más detallada al análisis del riesgo, señalando que el ecosistema actual de voz no se limita a una distinción entre tráfico nacional e internacional, sino que puede identificarse al menos tres fuentes funcionales de origen con perfiles de riesgo diferenciados. En primer lugar, el tráfico nacional directo, en el cual el proveedor de redes y servicios de telecomunicaciones (PRST) que presta el servicio controla el origen técnico de la llamada y mantiene la trazabilidad completa del tráfico, incluso en escenarios como la portabilidad numérica. En segundo lugar, el tráfico originado en plataformas tecnológicas tipo OTT o CPaaS, en el cual las llamadas pueden originarse en infraestructuras de nube y transportarse a través de carriers internacionales, lo que introduce una disociación entre el origen técnico de la llamada y la numeración presentada. Finalmente, SSC identifica el tráfico internacional en cadena, en el cual las llamadas atraviesan múltiples operadores, agregadores y plataformas antes de ingresar al país, reduciendo significativamente la trazabilidad del originador real y elevando el nivel de riesgo. En este contexto, SSC señala que el riesgo asociado a estos tres tipos de tráfico es, respectivamente, bajo, medio y alto.

En cuanto a las propuestas formuladas, se evidencia una convergencia en torno a la necesidad de que se adopten medidas regulatorias diferencias según el tipo de tráfico, el fortalecimiento de la trazabilidad de las llamadas, y la distribución de las responsabilidades de control entre los diferentes actores que participan en la cadena de prestación del servicio de voz. Así, **ASOBANCARIA** plantea la conveniencia de establecer controles más estrictos para el tráfico internacional, mientras que **CLARO** propone fortalecer el cumplimiento del plan de numeración nacional e internacional para las llamadas entrantes, incluyendo aquellas que presentan el código de país 57 u otros códigos internacionales utilizados con fines fraudulentos, y plantea además la posibilidad de bloquear de manera inmediata las rutas que no garanticen condiciones adecuadas de autenticación o trazabilidad.

Por su parte, **TELEFÓNICA** propone que los operadores de larga distancia internacional (LDI) que entregan llamadas a las redes nacionales asuman la responsabilidad de garantizar que el CLI no haya sido alterado durante el tránsito de la comunicación. En ese sentido, sugiere que, cuando el carrier internacional no pueda certificar la autenticidad del origen, el operador nacional debería estar facultado para rechazar dicho tráfico o etiquetarlo como no verificado. De manera complementaria, **TIGO** advierte que la obligación de control no debería recaer exclusivamente en el último eslabón de la cadena —esto es, en los operadores nacionales— y señala la necesidad de articular mecanismos sancionatorios y de responsabilidad que desincentiven la generación de eventos de fraude a lo largo de toda la cadena de prestación del servicio.

Adicionalmente, algunos agentes plantean mecanismos orientados a mejorar la identificación de llamadas legítimas por parte de los usuarios. En particular, **PTC** propone que determinados sectores como el financiero, el comercio, el sector salud o las aerolíneas utilicen numeración única o máscaras de numeración que permitan identificar de manera clara el origen de las llamadas legítimas, de modo que aquellas comunicaciones que se encuentren por fuera de dichos rangos puedan ser señaladas como potencial spam o fraude, permitiendo al usuario decidir si desea bloquearlas. En una línea similar, **SSC** plantea la posibilidad de implementar esquemas de etiquetado o señalización informativa de llamadas basados en niveles de confianza, que permitan distinguir entre llamadas verificadas, llamadas no verificadas o comunicaciones con posibles riesgos de fraude.

En atención a lo expuesto, la CRC considera que las propuestas formuladas por los agentes resultan útiles para el análisis del problema planteado. En particular, dichas propuestas aportan elementos relevantes para la gestión diferenciada del tráfico directo y del tráfico que ingresa a través de cadenas de intermediarios, especialmente en aspectos relacionados con la trazabilidad del origen de las llamadas, los mecanismos de autenticación, el control de comunicaciones sospechosas y el apoyo a eventuales procesos de investigación y judicialización de conductas fraudulentas.

No obstante, la eventual incorporación de estas medidas en el marco regulatorio estará sujeta a los resultados del correspondiente proceso de evaluación de alternativas regulatorias, el cual deberá considerar, entre otros aspectos, su viabilidad técnica, su proporcionalidad frente a los riesgos identificados y su compatibilidad con las competencias regulatorias atribuidas a la Comisión.

- *¿Qué mecanismos, herramientas o procedimientos tiene actualmente implementados su organización para detectar, prevenir y controlar el spoofing en llamadas de voz? ¿Qué nivel de efectividad han observado en estas medidas y qué retos técnicos y operativos han enfrentado en su aplicación?*

ASOBANCARIA

Informa que actualmente se desarrollan campañas de comunicación orientadas a la mitigación del fraude en este canal.

CLARO

Manifiesta que tiene implementadas herramientas de control con configuraciones específicas, asimismo, validaciones con los PCA o OT de los mensajes enviados. Asimismo, señala que el reto se

encuentra en el cambio constante del número originador que hace que el fraude lo que reduce su efectividad.

PTC

Indica que cuenta con una estrategia de concientización dirigida a clientes mediante mensajes de texto con recomendaciones de seguridad. Añade que, al detectar amenazas potenciales, envía comunicados oportunos para alertar y proteger a los usuarios. Menciona también un programa de "Alerta en línea" con recomendaciones de seguridad de la información a menores en colegios.

SSC

Menciona que cuenta con mecanismos operativos de monitoreo continuo del tráfico de voz, basados en el análisis de comportamiento (volúmenes, patrones horarios, destinos y rutas), que permiten identificar desviaciones asociadas a posibles eventos de suplantación. Adicionalmente, indica que mantiene una coordinación permanente con operadores de destino, de manera que, ante la notificación de tráfico originado en el exterior con comportamientos anómalos, aplica de forma inmediata bloqueos focalizados sobre los números o flujos específicos reportados, gestionando la situación en el menor tiempo posible.

Asimismo, mantiene relaciones estables con clientes empresariales confiables, lo que facilita la identificación de patrones legítimos y la detección temprana de desviaciones. Estas medidas han mostrado una efectividad media a alta en la contención de eventos de spoofing, particularmente cuando existe cooperación interoperatorial, aunque su alcance se ve limitado por la trazabilidad disponible en tráfico internacional en cadena, lo que representa el principal reto técnico y operativo.

TIGO

Señala que no hay herramientas antispoofing implementadas, sino que se realizan controles offline para
identificar posibles enmascaramientos del tráfico originado desde la red de TIGO, y además, cuenta con líneas de comunicación para compartir los hallazgos y aplicar las medidas pertinentes en cada red.

Indica que muy complejo identificar el enmascaramiento de las llamadas de origen internacional, dado que la cabecera de los registros de llamada puede ser modificada en el origen, y es técnicamente imposible detectar esta manipulación.

ZANYA PINEDA

Manifiesta que los mecanismos actualmente implementados para la detección, prevención y control del spoofing se concentran principalmente en análisis estadístico y comportamental del tráfico, tales como la identificación de patrones atípicos de oxigenación, picos inusuales de volumen, recurrencia de llamadas en ventanas de tiempo reducidas, duraciones anómalas o coincidencias entre rangos de numeración y destinos específicos. A estos mecanismos se suman listas internas de números previamente reportados, reglas heurísticas y modelos de detección basados en umbrales, los cuales son aplicados mayoritariamente por los operadores móviles en el punto de terminación de la llamada.

Frente a la efectividad de estas herramientas, menciona que es estructuralmente limitada teniendo en cuenta que el spoofing en llamadas de voz se sustenta, precisamente, en la capacidad de rotar de manera constante la identidad del número llamante (CLI), lo cual fue posible gracias a una asignación histórica masiva e indiscriminada de SIM Cards y numeración móvil, sin esquemas robustos de identificación del titular real ni mecanismos efectivos de trazabilidad.

En este contexto, indica que los sistemas de detección basados en listas negras o reincidencia pierden eficacia, dado que los actores fraudulentos pueden cambiar rápidamente de número, reutilizar rangos distintos o simular identidades legítimas, sin que ello implique un costo operativo significativo para ellos.

Agrega que, desde el punto de vista técnico y jurídico, existe una limitación de base y es que ningún actor del ecosistema puede determinar de manera objetiva si una llamada es fraudulenta antes de su terminación, ya que el contenido de la comunicación no puede ser interceptado, grabado ni analizado, en tanto ello vulneraría derechos fundamentales como la privacidad. En consecuencia, cualquier mecanismo que pretenda calificar una llamada como fraudulenta en tiempo real solo puede basarse en indicios indirectos, lo que incrementa significativamente el riesgo de falsos positivos y afectaciones al tráfico legítimo, lo que implica que los mecanismos actuales operan de manera reactiva, apoyándose en el reporte posterior del usuario final como principal insumo para confirmar la naturaleza fraudulenta de una llamada.

Indica que esta realidad demuestra que las soluciones centradas exclusivamente en filtros técnicos ex ante no solo son insuficientes, sino conceptualmente equivocadas, pues desconocen la forma en que se materializa el fraude en servicios de voz.

Adicionalmente, añade que los retos operativos se agravan cuando las llamadas fraudulentas ingresan por rutas internacionales o cadenas de intermediarios, donde la información sobre el originador real se diluye progresivamente. En estos escenarios, los operadores que terminan la llamada no cuentan con herramientas efectivas para verificar la autenticidad del CLI ni para reconstruir, en tiempo real, la cadena de responsabilidades, por lo que pretender que el operador móvil asuma un rol absoluto de control en este punto equivale a trasladarle una obligación imposible de cumplir de manera plena, al tiempo que se invisibiliza la responsabilidad estructural asociada a la administración inicial de la numeración.

En este contexto, finaliza indicando que los mecanismos actuales de detección y control del spoofing solo pueden considerarse instrumentos complementarios, útiles para mitigar impactos puntuales, pero incapaces de resolver el problema de fondo dado que su efectividad depende de la identificación efectiva del titular de la numeración, del fortalecimiento de los mecanismos de reporte ciudadano y de la trazabilidad progresiva de las llamadas.

RESPUESTA CRC:

Las respuestas recibidas frente a los mecanismos actualmente utilizados por la industria para detectar, prevenir y controlar el spoofing en llamadas de voz muestran, en primer lugar, una coincidencia general en que el problema se aborda hoy más desde esquemas de mitigación operativa y monitoreo posterior que desde soluciones capaces de impedir de manera plena la suplantación en tiempo real.

En esa línea, **SSC**, **TIGO** y **ZANYA PINEDA** describen controles basados en observación del tráfico, análisis de patrones y detección de anomalías, mientras que **CLARO** reporta la existencia de herramientas de control con configuraciones específicas y validaciones asociadas a los mensajes enviados. Por su parte, **ASOBANCARIA** y **PTC** enfatizan acciones de comunicación y concientización dirigidas a usuarios, más que herramientas técnicas de autenticación o verificación del originador. En conjunto, las respuestas evidencian que el ecosistema ya viene desplegando ciertas medidas de contención, pero también que tales medidas son heterogéneas en su alcance, naturaleza y propósito, pues unas se orientan a la detección técnica del tráfico y otras a la prevención mediante pedagogía y alertamiento al usuario.

Una segunda coincidencia relevante consiste en que varios agentes identifican el monitoreo del tráfico y el análisis de comportamiento como el principal mecanismo actualmente disponible. **SSC** explica que realiza monitoreo continuo del tráfico de voz con base en volúmenes, patrones horarios, destinos y rutas, lo que le permite identificar desviaciones y aplicar bloqueos focalizados cuando recibe notificaciones de tráfico anómalo, especialmente en coordinación con operadores de destino. **ZANYA PINEDA**, a su vez, describe con mayor detalle herramientas de análisis estadístico y comportamental, tales como la identificación de picos inusuales, recurrencia de llamadas en ventanas cortas, duraciones anómalas y coincidencias entre rangos de numeración y destinos específicos, complementadas con listas internas, reglas heurísticas y umbrales. **TIGO** también alude a controles offline para identificar posibles enmascaramientos del tráfico originado desde su red y a canales de comunicación para compartir hallazgos con otras redes. Aunque con distinto nivel de sofisticación, estas respuestas convergen en que el análisis de tráfico constituye hoy el núcleo de la respuesta operativa frente al spoofing.

No obstante, también se observan diferencias importantes en la forma de entender el problema y en el tipo de medidas priorizadas. Mientras **SSC** reporta una efectividad media a alta de sus mecanismos, especialmente cuando hay cooperación entre operadores, **TIGO** adopta una postura más restrictiva y sostiene que no cuenta con herramientas antispoofing implementadas, resaltando la imposibilidad técnica de detectar ciertas manipulaciones cuando la cabecera de la llamada es alterada en origen. **ZANYA PINEDA** profundiza aún más en esta limitación y plantea que ningún actor puede determinar objetivamente si una llamada es fraudulenta antes de su terminación, debido a restricciones técnicas y jurídicas que impiden analizar el contenido de la comunicación, por lo cual cualquier mecanismo solo puede operar sobre indicios indirectos y con riesgo de falsos positivos. En contraste, **ASOBANCARIA** y **PTC** ubican el énfasis en campañas de educación y alertas a clientes, incluyendo recomendaciones de seguridad, envío de comunicados oportunos y programas de formación, lo que revela una aproximación más preventiva desde la conducta del usuario que desde la autenticación de la llamada.

En cuanto a la efectividad observada y a los retos enfrentados, las respuestas también presentan elementos comunes. De manera transversal, los agentes coinciden en que la rotación constante del número originador, la posibilidad de alterar la identidad de la línea llamante y la baja trazabilidad del tráfico, en especial cuando intervienen rutas internacionales o cadenas de intermediación, reducen de forma significativa la eficacia de los controles existentes. **SSC** identifica como principal reto la limitada trazabilidad disponible en tráfico internacional en cadena. **TIGO** afirma que el enmascaramiento en llamadas de origen internacional es muy complejo de identificar. **ZANYA PINEDA** complementa esta visión al señalar que, cuando la llamada fraudulenta ingresa por rutas internacionales o múltiples intermediarios, la información sobre el originador real se diluye progresivamente y el operador que termina la llamada no cuenta con herramientas efectivas para verificar la autenticidad del CLI ni reconstruir en tiempo real la cadena de responsabilidades.

En ese contexto, lo manifestado por los agentes constituye un insumo relevante para la delimitación del alcance de las medidas que integran las alternativas regulatorias asociadas al eje temático de fraude en voz, así como para su evaluación con criterios técnicos adecuados. En particular, estas respuestas permiten identificar qué medidas que parecen más alineadas con la realidad operativa de las empresas, cuáles enfrentan barreras técnicas significativas, qué instrumentos complementarios pueden generar mayor efectividad y dónde se ubican los principales riesgos de implementación. De esta forma, la información aportada fue tenida en cuenta para valorar la pertinencia, proporcionalidad y factibilidad de las alternativas, evitando aproximaciones desconectadas de las capacidades reales del sector y privilegiando soluciones que reconozcan tanto la necesidad de proteger a los usuarios como las restricciones técnicas, jurídicas y operativas que hoy enfrenta el ecosistema para contener el denominado spoofing en llamadas de voz.

- *¿Qué efectos positivos y negativos prevé en la prohibición de llamadas internacionales con identidad de línea llamante CLI nacional? ¿Qué excepciones o consideraciones deberían contemplarse para no afectar la prestación de servicios legítimos?*

ASOBANCARIA

Destaca como efecto positivo una mayor trazabilidad y el fortalecimiento de la confianza de los usuarios. Añade que, para la gestión de excepciones, podrían contemplarse listas específicas con procesos de KYC que eviten afectar servicios legítimos.

CLARO

Expone que la medida reduciría el fraude por phishing y reclamaciones por wangiri, debido al uso de números en uso por parte de usuarios o por recepción de llamadas para campañas fuera de los horarios establecidos, así mismo señala que se mejoraría en la confianza del usuario en el momento de responder sus llamadas si decide hacerlo.

PTC

Señala como positivo el control de dispersión de llamadas y llamadas cortas, y refiere que existen controles automáticos para bloquear líneas unilateralmente cuando se detectan llamadas automáticas a listas o numeraciones continuas. No obstante, indica que la efectividad es muy baja porque las líneas detectadas suelen tener planes ilimitados, por lo que no sería viable el bloqueo sin evidencia concreta de este tipo de comportamientos. Adicionalmente, sugiere el uso de máscaras o prefijos que permitan identificar llamadas LDI entrantes con numeración local.

SSC

Desde la perspectiva de **SSC**, en línea con la posición del sector, la prohibición de llamadas internacionales con CLI nacional puede generar beneficios limitados frente a esquemas básicos de suplantación, pero no garantiza una reducción efectiva del fraude y conlleva impactos negativos relevantes sobre la prestación de servicios legítimos, por lo que no resulta adecuada como medida generalizada.

El spoofing consiste en la manipulación del identificador de la línea llamante para ocultar el origen real de la llamada, y puede realizarse tanto con CLI nacional como internacional. En consecuencia, centrar la mitigación en la nacionalidad del CLI no aborda el problema estructural, que es la falta de trazabilidad y autenticación del origen.

Por lo anterior, **SSC** considera más efectivo priorizar enfoques proporcionales, basados en trazabilidad, monitoreo de comportamiento, cooperación interoperatorial y esquemas de etiquetado informativo, contemplando excepciones para tráfico empresarial legítimo, en lugar de prohibiciones generales basadas únicamente en la presentación del CLI.

TELEFÓNICA

Identifica como efecto positivo la eliminación casi inmediata de una gran porción del fraude de suplantación (vishing), ya que técnicamente es anómalo que una llamada originada en el exterior presente un número fijo o móvil nacional, salvo en casos muy específicos. Sin embargo, **TELEFÓNICA** anticipa un efecto negativo crítico si no se gestionan adecuadamente las excepciones. Sugiere que la regulación contemple excepciones técnicas claras y automáticas para permitir el tráfico de abonados nacionales que se encuentran viajando y utilizando su línea en el exterior (roaming), asegurando que los sistemas de señalización puedan distinguir entre un viajero legítimo y una llamada suplantada.

TIGO

Señala que entre los efectos positivos se encuentra:

- El bloqueo de llamadas internacionales con identidad de linealínea llamante CLI nacional, podría implicar un desincentivo al enmascaramiento de llamadas.

Mientras que entre los efectos negativos identifica los siguientes:

- No se prevé sanción u obligación de los carrier nacionales o internacionales, o del originador, o intermediarios de las llamadas. La responsabilidad se sobrecarga en el agente terminante de la comunicación.
- En este sentido la CRC podría más bien implementar una medida prohibitiva de la práctica de enmascaramiento, estableciendo que, en caso de que esta práctica sea detectada se establezcan multas para quien la promueva o permita.
- Es una alternativa que técnicamente demanda costos muy altos sólo para el proceso de detección, y no garantiza la eliminación de la generación de fraudes con origen internacional.
- En los casos, en los que el enmascaramiento es aplicado como medida de seguridad para protección del llamante, así como, llamadas de emergencia o denuncias anónimas que requieren protección de los usuarios, tendrán que disponerse medidas excepcionales. Y en muchos casos este tipo de llamadas serán restringidas.
- Los bloqueos de llamada podrían potencialmente causar perjuicios a los usuarios.

ZANYA PINEDA

Al respecto, menciona que la prohibición de llamadas internacionales que presenten un identificador de línea llamante (CLI) nacional puede generar, en apariencia, un impacto positivo inmediato en la reducción de ciertos esquemas de suplantación, particularmente aquellos en los que actores

fraudulentos simulan ser entidades locales, cómo bancos, operadores, entidades públicas o empresas de servicios, para inducir al error al usuario final. Desde una lógica estrictamente reactiva, esta medida permitiría bloquear una tipología específica de fraude asociada al spoofing internacional con numeración nacional.

Sin embargo, menciona que una evaluación más profunda evidencia que esta prohibición conlleva riesgos estructurales significativos y puede producir efectos adversos desproporcionados sobre el ecosistema de comunicaciones de voz en Colombia.

Indica en primer lugar que una restricción absoluta desconoce la realidad operativa del mercado global de telecomunicaciones, en el que múltiples servicios legítimos utilizan infraestructuras internacionales para originar llamadas que, por razones técnicas, contractuales o de continuidad del negocio, presentan un CLI nacional.

Sostiene que la prohibición generalizada de este tipo de llamadas podría traducirse, en la práctica, en una barrera artificial a la prestación transfronteriza de servicios como plataformas de servicios compartidos, contact centers internacionales, soluciones de continuidad operativa, entre otros, afectando no solo a empresas legalmente constituidas, sino también a los propios usuarios finales, quienes podrían dejar de recibir comunicaciones legítimas relacionadas con servicios financieros, de salud, logísticos o de soporte técnico.

Añade que, desde una perspectiva regulatoria, esta medida resulta problemática en tanto vulnera principios como la neutralidad tecnológica, la proporcionalidad y la promoción de la competencia, al imponer una restricción que no distingue entre tráfico legítimo y tráfico fraudulento, y podría generar un efecto de concentración del mercado al fortalecer la posición de los operadores móviles que terminan las llamadas, quienes pasarían a controlar de manera casi exclusiva el acceso del tráfico internacional hacia usuarios móviles en Colombia. En lugar de mitigar el fraude, la medida podría terminar consolidando un modelo en el que quienes históricamente contribuyeron al desorden inicial, mediante la asignación masiva y poco controlada de SIM Cards, se posicionan como los únicos «guardianes» del sistema.

Asegura que la medida actúa únicamente sobre una manifestación del fraude, pero no sobre su causa estructural, que radica en la falta de identificación efectiva del originador real de la llamada y en la ausencia de mecanismos robustos de trazabilidad a lo largo de toda la cadena de valor, por lo que cualquier restricción al uso de CLI nacional en llamadas internacionales debe ser selectiva, condicionada y basada en criterios objetivos de verificación, y no una prohibición absoluta.

En ese sentido, considera indispensable contemplar excepciones claras para tráfico legítimo, soportadas en esquemas de registro del originador, acuerdos de confianza entre operadores, mecanismos de autenticación progresiva y procesos de validación ex post que permitan identificar responsabilidades en caso de abuso.

RESPUESTA CRC:

La Comisión leyó y analizó con atención las respuestas de **ASOBANCARIA, CLARO, PTC, SSC, TELEFÓNICA, TIGO** y **ZANYA PINEDA**, en los que, de manera general, subrayaron los efectos positivos y negativos relacionados con la prohibición de llamadas internacionales con identidad de

línea llamante CLI nacional, así como las excepciones o consideraciones que deberían implementarse para no afectar la prestación de servicios legítimos.

De las respuestas recibidas se identifica una tendencia en las observaciones que considera que la medida objeto de discusión es positiva. En concreto, **ASOBANCARIA** destaca como efecto positivo la mayor trazabilidad y el fortalecimiento de la confianza de los usuarios. En esa línea, **CLARO** opina que se reduciría el fraude por phishing y reclamaciones por wangiri, mientras que **PTC** sostiene que resulta deseable el control de dispersión de llamadas y llamadas cortas. Para **TELEFÓNICA** la medida es positiva ya que elimina una gran porción del fraude de suplantación (vishing) y, a su vez, **TIGO** señala que la medida genera un desincentivo al enmascaramiento de llamadas. **ZANYA PINEDA** sostiene que la medida tiene un impacto positivo inmediato en la reducción de esquemas de suplantación.

Por su parte, existe otra tendencia de respuestas según las cuales se considera que la medida requiere de ciertas excepciones. Al respecto, **ASOBANCARIA** sostiene que deben contemplarse listas específicas con procesos de KYC que eviten afectar servicios legítimos. A su turno, **PTC** recomienda el uso de máscaras o prefijos que permitan identificar llamadas LDI entrantes con numeración local. **SSC** sugiere excepciones para tráfico empresarial legítimo, en lugar de prohibiciones generales basadas únicamente en la presentación del CLI. En adición a lo anterior, **TELEFÓNICA** sugiere la incorporación de excepciones técnicas que sean claras y automáticas para permitir el tráfico de abonados nacionales que se encuentran viajando y utilizando su línea en el exterior (roaming). **ZANYA PINEDA** coincide en que se necesitan excepciones claras para tráfico legítimo, soportadas en esquemas de registro del originador, acuerdos de confianza entre operadores, mecanismos de autenticación progresiva y procesos de validación ex post.

Finalmente, en materia de efectos negativos, **PTC** advierte que la efectividad de la medida, si bien es positiva, puede llegar a ser muy baja porque las líneas detectadas suelen tener planes ilimitados, por lo que no sería viable el bloqueo sin evidencia concreta de este tipo de comportamientos. En sentido similar, **SSC** indica que, si bien la prohibición de llamadas internacionales con CLI nacional puede generar beneficios limitados frente a esquemas básicos de suplantación, lo cierto es que esta medida no garantiza una reducción efectiva del fraude y conlleva impactos negativos relevantes sobre la prestación de servicios legítimos. Por su parte, **TIGO** es claro en sostener que no existen sanciones para los originadores, los costos de la medida son muy altos y se requiere de medidas excepcionales. Los comentarios de **ZANYA PINEDA** coinciden, en términos generales, con estas apreciaciones.

En consideración de todo lo anterior, la CRC coincide con los efectos positivos subrayados por los interesados. A su vez, la Comisión observa que los aportes recibidos convergen en la necesidad de adoptar excepciones a la medida propuesta que sean objetivos y que, a su turno, aumenten la efectividad de ella. Lo anterior, ciertamente, será tenido en cuenta por esta Comisión al instante de ajustar/complementar las alternativas definitivas, así como al momento de su evaluación.

- *¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema que permita el enmascaramiento de la identidad de la línea llamante CLI en llamadas internacionales, siempre que estas sean etiquetadas en el dispositivo del usuario como "No verificada" o "Probable fraude"? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la prevención del fraude, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?*

ASOBANCARIA

Informa que el principal reto consiste en diferenciar adecuadamente entre líneas que deban ser etiquetadas como "No verificadas" o "Probable fraude", así como en lograr una adopción efectiva del esquema y que la etiqueta proporcione información útil al usuario.

CLARO

Expone que en la práctica, la evidencia muestra que las etiquetas o advertencias en los dispositivos ("No verificada" o "Probable fraude") son poco efectivas, ya que los usuarios las ignoran o no comprenden su alcance, y que desde el punto de vista técnico, no es posible identificar de manera confiable el origen del tráfico para diferenciar llamadas internacionales con CLI nacional, tráfico de clientes en roaming o tráfico cursado desde redes de otros operadores, lo que genera un alto riesgo de falsos positivos y etiquetados erróneos.

Expone que, afecta directamente la experiencia del usuario, quien continuará recibiendo las llamadas no deseadas, ahora acompañadas de alertas confusas, incrementando la molestia y las reclamaciones, sin una reducción real del fraude, como en el caso de estafas tipo Wangiri. Además, que la medida implica los siguientes retos técnicos y operativos:

- Interoperabilidad tecnológica: Requiere adaptar sistemas SIP/SS7 y equipos de usuario para soportar etiquetas diferenciales;
- Coordinación entre operadores: Unificación de criterios de "falsos positivos" y actualización de estándares.
- Experiencia del usuario: El etiquetado debe ser claro, evitar alarmar sin razón o saturar la interfaz.
- Evitar bloquear llamadas legítimas de empresas internacionales, aliados o servicios críticos

Concluye, que la CRC primero debe evaluar formalmente la efectividad de las medidas existentes, fortalecer procesos de recuperación y realizar un Análisis de Impacto Normativo (AIN) antes de implementar nuevos desarrollos, garantizando así una política eficiente, proporcional y basada en evidencia. En consecuencia, no considera que la propuesta sea viable o necesaria.

PTC

Identifica como principal reto validar que se trata de una llamada no verificada o de potencial fraude y comprobar que efectivamente es fraude. Añade que deben existir mecanismos que informen cuando no se trata de fraude.

SSC

Desde la perspectiva de **SSC**, la implementación de un esquema que permita el enmascaramiento del CLI en llamadas internacionales, acompañado de etiquetado informativo en el dispositivo del usuario, representa una oportunidad relevante y moderna para fortalecer la protección del usuario y la prevención del fraude, siempre que se diseñe bajo criterios de proporcionalidad, trazabilidad y experiencia de usuario.

Señala las siguientes ventajas e impactos positivos:

• Empoderamiento del usuario final. El etiquetado permite que el usuario tome decisiones informadas sobre si atender o no una llamada, sin recurrir a bloqueos automáticos. Este enfoque es consistente con el uso extendido de soluciones de identificación de llamadas como Truecaller, Google Call Screen / Verified Calls (Android), Apple Call Identification & Silence Unknown Callers (iOS) y Hiya (integrada en dispositivos Samsung y operadores en varios países), las cuales ya clasifican llamadas como spam, no verificadas o verificadas, y han demostrado ser efectivas para reducir la exposición al fraude.

• Gestión de confianza, no solo de riesgo. El esquema no debe limitarse a etiquetas negativas ("No verificada" o "Probable fraude"), sino que puede incorporar etiquetas positivas, tales como "Empresa verificada", "Llamada empresarial" o "Servicio de atención al cliente", que incrementan la confianza del usuario y preservan la contactabilidad de servicios legítimos.

• Mitigación proporcional del fraude. A diferencia de la prohibición o el bloqueo generalizado, el etiquetado reduce el impacto sobre tráfico legítimo y evita el desplazamiento del fraude hacia otros esquemas, contribuyendo a una mitigación más sostenible.

• Alineación con tendencias internacionales. Este enfoque es coherente con prácticas ya implementadas en ecosistemas móviles avanzados y con las alternativas analizadas por la CRC.

En cuanto a retos y desafíos considera los siguientes:

• Definición clara y estandarizada de etiquetas. Es fundamental establecer criterios técnicos y regulatorios homogéneos para la asignación de etiquetas, evitando interpretaciones inconsistentes entre operadores, plataformas y fabricantes de dispositivos.

• Gobernanza y responsabilidad sobre la clasificación. Debe definirse quién asigna, valida y actualiza las etiquetas (PRST, plataformas, terceros), así como los mecanismos de reclamación y corrección para evitar errores o afectaciones reputacionales.

• Interoperabilidad técnica. La efectividad del esquema depende de su integración con sistemas operativos, fabricantes de dispositivos y redes, así como de la compatibilidad entre tecnologías y mercados.

• Experiencia de usuario. Un exceso de etiquetas negativas puede generar fatiga o desconfianza generalizada. Por ello, el esquema debe equilibrar advertencias con señales positivas de confianza.

Frente a la contribución a la protección del usuario y prevención del fraude, **SSC** considera que el etiquetado informativo, combinado con enmascaramiento del CLI cuando no exista verificación suficiente, constituye una herramienta eficaz de protección al usuario, al tiempo que preserva la prestación de servicios legítimos. Este enfoque permite reducir el impacto del fraude sin depender exclusivamente de bloqueos, y traslada la mitigación hacia un modelo de gestión de confianza, acorde con el ecosistema digital actual.

Al respecto sugiere el siguiente listado de etiquetas no exhaustivo:

• Empresa verificada
• Llamada empresarial
• Servicio de atención al cliente
• Origen internacional
• Número no verificado
• Posible fraude
• Spam reportado por usuarios

Finaliza indicando que el etiquetado informativo no debe concebirse únicamente como una advertencia, sino como un mecanismo de gestión de confianza, ya adoptado por plataformas y sistemas operativos líderes, que permite proteger al usuario, preservar la contactabilidad y mitigar el fraude de manera proporcional y sostenible.

TELEFÓNICA

Señala como ventaja el hecho de empoderar al usuario con información en tiempo real antes de contestar, reduciendo la tasa de éxito del fraude sin bloquear comunicaciones que podrían ser legítimas, pero técnicamente no verificables. Por su parte, identifica como retos técnicos y operativos significativos el hecho de que esta funcionalidad depende de que los terminales (equipos móviles) soporten la visualización de dichas etiquetas y de que la red pueda transmitir esa información de señalización hasta el usuario final. Al respecto, **TELEFÓNICA** advierte que existe el riesgo de generar "falsos positivos" que etiqueten llamadas legítimas de empresas internacionales como fraude, afectando la operación comercial de clientes corporativos. Finalmente, dice que la implementación requiere inversiones en el núcleo de la red para habilitar estas capacidades de marcado, cuyo costo debe ser evaluado frente al beneficio real.

TIGO

Entre las ventajas señala que El etiquetado de la llamada ofrece la posibilidad al usuario de identificar un riesgo potencial de acuerdo con sus necesidades y criterios; y en todo caso tener referencia. Si embargo, identifica los siguientes retos:

1. Técnicos
   - Actualización del Core y coordinación con redes internacionales para implementar la infraestructura de autenticación STIR/SHAKEN.
   - Interoperabilidad global, para que el sistema funcione. Todos los países deben soportar los mecanismos de autenticación
   - Evitar la restricción de las llamadas en las que se practica enmascaramiento es «legal», bien por necesidad de protección al usuario, o por condiciones técnicas

2. Operativos
   - Coordinación entre operadores para acordar formatos y mecanismos de clasificación
   - Necesidad de capacitación al usuario para evitar confusiones con el etiquetado y las reglas de bloqueo
   - La CRC debe establecer una normatividad clara sobre el uso, exclusiones y sanciones relacionadas con los mecanismos de clasificación.

Entre los posibles impactos este operador señala que esta medida implicaría altos costos de implementación sin garantizar la eliminación del fraude en llamadas internacionales, dado que los esquemas de suplantación también pueden realizarse mediante numeración internacional sin enmascaramiento. Identifica que, en este escenario, aunque los defraudadores asumirían cargos de roaming, conservarían la posibilidad de ejecutar fraudes desde el exterior, lo que reduciría la efectividad de la medida y podría generar un uso ineficiente de los recursos destinados a su implementación.

ZANYA PINEDA

Menciona al respecto que esta opción constituye una alternativa regulatoria más equilibrada, proporcional y compatible con la realidad técnica del servicio de voz, que las propuestas de bloqueo o prohibición absoluta, dado que reconoce la premisa fundamental de que los servicios de voz no es posible determinar con certeza la naturaleza fraudulenta de una llamada antes de su terminación, y, por tanto, cualquier solución efectiva debe necesariamente involucrar al usuario final como actor central del proceso de mitigación del riesgo.

Indica que, desde la perspectiva de protección al usuario, este esquema resulta especialmente valioso porque reduce la asimetría de información que actualmente existe entre quien origina la llamada y quien la recibe al introducir una señal de advertencia que refuerza la prevención sin imponer una carga excesiva sobre el sistema ni sobre los actores intermedios.

No obstante, asegura que la eficacia de esta medida depende críticamente de evitar etiquetados excesivamente agresivos o indiscriminados, por lo que su implementación debe sustentarse en criterios objetivos, trazables y verificables, tales como la ausencia de información suficiente sobre el originador en la cadena de interconexión, la falta de registro previo del número o la imposibilidad técnica de validar el CLI, y no en presunciones automáticas de fraude.

Solicita al respecto que la Comisión defina lineamientos claros sobre los estándares mínimos de señalización, presentación del etiquetado en los dispositivos y responsabilidades de cada actor en la cadena, así como garantizar que el etiquetado sea consistente entre redes, evitando escenarios en los que una misma llamada sea presentada de manera distinta según el operador de destino, lo cual generaría confusión y fragmentación de la experiencia del usuario.

En términos de experiencia de usuario, menciona que el etiquetado debe ser claro, comprensible y no alarmista. Mensajes como «No verificada» o «Origen no autenticado» resultan más adecuados que calificaciones categóricas, en la medida en que informan sin inducir pánico o rechazo automático. Este esquema permite avanzar hacia un modelo de control distribuido, en el que la mitigación del fraude no recae exclusivamente en los operadores móviles que terminan la llamada, sino que se apoya en una combinación de transparencia, pedagogía, reporte ciudadano y trazabilidad progresiva.

RESPUESTA CRC:

A partir de los aportes recibidos, se identifican coincidencias relevantes y posiciones divergentes frente a la alternativa regulatoria que permitiría el enmascaramiento del CLI en llamadas internacionales, siempre que dichas llamadas sean etiquetadas en el dispositivo del usuario como "No verificada" o "Probable fraude". En términos generales, los agentes coinciden en que esta alternativa representa

un enfoque distinto al bloqueo o prohibición, al introducir mecanismos de información al usuario como herramienta central de mitigación del riesgo, aunque difieren de manera significativa en la valoración de su efectividad práctica, sus costos y sus impactos sobre la experiencia del usuario.

De manera común, varios agentes reconocen como ventaja potencial el hecho de que el etiquetado informativo puede empoderar al usuario, al reducir la asimetría de información entre quien origina la llamada y quien la recibe, permitiéndole tomar decisiones más informadas sobre si atender o no una comunicación entrante (ASOBANCARIA, SSC, TELEFÓNICA, TIGO, ZANYA PINEDA). Este enfoque es consistente con la intención de la CRC al explorar alternativas que no dependan exclusivamente de bloqueos automáticos, y que reconozcan las limitaciones técnicas inherentes al servicio de voz, donde no es posible determinar con certeza la naturaleza fraudulenta de una llamada antes de su terminación. En este sentido, el esquema de etiquetado se percibe como una herramienta de mitigación proporcional, que preserva la prestación de servicios legítimos y reduce el riesgo de desplazamiento del fraude hacia otros mecanismos.

Asimismo, existe coincidencia en que la medida podría contribuir parcialmente a la prevención del fraude, en la medida en que reduce la tasa de éxito de las estafas al alertar al usuario y generar desconfianza frente a llamadas cuyo origen no puede ser autenticado (SSC, TELEFÓNICA, TIGO, Zanya Pineda). Desde esta perspectiva, el etiquetado no elimina el fraude, pero puede disminuir su efectividad, especialmente cuando se articula con esquemas de reporte por parte del usuario y con mecanismos progresivos de trazabilidad y análisis posterior.

No obstante, los aportes también evidencian retos técnicos y operativos significativos que generan posiciones divergentes sobre la viabilidad de la alternativa. De manera reiterada se señala la dificultad de diferenciar de forma confiable entre llamadas que deben ser etiquetadas como "No verificadas" y aquellas que podrían considerarse "Probable fraude", dada la complejidad de las cadenas internacionales de interconexión y la limitada disponibilidad de información sobre el originador real del tráfico (ASOBANCARIA, CLARO, PTC, Zanya Pineda). En particular, CLARO plantea una posición crítica al señalar que, en la práctica, no es posible identificar de manera confiable el origen del tráfico para aplicar etiquetas diferenciadas, lo que incrementa el riesgo de falsos positivos, etiquetados erróneos y afectación de llamadas legítimas, incluyendo tráfico de roaming, aliados internacionales o servicios críticos.

En esta misma línea, varios agentes advierten que el esquema enfrenta desafíos importantes de interoperabilidad técnica, al requerir adaptaciones en redes SIP/SS7, en los núcleos de red, en la señalización y en los propios terminales de usuario para soportar la visualización consistente de las etiquetas (CLARO, TELEFÓNICA, TIGO, SSC). Estos desafíos se traducen en costos de implementación relevantes, cuyo beneficio en términos de reducción efectiva del fraude no resulta evidente para todos los actores, especialmente si el etiquetado no se acompaña de mecanismos robustos de autenticación del origen como STIR/SHAKEN o equivalentes.

Otro punto de convergencia parcial es el riesgo de afectación de la experiencia del usuario. Mientras algunos agentes consideran que el etiquetado puede ser útil si se diseña de forma clara y no alarmista (SSC, Zanya Pineda), otros advierten que un exceso de advertencias o etiquetas confusas puede generar fatiga, desensibilización del usuario y aumento de reclamaciones, sin una reducción real del fraude (CLARO). En este sentido, se destaca que la efectividad del esquema depende críticamente del diseño de las etiquetas, de su comprensión por parte del usuario y de una estrategia de pedagogía adecuada, aspectos que no son triviales desde el punto de vista regulatorio.

Las posiciones divergentes se hacen más evidentes en la valoración final de la alternativa. Mientras SSC, TELEFÓNICA, TIGO y Zanya Pineda consideran que el etiquetado informativo, bien diseñado y articulado con otras medidas, puede constituir una alternativa equilibrada y moderna, CLARO concluye que la medida no es viable ni necesaria en el contexto colombiano actual, al considerar que su efectividad es baja y sus costos y riesgos son elevados. ASOBANCARIA y PTC adoptan posiciones intermedias, resaltando los retos de clasificación y la necesidad de contar con mecanismos claros que permitan también identificar cuando una llamada no es fraudulenta.

Desde la intención regulatoria de la CRC, los insumos recibidos permiten concluir que esta alternativa no debe entenderse como una solución autónoma ni sustitutiva de otras medidas más estructurales, como la autenticación del origen, la limitación del spoofing o la mejora de la trazabilidad en cadenas internacionales. Sin embargo, también evidencian que el etiquetado informativo puede aportar valor como herramienta complementaria, orientada a la gestión de confianza y al empoderamiento del usuario, siempre que se diseñe bajo criterios estrictos de proporcionalidad, estandarización, interoperabilidad y experiencia de usuario.

En consecuencia, la acción a tomar por parte de la CRC es mantener esta alternativa dentro del conjunto de opciones regulatorias en evaluación, pero condicionarla expresamente a un diseño cuidadoso que incluya criterios homogéneos de etiquetado, reglas claras de gobernanza y responsabilidad, salvaguardas frente a falsos positivos y una evaluación rigurosa de costos y beneficios en el marco del Análisis de Impacto Normativo. Asimismo, la CRC debería considerar si, en ausencia de avances significativos en autenticación del origen y control del spoofing, la implementación de este esquema podría resultar prematura o de efectividad limitada, lo que podría llevar a ajustar su alcance o postergar su adopción hasta que se cuente con condiciones técnicas y operativas más favorables.

- *¿Qué oportunidades y retos identifica en la adopción de protocolos de autenticación como STIR/SHAKEN/RCD? ¿Qué condiciones técnicas y regulatorias serían necesarias para su implementación efectiva? ¿Considera que, con la implementación de este protocolo de autenticación, no resulta necesaria la implementación de medidas de filtrado de tráfico o listas de no originación (DNO)?*

ASOBANCARIA

Sostiene que la adopción de STIR/SHAKEN ofrece una oportunidad para fortalecer la autenticación del origen de las llamadas y reducir la suplantación asociada al spoofing, aumentando la confianza en el servicio de voz. Sin embargo, **ASOBANCARIA** añade que el principal reto es asegurar su efectividad en la detección del fraude, la correcta categorización de las llamadas y una experiencia de usuario adecuada, evitando falsos positivos. Por ello, propone que se complementen estos protocolos con mecanismos adicionales como sistemas de filtrado y listas Do Not Originate (DNO, por sus siglas en inglés) para lograr una mitigación integral del fraude.

CLARO

Expone que no considera viable implementar STIR/SHAKEN en este momento debido a la alta complejidad de interoperabilidad entre operadores nacionales, operadores de LDI y carriers internacionales, lo que podría afectar el acceso de las comunicaciones al país. Además, su

implementación implica altos costos de licenciamiento, una operación técnica compleja y tiempos largos de despliegue que podrían quedar rápidamente desactualizados frente a la evolución del fraude. En su lugar, se considera suficiente fortalecer el cumplimiento del plan de numeración internacional y los controles sobre el tráfico entrante. Por ello, solicita a la CRC evaluar primero la efectividad de las medidas actuales, fortalecer los procesos de recuperación y realizar un Análisis de Impacto Normativo antes de adoptar nuevas soluciones técnicas.

SSC

Considera que protocolos de autenticación como STIR/SHAKEN/RCD son útiles para verificar el identificador de llamadas cuando existe control sobre el origen de la llamada, pero no son una solución completa, especialmente en llamadas internacionales en cadena o provenientes de plataformas OTT / CPaaS, donde la autenticación no siempre es posible. Por esta razón, indica que aun con la implementación de estos protocolos, siguen siendo necesarias otras medidas como el monitoreo del tráfico basado en comportamiento, el intercambio de alertas entre operadores y el uso limitado y estandarizado de listas de no originación (DNO). En consecuencia, **SSC** considera que la mitigación del fraude debe abordarse mediante un enfoque combinado, que use la autenticación como una herramienta más, y no como un sustituto de todas las demás medidas.

TELEFÓNICA

Considera que la adopción en Colombia enfrenta un reto estructural insalvable en el corto plazo, ya que este protocolo solo funciona sobre redes basadas enteramente en IP (SIP). En su opinión, mientras existan interconexiones TDM tradicionales en la red nacional, la "firma digital" de autenticación se perderá en el tránsito, haciendo inefectiva la inversión. Sobre esa base, **TELEFÓNICA** advierte que se requiere una condición regulatoria previa equivalente a un plan de migración tecnológica de todo el sector hacia la interconexión IP. Adicionalmente, considera que STIR/SHAKEN no sustituye otras medidas ya que es una herramienta complementaria. En su sentir, las listas de no originación (DNO) seguirían siendo útiles para proteger números que nunca deben originar llamadas (como líneas de atención al cliente inbound), independientemente del protocolo de señalización usado.

ZANYA PINEDA

Menciona que los protocolos de autenticación de identidad de llamadas como STIR/SHAKEN y RCD representan, en términos conceptuales, un avance relevante en la mitigación del spoofing en servicios de voz, en la medida en que buscan garantizar la integridad del identificador de la línea llamante (CLI) mediante mecanismos criptográficos y de señalización estandarizada, dado que su principal aporte consiste en permitir que el operador que origina la llamada certifique, con distintos niveles de confianza, que el número presentado corresponde efectivamente al usuario o entidad autorizada para utilizarlo.

No obstante, indica que la adopción de estos protocolos en el contexto colombiano enfrenta limitaciones estructurales que impiden considerarlos como una solución integral o autosuficiente frente al fenómeno del fraude en llamadas de voz. En primer lugar, asegura que la efectividad de STIR/SHAKEN depende de un supuesto que no siempre se cumple en la práctica, y es la existencia de una identificación previa, verificable y confiable del originador de la llamada, por lo que en escenarios donde la numeración fue asignada de manera masiva, sin controles robustos de identidad, o donde el

tráfico se origina a través de cadenas internacionales con múltiples intermediarios, la capacidad de certificar el origen real de la llamada se ve seriamente comprometida.

Desde una perspectiva técnica, agrega que estos protocolos funcionan de manera óptima en entornos relativamente cerrados o con alto grado de madurez institucional, donde los operadores comparten estándares homogéneos, existe interoperabilidad plena y la cadena de interconexión es corta y transparente. Sin embargo, el ecosistema colombiano de voz se caracteriza por una alta fragmentación, con la coexistencia de PRSTM, operadores de tránsito, OTT, CAPS y plataformas tecnológicas internacionales, lo que dificulta la implementación uniforme de STIR/SHAKEN y reduce significativamente su alcance en el tráfico que ingresa por rutas internacionales o esquemas indirectos.

Adicionalmente, asegura que la implementación de estos protocolos implica costos económicos y operativos relevantes, tanto para los operadores móviles como para otros actores del sector. La adecuación de redes, la actualización de sistemas de señalización, la gestión de certificados digitales y la operación continua del esquema de autenticación pueden resultar desproporcionadas para actores más pequeños, lo que podría generar barreras de entrada o exclusión indirecta, contrarias a los principios de libre competencia y neutralidad tecnológica que deben orientar la regulación del sector.

Desde el punto de vista regulatorio, menciona que resulta igualmente problemático asumir que la adopción de STIR/SHAKEN elimina la necesidad de otras medidas de mitigación del fraude. Estos protocolos no previenen el fraude en sí mismo, sino que autentican la integridad del CLI. Es decir, certifican que el número no fue alterado durante la transmisión, pero no garantizan que el titular del número no esté incurriendo en conductas fraudulentas. En consecuencia, incluso llamadas plenamente autenticadas pueden ser utilizadas para cometer estafas, especialmente cuando el fraude se basa en el uso de información parcialmente real y en técnicas de ingeniería social.

Por esta razón, no considera adecuado plantear que la implementación de STIR/SHAKEN haga innecesarias medidas complementarias como los esquemas de reporte del usuario, las listas de no originación (DNO) o los mecanismos de etiquetado informativo, teniendo en cuenta que el usuario final continúa siendo el único actor capaz de identificar el engaño en el momento en que se materializa, y su reporte sigue siendo un insumo esencial para activar procesos correctivos, administrativos y, eventualmente, judiciales.

Finaliza mencionando que la implementación debe ser progresiva, flexible y compatible con otros mecanismos ya existentes, evitando enfoques maximalistas que pretendan resolver un problema estructural mediante una única solución técnica.

TIGO

Indica que antes de listar las oportunidades y retos que supone la implementación de los protocolos de autenticación, se debe hacer énfasis en el hecho que la autenticación de las llamadas de origen internacional depende de la gestión y certificación de los originadores, lo cual no es gestionable por los PRST's locales en Colombia principalmente porque los protocolos STIR/SHAKEN no corresponden a estándares de implementación global y adicionalmente al no establecerse en todos los acuerdos internacionales con conexiones directas pueden involucrarse intermediarios que hagan tránsito de las llamadas que no aplican estos protocolos, y rompen la cadena de autenticación.

Señala que las obligaciones para mitigar el fraude en llamadas deben extenderse a los carriers internacionales y a los originadores del tráfico, evitando concentrar la carga únicamente en los PRST, dado que estos no controlan integralmente el proceso. Entre las oportunidades se destaca que herramientas como STIR/SHAKEN pueden ayudar a los usuarios a distinguir llamadas legítimas de sospechosas. No obstante, su implementación enfrenta retos importantes: el protocolo no tiene adopción global, los PRST no pueden certificar plenamente llamadas internacionales, existe fragmentación tecnológica entre redes IP y tradicionales, y la efectividad depende de que todos los intermediarios certifiquen la llamada. Además, su adopción requiere redes IP, infraestructura de autenticación y certificados digitales, cooperación entre operadores, actualización de software y coordinación operativa. Finalmente, se considera que las listas de No Originación (DNO) son ineficientes como mecanismo de control del fraude.

RESPUESTA CRC:

A partir de los comentarios recibidos se identifican coincidencias relevantes entre los agentes respecto a las oportunidades y limitaciones asociadas a la adopción de protocolos de autenticación de llamadas como STIR/SHAKEN y RCD, así como respecto a su relación con otras medidas de mitigación del fraude en el servicio de voz móvil.

En términos generales, los comentarios a la consulta evidencian un reconocimiento transversal de que estos protocolos representarían un avance técnico importante frente a la necesidad de garantizar la autenticación del origen de las llamadas y reducir las prácticas de suplantación de identidad (spoofing), en la medida en que permiten verificar la integridad del identificador de la llamada entrante (CLI) mediante mecanismos de certificación y firma digital. Bajo esta perspectiva, varios aportes coindicen en señar que estos esquemas pueden contribuir a mejorar la trazabilidad del tráfico de voz para y fortalecer la confianza de los usuarios en este canal.

Sin embargo, los comentarios coinciden en señalar retos técnicos estructurales para la implementación de estos protocolos en el contexto colombiano, particularmente en lo relacionado con la interoperabilidad de las redes, la coexistencia de infraestructuras basadas en tecnologías IP y TDM, y la participación de múltiples intermediarios en las cadenas de interconexión internacional. En efecto, varios aportes destacan que la efectividad de STIR/SHAKEN depende en gran medida de la existencia de ecosistemas de interconexión homogéneos basados en protocolos IP (SIP), así como de la adopción coordinada de estos estándares por parte de los distintos actores que intervienen en el enrutamiento de las llamadas. En entornos donde persisten segmentos de red no IP o donde las llamadas atraviesan múltiples intermediarios internacionales, la cadena de autenticación puede romperse, reduciendo la eficacia del mecanismo.

Adicionalmente, algunos comentarios de la consulta resaltan las consideraciones económicas y operativas asociadas a la implementación de estos protocolos, tales como la necesidad de adecuar las infraestructuras de red, gestionar certificados digitales, implementar sistemas de autenticación y coordinar procesos de interoperabilidad entre operadores. De igual manera, se identifica que las observaciones coinciden en señalar que la efectividad de estos protocolos también depende significativamente de la disponibilidad de mecanismos robustos de verificación de identidad del originador del tráfico, esquemas claros de certificación y responsabilidades definidas para los actores que participan en la generación y terminación de llamadas. Así mismo indican que la autenticación de llamadas internacionales es un reto adicional, en la medida en que los operadores nacionales no tienen

control directo sobre los originadores del tráfico ni sobre todos los intermediarios que participan en el enrutamiento de las comunicaciones.

En cuanto a la relación entre la adopción de estos protocolos y la necesidad de otras medidas de mitigación del fraude, los comentarios evidencian una tendencia a considerar que STIR/SHAKEN no sustituye la implementación de mecanismos complementarios, tales como listas de no originación, esquemas de monitoreo de tráfico o mecanismos de filtrado. Bajo esta perspectiva, la autenticación del CLI se concibe como un componente adicional dentro de un conjunto más amplio de herramientas orientadas a fortalecer la integridad de las comunicaciones y a reducir el fraude en el servicio de voz.

En consideración de lo anterior, la CRC identifica que los comentarios recibidos aportan elementos técnicos relevantes que constituyen insumos útiles para el análisis de la evolución tecnológica de los mecanismos de autenticación del identificador de llamada. No obstante, y en consistencia con lo expuesto previamente en la sección de respuestas a los comentarios de la temática 1 del eje del servicio de voz móvil, la Comisión considera que la posible implementación de soluciones como STIR/SHAKEN/RCD deben ser evaluadas bajo escenarios que incorporen los distintos elementos indicados por los operadores, tales como los costos, la complementariedad con las demás alternativas el grado de avance de la red IP, razón por la cual se mantiene dentro de las alternativas regulatorias que serán evaluadas en esta etapa del AIN. Sin perjuicio de lo anterior, los elementos técnicos planteados en los comentarios serán tenidos en cuenta como referentes para el seguimiento de la evolución tecnológica del sector y para eventuales análisis regulatorios futuros en la materia.

- *¿Qué parámetros y tecnologías considera más adecuados para estandarizar los modelos de monitoreo y filtrado de tráfico de voz? ¿Cómo garantizar que no se generen falsos positivos (que terminen afectando el tráfico legítimo), así como la protección de la privacidad de las comunicaciones y la proporcionalidad de las medidas?*

ASOBANCARIA

A su juicio, se requiere el uso de tecnologías que evalúen el riesgo de cada llamada considerandos variables como originador, receptor, recurrencia, velocidad y duración, ajustando continuamente los parámetros para reducir falsos positivos.

CLARO

Expone que los modelos de monitoreo y filtrado tienen igual un muy pequeño rango de falsos positivos; sin embargo, estos casos si se gestionan correctamente no debieran afectar de manera significativa a los clientes.

SSC

Considera especialmente efectivo el intercambio operativo de alertas entre PRST, mediante el cual los operadores de destino notifican oportunamente la existencia de quejas de usuarios o comportamientos anómalos asociados a numeraciones específicas. Con base en estas alertas, **SSC** aplica medidas de mitigación focalizadas, tales como el bloqueo de los números reportados, evitando acciones generalizadas sobre rutas o rangos completos. Indica que este mecanismo permite una respuesta rápida, basada en evidencia, reduce significativamente los falsos positivos y protege la prestación de

servicios legítimos, constituyéndose en una práctica alineada con los principios de proporcionalidad y cooperación inter operacional promovidos por la CRC.

TELEFÓNICA

Opina que los parámetros más adecuados deben basarse en métricas objetivas de comportamiento de red, tales como la Tasa de Establecimiento de Llamadas (CSR - Call Setup Rate) y la duración promedio de las llamadas (ACD - Average Call Duration). Adiciona que un volumen masivo de llamadas cortas o intentos fallidos desde un mismo origen es un indicador técnico estándar de robocalling. En su opinión, para garantizar la minimización de falsos positivos es crucial que los umbrales de detección no sean estáticos, sino que se ajusten dinámicamente mediante aprendizaje automático (machine learning), y que existan listas blancas para grandes generadores de tráfico legítimo (ej. call centers autorizados). Concluye en el sentido de decir que la protección de la privacidad se garantiza analizando metadatos de señalización (quién llama a quién y cuánto dura) sin intervenir el contenido de audio de la comunicación.

TIGO

Propone que los controles antifraude se basen en analítica de comportamiento a partir de parámetros como volumen de llamadas, duración promedio, tasa de intentos fallidos, patrones temporales atípicos, relación origen–destino y cambios abruptos frente al comportamiento histórico. Agrega que estos criterios permitirían identificar patrones sospechosos mediante análisis posterior y no en tiempo real. Asimismo, recomienda que las medidas que afecten el tráfico se adopten únicamente después de la verificación de la información, garantizando que sean posteriores, confirmadas y reversibles, con el fin de evitar falsos positivos, preservar la continuidad del servicio y proteger la privacidad de las comunicaciones al no interferir durante el establecimiento de la llamada.

ZANYA PINEDA

Menciona que los modelos de monitoreo y filtrado de tráfico de voz destinados a mitigar el fraude deben construirse necesariamente sobre parámetros técnicos objetivos, observables y no intrusivos, que respeten los límites constitucionales y legales del servicio de telecomunicaciones. En el caso específico de las llamadas de voz, cualquier esquema regulatorio debe partir de la premisa ineludible que el contenido de la comunicación no puede ser inspeccionado, grabado ni analizado, pues ello vulneraría el derecho fundamental a la privacidad de los usuarios. En consecuencia, los modelos de detección solo pueden operar sobre metadatos y comportamientos de red, nunca sobre la conversación en sí misma.

En este contexto, indica que los parámetros más adecuados para el monitoreo del tráfico de voz son aquellos asociados a patrones de comportamiento anómalos, tales como volúmenes inusuales de llamadas en periodos cortos, intentos repetitivos hacia múltiples destinos, duraciones atípicas, ratios elevadas de llamadas no contestadas, correlaciones entre rangos de numeración y destinos específicos, o cambios abruptos en la geolocalización lógica del tráfico. Estos indicadores, analizados de manera conjunta y contextual, pueden servir como señales de alerta temprana, pero no constituyen prueba suficiente de fraude por sí mismos. Precisamente por esta razón, indica que el filtrado automático y definitivo del tráfico basado únicamente en modelos algorítmicos representa un riesgo significativo de falsos positivos, con impactos directos sobre comunicaciones legítimas.

Desde la perspectiva del principio de proporcionalidad, asegura que cualquier medida de filtrado debe cumplir tres condiciones esenciales: idoneidad, necesidad y proporcionalidad en sentido estricto. Esto implica que el filtrado no puede ser la primera ni la única respuesta frente a una alerta, sino una medida gradual, sujeta a verificación posterior. Las señales de riesgo deben activar procesos de análisis adicionales, contrastarse con información histórica, cruzarse con reportes de usuarios y, en caso de duda razonable, permitir la continuidad del tráfico mientras se adelantan las verificaciones correspondientes.

Asimismo, añade que resulta indispensable que los esquemas de monitoreo y filtrado incorporen mecanismos claros de reclamación y corrección, tanto para los usuarios finales como para los actores del sector afectados por bloqueos o marcaciones indebidas. La existencia de canales ágiles para impugnar decisiones automáticas, solicitar revisiones técnicas y obtener restablecimientos oportunos del servicio no solo protege derechos, sino que fortalece la legitimidad del sistema y la confianza en las medidas regulatorias adoptadas.

Añade que, en términos de gobernanza, el monitoreo del tráfico de voz no puede quedar sujeto a decisiones opacas o discrecionales de un número reducido de operadores, por lo que resulta fundamental que la Comisión establezca estándares mínimos comunes, criterios transparentes y obligaciones de trazabilidad sobre las decisiones de filtrado, de manera que estas puedan ser auditadas posteriormente. La auditoría regulatoria cumple un rol clave para evitar abusos, prácticas discriminatorias o el uso del filtrado como herramienta de control del mercado bajo el pretexto de la lucha contra el fraude.

Finaliza mencionando que la protección de la privacidad debe ser un eje transversal de cualquier modelo de monitoreo, lo que implica limitar estrictamente el tratamiento de datos al mínimo necesario, garantizar la anonimización cuando sea posible, definir tiempos claros de retención de información y asegurar que los datos recolectados no sean reutilizados con fines distintos a la prevención del fraude.

RESPUESTA CRC:

A partir de los comentarios recibidos, se identifican puntos de consenso entre los agentes respecto a los parámetros y condiciones que deberían orientar los modelos de monitoreo y filtrado del tráfico de voz para la mitigación del fraude. En particular, **ASOBANCARIA**, **TELEFÓNICA** y **TIGO** coinciden en que estos modelos deben basarse en parámetros técnicos objetivos asociados al comportamiento del tráfico, tales como volumen de llamadas, duración promedio, recurrencia, velocidad de generación de llamadas, tasa de intentos fallidos o relaciones entre origen y destino. En la misma línea, **TELEFÓNICA** destaca el uso de métricas de red como la tasa de establecimiento de llamadas (CSR) y la duración promedio de las llamadas (ACD) para identificar patrones asociados a robocalling.

Asimismo, los agentes coinciden en que los sistemas de monitoreo pueden generar falsos positivos, aunque **CLARO** considera que estos son marginales y gestionables, mientras que **SSC** señala que el uso de mecanismos focalizados basados en alertas específicas permite reducir su impacto. Adicionalmente, existe coincidencia en que estos modelos deben preservar la privacidad de las comunicaciones, operando exclusivamente sobre metadatos de señalización y sin analizar el contenido de las llamadas, como lo destacan **TELEFÓNICA** y **ZANYA PINEDA**.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

No obstante, se observan divergencias respecto al alcance y momento de aplicación de las medidas de filtrado del tráfico sospechoso. Por una parte, **CLARO** considera viable la implementación operativa de sistemas de monitoreo y filtrado siempre que se gestionen adecuadamente los posibles falsos positivos. En contraste, **TIGO** y **ZANYA PINEDA** advierten que las medidas que afecten el tráfico deberían adoptarse únicamente después de procesos de verificación adicionales, de manera que las acciones sean confirmadas, proporcionales y reversibles, evitando afectar comunicaciones legítimas. A su vez, **SSC** plantea que las medidas de mitigación deberían ser focalizadas sobre numeraciones o casos específicos, a partir del intercambio de alertas entre operadores, en lugar de aplicar bloqueos generalizados sobre rutas o rangos completos de numeración.

En cuanto a las propuestas, los agentes plantean diversas medidas orientadas a fortalecer la prevención del fraude. Así, **ASOBANCARIA** y **TELEFÓNICA** sugieren el uso de tecnologías analíticas y modelos dinámicos de detección, incluyendo técnicas de aprendizaje automático para ajustar los umbrales de identificación de patrones sospechosos. Por su parte, **SSC** propone fortalecer los mecanismos de cooperación inter operacional e intercambio de alertas para facilitar respuestas rápidas y focalizadas frente a numeraciones reportadas por comportamientos anómalos. De manera complementaria, **TIGO** plantea que las medidas de mitigación deben aplicarse de forma gradual y verificable, mientras que **ZANYA PINEDA** propone incorporar garantías regulatorias adicionales, tales como criterios transparentes para el filtrado, mecanismos de reclamación y corrección, auditoría regulatoria de las decisiones de bloqueo y salvaguardas para la protección de la privacidad, incluyendo la limitación del tratamiento de datos al mínimo necesario y la definición de tiempos claros de retención de la información.

En este contexto, la CRC considera que las propuestas formuladas por los agentes aportan elementos útiles para el análisis de los parámetros y tecnologías más adecuados para la estandarización de modelos de monitoreo y filtrado del tráfico de voz, así como para la identificación de mecanismos que permitan minimizar la generación de falsos positivos que puedan afectar el tráfico legítimo, garantizando al mismo tiempo la protección de la privacidad de las comunicaciones y la proporcionalidad de las medidas que eventualmente se adopten orientadas a la mitigación del fraude en servicios de voz. No obstante, la eventual incorporación de estas medidas en el marco regulatorio estará sujeta a los resultados del correspondiente proceso de evaluación de alternativas regulatorias, el cual deberá considerar, entre otros aspectos, su viabilidad técnica, su proporcionalidad frente a los riesgos identificados y su compatibilidad con las competencias regulatorias atribuidas a la Comisión.

De igual forma, la Comisión coincide con los agentes en que cualquier esquema de monitoreo del tráfico debe sustentarse en el análisis de parámetros técnicos y metadatos asociados al comportamiento de las comunicaciones, y en ningún caso en la inspección del contenido de las llamadas, en atención a las garantías constitucionales y legales que protegen la privacidad de las comunicaciones. No obstante, se resalta que los mecanismos de monitoreo y etiquetado del tráfico se desarrollan con anterioridad al establecimiento de la llamada, con el propósito de prevenir el contacto fraudulento con los usuarios finales a través de los servicios tradicionales de voz, sin que ello implique, en ningún caso, la intervención o análisis del contenido de la comunicación.

- *¿Qué actores deberían participar en una plataforma nacional de intercambio de alertas sobre fraudes en llamadas? ¿Qué mecanismos de gobernanza y protección de datos serían necesarios?*

ASOBANCARIA

Comenta que una plataforma nacional de alertas debería involucrar a entes gubernamentales, PRST, entidades financieras y grandes conglomerados comerciales, bajo un esquema de gobernanza claro. En su sentir, esta articulación permitiría compartir alertas oportunas, identificar patrones de fraude y fortalecer la respuesta coordinada del ecosistema frente a incidentes de fraude.

CLARO

considera que los actores clave son operadores fijos y móviles, CRC, CSIRT Nacional; proveedores de soluciones antifraude; empresas con alto volumen de llamadas y proveedores de contenido, y los carriers internacionales.

SFC

Menciona que, si bien la infraestructura técnica de la plataforma es competencia de la CRC y los operadores, su alcance operativo debe ser intersectorial. Para la SFC, el éxito de esta medida depende de que las entidades financieras no sean solo receptoras de información, sino actores activos en el reporte de alertas. El interés institucional radica en que esta plataforma funcione como un mecanismo de debida diligencia para prevenir el fraude sistémico, asegurando que la información de seguridad fluya con la misma rapidez con la que operan las redes criminales, protegiendo así la confianza en el ecosistema financiero.

Ahora bien, en lo que refiere a la gobernanza y protección de los datos, indica que cada uno de los sectores participantes deberán verificar la efectividad de los controles adoptados para garantizar el adecuado tratamiento de los datos de los usuarios, de conformidad con el régimen aplicable a cada sector, por lo que se requiere de estrategias articuladas entre las diferentes autoridades y partes interesadas.

SSC

Considera que una plataforma nacional de intercambio de alertas sobre fraude en llamadas de voz debería contar, como mínimo, con la participación de los siguientes actores del ecosistema:

• Proveedores de Redes y Servicios de Telecomunicaciones (PRST) que gestionan tráfico de voz, incluidos operadores fijos, móviles y de larga distancia internacional, en su calidad de responsables de la gestión técnica del tráfico y de la aplicación de medidas de mitigación.
• Operadores de destino, en tanto son quienes reciben de manera directa los reportes y quejas de los usuarios finales y pueden identificar tempranamente eventos de fraude.
• Proveedores de plataformas tecnológicas de comunicaciones, tales como plataformas OTT, CPaaS o contact center en la nube, en la medida en que originan o gestionan volúmenes relevantes de tráfico de voz.
• La Comisión de Regulación de Comunicaciones (CRC), en su rol de definición de lineamientos regulatorios, supervisión y seguimiento del funcionamiento del esquema, sin que ello implique necesariamente la operación técnica de la plataforma.
• Autoridades competentes, únicamente para efectos de investigación y judicialización, cuando exista fundamento legal y solicitud expresa.

SSC considera indispensable que la plataforma se rija por un esquema de gobernanza claro, que contemple, al menos, los siguientes elementos:

• Finalidad específica y limitada, orientada exclusivamente a la prevención y mitigación del fraude en llamadas de voz.
• Intercambio de información mínima necesaria, circunscrita a metadatos técnicos y operativos (por ejemplo, numeración involucrada, tipo de evento, ventana temporal y operador reportante), excluyendo el contenido de las comunicaciones.
• Trazabilidad y responsabilidad sobre las alertas, identificando el origen de la alerta, la fecha de reporte y los criterios técnicos utilizados.
• Controles de acceso, auditoría y seguridad de la información, que prevengan usos indebidos o no autorizados.
• Cumplimiento de los principios de protección de datos personales, en particular minimización, finalidad, proporcionalidad y retención limitada.

TIGO

Este operador indica que una plataforma nacional de intercambio de alertas sobre fraude en llamadas debe incorporar la participación coordinada de entidades públicas (CRC, MinTIC, SIC y autoridades de seguridad), todos los actores del ecosistema de voz (carriers, PRST, agregadores, call centers y fabricantes de tecnología), gestores de información antifraude y usuarios. En materia de gobernanza, plantea que las entidades públicas definan obligaciones y responsabilidades para todos los actores del sistema, participen activamente en la investigación de los responsables de fraude y estructuren un régimen sancionatorio justo que priorice la penalización de quienes ejecutan o promueven actividades fraudulentas. Asimismo, resalta que un sistema sancionatorio efectivo para asignatarios de recursos de identificación y carriers internacionales constituye un mecanismo clave de disuasión, pues centrar los esfuerzos únicamente en la detección resulta costoso e insuficiente frente a la adaptación de las modalidades delictivas.

ZANYA PINEDA

Menciona que la plataforma debe estructurarse bajo un modelo de participación amplia, plural y equilibrada, que refleje la realidad del ecosistema de telecomunicaciones y evite trasladar el control del sistema a un número reducido de operadores móviles. En este sentido, indica que los actores que deben participar no pueden limitarse exclusivamente a los PRSTM, sino que deben incluir a usuarios finales, operadores móviles, operadores de tránsito, PSRT, OTT, CaaPS, integradores tecnológicos, y autoridades competentes, con roles claramente diferenciados y complementarios.

Añade también que el usuario final debe ser reconocido como un actor central del sistema, en tanto es el primer eslabón capaz de identificar con certeza la materialización del fraude. Su participación se materializa a través de mecanismos sencillos, accesibles y estandarizados de reporte, que alimenten la plataforma con alertas cualificadas. Excluir al usuario o relegarlo a un rol pasivo desconoce la naturaleza misma del fraude en servicios de voz, que solo se evidencia durante la interacción directa.

Resalta que los PRSTM y los operadores de tránsito cumplen un rol técnico relevante pero no deben ostentar control exclusivo ni decisorio sobre la validación o las consecuencias de dichas alertas, por lo que su función debe estar delimitada a la colaboración técnica y a la ejecución de medidas proporcionales definidas bajo estándares regulatorios claros.

Añade que los OTT, CaaPS e integradores tecnológicos deben participar activamente, en tanto forman parte real y legítima de la cadena de valor del tráfico de voz, especialmente en escenarios internacionales o híbridos, por lo que su exclusión no solo debilitaría la trazabilidad del sistema, sino que reforzaría una visión fragmentada y sesgada del problema, además de afectar actores que generan empleo, innovación y competitividad en el país.

En cuanto a la administración, señala que la plataforma debe operar bajo un esquema liderado y supervisado por la Comisión, como autoridad técnica e independiente, pero con reglas claras que impidan la captura regulatoria o el uso estratégico de la información por parte de actores dominantes, por lo que la Comisión debe definir los estándares mínimos de operación, criterios de validación de alertas, niveles de acceso a la información, responsabilidades de cada actor y mecanismos de auditoría periódica, garantizando transparencia, trazabilidad y rendición de cuentas.

Asegura que es fundamental que la gobernanza incorpore un modelo de decisiones no automatizado ni discrecional, en el que las alertas no se traduzcan automáticamente en bloqueos, listas de no originación (DNO) o sanciones, sino que activen procesos graduales de análisis, contraste y verificación, ya que este enfoque protege el debido proceso, reduce el riesgo de falsos positivos y evita que la plataforma se convierta en un instrumento de exclusión o control del mercado.

En materia de protección de datos, añade que la plataforma debe regirse estrictamente por los principios de minimización, finalidad, proporcionalidad y seguridad de la información, en el sentido que la información compartida debe limitarse a los datos estrictamente necesarios para la mitigación del fraude, evitando el tratamiento del contenido de las comunicaciones y privilegiando el uso de metadatos anonimizados o seudonimizados cuando sea posible. Asimismo, resalta que deben establecerse políticas claras de retención de datos, con plazos definidos y mecanismos de eliminación segura, así como controles de acceso diferenciados según el rol de cada actor.

Finaliza añadiendo que es indispensable implementar mecanismos de auditoría técnica y jurídica, que permitan verificar el uso adecuado de la información, detectar posibles abusos y garantizar que las alertas no sean utilizadas con fines distintos a la prevención del fraude, como prácticas anticompetitivas o estrategias de bloqueo selectivo, ya que la confianza en la plataforma dependerá, en gran medida, de la existencia de estas salvaguardas y de la percepción de imparcialidad en su operación.

RESPUESTA CRC:

Las respuestas recibidas frente a la pregunta sobre los actores que deberían participar en una plataforma nacional de intercambio de alertas sobre fraudes en llamadas muestran, como punto de coincidencia principal, que los agentes consideran necesario un esquema de participación amplio e intersectorial, y no una herramienta restringida exclusivamente a los operadores de telecomunicaciones. **ASOBANCARIA** plantea la participación de entes gubernamentales, PRST, entidades financieras y grandes conglomerados comerciales, al considerar que esta articulación permitiría compartir alertas oportunas, identificar patrones y fortalecer una respuesta coordinada del ecosistema.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En la misma dirección, **CLARO** identifica como actores clave a los operadores fijos y móviles, la CRC, el CSIRT Nacional, los proveedores de soluciones antifraude, las empresas con alto volumen de llamadas, los proveedores de contenido y los carriers internacionales. La **SFC** también insiste en que, aunque la infraestructura técnica pueda recaer en la CRC y los operadores, el alcance operativo debe ser intersectorial y requiere la participación de las entidades financieras en el reporte de alertas. En conjunto, estas respuestas reflejan una visión convergente según la cual la efectividad de la plataforma dependería de incorporar a los distintos actores que detectan, originan, gestionan o reciben información relevante sobre eventos de fraude.

Aun cuando existe esa coincidencia en torno a la necesidad de una participación amplia, las respuestas difieren en la manera de delimitar el universo de actores y en el peso asignado a cada uno de ellos dentro del esquema. SSC propone una conformación mínima que incluya PRST que gestionan tráfico de voz, operadores de destino, proveedores de plataformas tecnológicas de comunicaciones como OTT, CPaaS o contact center en la nube, la CRC y autoridades competentes, estas últimas únicamente para investigación y judicialización cuando exista fundamento legal y solicitud expresa. **TIGO** amplía aún más el espectro al incluir entidades públicas como la CRC, el MinTIC, la SIC y las autoridades de policía, así como carriers, PRST, agregadores, call centers, fabricantes de tecnología, gestores de información antifraude y usuarios.

Por su parte, **ZANYA PINEDA** insiste en que la plataforma debe estructurarse bajo un modelo plural y equilibrado que incluya usuarios finales, operadores móviles, operadores de tránsito, PSRT, OTT, CaaPS, integradores tecnológicos y autoridades competentes, con roles diferenciados y complementarios. Esta última respuesta introduce, además, una preocupación explícita por evitar que el control del sistema quede concentrado en un grupo reducido de operadores móviles, lo que marca una diferencia relevante frente a aproximaciones más centradas en los agentes tradicionales del mercado de voz.

Diversos actores coinciden en que la CRC debe orientar, liderar o supervisar el sistema, sin necesariamente operarlo. Claro la considera actor clave; **SSC** le asigna funciones regulatorias y de supervisión; **ZANYA PINEDA** sugiere un esquema liderado por la Comisión como autoridad técnica e independiente. La **SFC** indica que la infraestructura técnica es responsabilidad de la CRC y operadores, pero destaca que el éxito dependerá también del aporte de otros sectores, especialmente el financiero. Aunque no hay consenso sobre el diseño institucional, se reconoce que la Comisión debe definir estándares, coordinar y dar seguimiento al esquema en colaboración con autoridades y agentes del sector.

En materia de gobernanza, las respuestas también presentan varias semejanzas. **SSC** plantea que la plataforma debe regirse por una finalidad específica y limitada a la prevención y mitigación del fraude en llamadas de voz, con intercambio de información mínima necesaria, trazabilidad de las alertas, controles de acceso, auditoría y seguridad de la información, así como observancia de principios de protección de datos personales. La **SFC**, desde una perspectiva sectorial, señala que cada sector participante deberá verificar la efectividad de sus controles para asegurar el adecuado tratamiento de los datos conforme al régimen aplicable, lo que exige estrategias articuladas entre autoridades y partes interesadas. **TIGO**, en cambio, pone un énfasis particular en que las entidades públicas definan obligaciones y responsabilidades para todos los actores, participen activamente en la investigación de los responsables del fraude y estructuren un régimen sancionatorio justo, especialmente respecto de asignatarios de recursos de identificación y carriers internacionales.

ZANYA PINEDA complementa esta discusión al proponer que la CRC defina estándares mínimos de operación, criterios de validación de alertas, niveles de acceso a la información, responsabilidades y mecanismos de auditoría periódica, al tiempo que prevenga la captura regulatoria y el uso estratégico de la información por actores dominantes. En consecuencia, las respuestas coinciden en exigir reglas claras de gobernanza, aunque difieren en el mayor o menor énfasis que asignan a la supervisión, la trazabilidad, el régimen sancionatorio y las garantías de neutralidad del sistema.

Frente a la protección de datos y las salvaguardas necesarias, también se advierten puntos comunes y algunas diferencias. **SSC** y **ZANYA PINEDA** coinciden en que la información compartida se debe limitarse a los datos estrictamente necesarios para la mitigación del fraude, privilegiando metadatos técnicos y operativos y excluyendo el contenido de las comunicaciones. Ambas respuestas resaltan principios como minimización, finalidad, proporcionalidad y seguridad de la información, y **ZANYA PINEDA** añade la conveniencia de usar datos anonimizados o seudonimizados cuando sea posible, establecer políticas claras de retención y eliminación segura, y diferenciar los niveles de acceso según el rol de cada actor.

La SFC, aunque no desarrolla un esquema técnico específico, también destaca que cada sector debe asegurar el tratamiento adecuado de los datos conforme al régimen que le resulte aplicable. Adicionalmente, **ZANYA PINEDA** enfatiza la necesidad de que las alertas no produzcan automáticamente bloqueos, DNO o sanciones, sino que activen procesos graduales de análisis, contraste y verificación, como mecanismo para proteger el debido proceso, reducir falsos positivos y evitar que la plataforma sea utilizada con fines anticompetitivos o de exclusión selectiva.

Las respuestas recibidas sirven como insumo para que la CRC precise el alcance de las medidas asociadas a esta temática específica y valore su viabilidad dentro de las alternativas regulatorias, en particular en relación con la identificación de los actores que podrían participar en una plataforma de intercambio de alertas y en relación con sus parámetros de funcionamiento.

- *¿Cuáles considera que serían los retos técnicos y económicos de construir y operar la plataforma de alertas bajo un modelo centralizado vs un modelo distribuido? ¿Qué mecanismos considera deben ser adoptados y estandarizados para validar la veracidad de una alerta antes de su distribución mediante la plataforma de intercambio?*

CLARO

Considera que existen medidas más eficaces que la implementación de una plataforma centralizada, la cual implicaría altos costos operativos y administrativos. Por ello, se solicita a la CRC evaluar primero la efectividad de la suspensión provisional, fortalecer los procesos de recuperación y articulación sectorial, y realizar un Análisis de Impacto Normativo antes de adoptar nuevas soluciones técnicas. Expone que, dado el tiempo y los retos de implementación, la medida propuesta no es viable.

SSC

En relación con la arquitectura de la plataforma, **SSC** identifica las siguientes consideraciones:

• Un modelo centralizado puede facilitar una visión agregada del ecosistema y la aplicación uniforme de criterios, pero presenta retos asociados a mayores costos de implementación y operación, riesgos de concentración de información sensible y posibles cuellos de botella operativos.

Un modelo distribuido, basado en estándares mínimos comunes de intercambio, permite una implementación más gradual, reduce costos, favorece la agilidad operativa y limita la concentración de datos sensibles, aunque requiere un mayor esfuerzo de coordinación y estandarización entre los actores.

Desde la perspectiva de **SSC**, un modelo distribuido con lineamientos técnicos comunes definidos por la CRC resulta más viable en términos técnicos y económicos, al menos en una fase inicial de implementación.

Por otro lado, menciona que para garantizar la confiabilidad del esquema y evitar la generación de falsos positivos o abusos, considera necesario estandarizar, previo a la distribución de una alerta, los siguientes mecanismos:

• Definición objetiva de los criterios que constituyen una alerta válida, tales como la existencia de múltiples quejas de usuarios, patrones de tráfico anómalos consistentes o reincidencia.
• Aporte de evidencia técnica mínima, suficiente para sustentar la alerta, sin incluir información sensible o contenido de las comunicaciones.
• Clasificación del nivel de severidad de la alerta, diferenciando alertas informativas de alertas críticas.
• Mecanismos de revisión, actualización y corrección, que permitan aclarar o retirar alertas cuando se identifiquen errores.
• Asignación de responsabilidad al emisor de la alerta, evitando reportes anónimos o sin sustento técnico.

SSC considera que una plataforma nacional de intercambio de alertas debe diseñarse bajo principios de cooperación interoperatorial, proporcionalidad, trazabilidad y protección de datos, de manera que permita una mitigación eficaz y oportuna del fraude en llamadas de voz, sin generar cargas desproporcionadas ni afectar la prestación de servicios legítimos.

ZANYA PINEDA

Al respecto menciona que la creación de una plataforma nacional de intercambio de alertas sobre fraude en llamadas de voz debe concebirse como un mecanismo estructural de coordinación sectorial, y no como una herramienta de control centralizado del tráfico. Indica que su diseño debe partir de una premisa esencial que ha sido históricamente subestimada en las discusiones regulatorias: el usuario final es el primer y único actor que puede identificar con certeza cuándo una llamada es fraudulenta, dado que el fraude se materializa a través de la interacción directa y del uso de información parcialmente verdadera que solo se revela durante la conversación.

En este sentido, añade que el insumo principal de la plataforma no debe ser exclusivamente el análisis técnico de tráfico, sino el reporte ciudadano, entendido como una señal cualificada que activa procesos de verificación, trazabilidad y eventual actuación administrativa o judicial.

Añade que, desde el punto de vista técnico y económico, un modelo centralizado de plataforma de alertas presenta riesgos significativos, por lo que concentrar la recepción, validación y distribución de

alertas en una única entidad o infraestructura puede derivar en cuellos de botella operativos, altos costos de implementación y mantenimiento, y riesgos de captura regulatoria o uso estratégico de la información. Además, un sistema centralizado puede convertirse, de facto, en un mecanismo de control indirecto del tráfico, con impactos sobre la competencia y la neutralidad del mercado.

En contraste, señala que un modelo distribuido (basado en estándares comunes, interoperabilidad y responsabilidades compartidas) ofrece ventajas claras en términos de resiliencia, escalabilidad y neutralidad tecnológica. En este esquema, cada actor mantiene sus propios sistemas de recepción y gestión de alertas, pero comparte información relevante bajo reglas claras y homogéneas definidas por la Comisión. Este enfoque reduce la dependencia de un único punto de control, facilita la participación de actores de distinto tamaño y evita que la plataforma se convierta en una barrera de entrada o en un instrumento de exclusión.

Añade que la Comisión debe establecer mecanismos de supervisión y auditoría periódica que permitan evaluar el uso de la plataforma, prevenir abusos y asegurar que las alertas no sean utilizadas como herramientas de competencia desleal, bloqueo estratégico o discriminación de actores del mercado. La
confianza en el sistema depende, en gran medida, de que todos los participantes perciban reglas claras, equitativas y aplicadas de manera uniforme.

Finaliza indicando que, más allá de su función operativa, una plataforma nacional de alertas de fraude en voz constituye una herramienta estratégica de política pública, en tanto permite identificar tendencias, patrones emergentes y modalidades de fraude, alimentar procesos pedagógicos dirigidos a los usuarios y orientar decisiones regulatorias basadas en evidencia. Su valor no radica en el bloqueo inmediato, sino en la construcción progresiva de trazabilidad, responsabilidad y conocimiento colectivo del fenómeno.

RESPUESTA CRC:

Antes de pronunciarse de manera concreta en relación con estas respuestas, la Comisión considera oportuno recordar que, en líneas precedentes, específicamente en el análisis de las respuestas a los comentarios de la TEMÁTICA 2, la CRC concluyó que la TEMÁTICA 2 original debe separarse en dos temáticas distintas en aras de aportar claridad a la hora de proceder con la evaluación. En la nueva TEMÁTICA 2 se incluirá, como parte de las alternativas regulatorias, la posibilidad de contar con una plataforma nacional de alertas centralizada para generar notificaciones en tiempo real a todos los PRST y entidades conectadas o, en su lugar, establecer mecanismos formales de coordinación entre los PRST y la CRC, así como otras entidades (no necesariamente mediante una plataforma). A su turno, en la nueva temática 3 se analizarán las alternativas regulatorias para la definición o no de lineamientos para monitoreo y etiquetado de tráfico mediante la identificación de patrones sospechosos. En cuanto a la nueva temática 3, la CRC ya aclaró que el monitoreo y etiquetado de tráfico deben ser incluidos como parte de la evaluación de las alternativas regulatorias, y está de acuerdo en que ningún mecanismo de monitoreo de voz debe basarse en inspección de contenido.

Una vez aclarado lo anterior, y con base en las respuestas recibidas a la consulta, se identifican coincidencias relevantes entre los agentes respecto a los retos técnicos y económicos de construir y operar la plataforma de alertas bajo un modelo centralizado en comparación con un modelo distribuido.

En términos generales, **CLARO** opina que la plataforma centralizada es costosa y que la CRC debería considerar otras alternativas. **SSC** coincide en que un modelo centralizado representa mayores costos de implementación y operación, así como riesgos de concentración de información sensible. En esa misma línea, **ZANYA PINEDA** advierte que un modelo centralizado de plataforma de alertas presenta riesgos significativos, como cuellos de botella operativos, altos costos de implementación y mantenimiento, y riesgos de captura regulatoria o uso estratégico de la información.

De otra parte, **SSC** sostiene que un modelo distribuido permite una implementación más gradual, reduce costos y favorece la agilidad. En esa misma línea, **ZANYA PINEDA** afirma que un modelo distribuido ofrece ventajas claras en términos de resiliencia, escalabilidad y neutralidad tecnológica, toda vez que cada actor mantiene sus propios sistemas de recepción y gestión de alertas, pero comparte información relevante bajo reglas claras y homogéneas definidas por la Comisión. **ZANYA PINEDA** adiciona, en resumen, que el insumo principal de la plataforma no debe ser exclusivamente el análisis técnico de tráfico, sino el reporte ciudadano, entendido como una señal cualificada que activa procesos de verificación, trazabilidad y eventual actuación administrativa o judicial.

En consideración de lo anterior, la CRC identifica que los comentarios recibidos aportan elementos como insumos técnicos y económicos relevantes para tener en cuenta durante el proceso de evaluación que se desarrolla en el marco del AIN, los cuales serán considerados como parte del análisis de alternativas regulatorias, especialmente en lo relacionado con los retos de un modelo centralizado frente a un modelo distribuido.

- *¿Qué ventajas y desafíos observa en la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias? ¿Considera que esta medida podría ser efectiva para facilitar la identificación y denuncia de fraudes por parte de los usuarios?*

ASOBANCARIA

Comenta que la efectividad de la medida es limitada si se implementa de manera aislada, pero podría aportar ventajas si se articula con las demás temáticas del proyecto.

CLARO

Expone que la medida no generaría el impacto esperado, ya que los usuarios no conocen los rangos de numeración. Además, su implementación implicaría desafíos como la reducción de la disponibilidad general de números al reservar rangos para usos comerciales, altos costos de ajuste en sistemas y procesos para operadores y plataformas para incorporar los rangos, incluyendo actualización de señalización y registros gubernamentales; la necesidad de establecer normativas y controles claros con sanciones por incumplimiento, y el riesgo de que las estafas se realicen incluso desde rangos autorizados. En conclusión, señala que no se identifican ventajas significativas en su adopción.

PTC

Manifiesta que la medida propuesta resulta adecuada.

SSC

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Desde su perspectiva, la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias presenta algunas ventajas potenciales en términos de identificación del tipo de llamada por parte del usuario final, pero también desafíos técnicos, operativos y de efectividad, que deben ser cuidadosamente considerados antes de su adopción.

Frente a las ventajas potenciales destaca las siguientes:

• Facilitación de la identificación por parte del usuario. El uso de rangos exclusivos podría permitir que los usuarios reconozcan de manera más sencilla que una llamada tiene fines comerciales o publicitarios, lo que podría contribuir a una toma de decisiones más informada al momento de atender la llamada.
• Apoyo a la denuncia y gestión de reclamos. Al existir rangos claramente identificables, los usuarios podrían asociar con mayor facilidad una llamada sospechosa a un tipo de tráfico específico, lo que podría facilitar la denuncia de usos indebidos y la gestión posterior por parte de los operadores.
• Claridad regulatoria sobre el uso de la numeración. La medida podría aportar mayor claridad respecto a los usos permitidos de ciertos rangos, facilitando la supervisión y el control regulatorio.

En cuanto a los desafíos y limitaciones, menciona lo siguiente:

• Riesgo de pérdida de efectividad por saturación o bloqueo generalizado. En la práctica, los usuarios tienden a bloquear de forma sistemática rangos identificados como comerciales, lo que puede afectar comunicaciones legítimas y reducir significativamente la contactabilidad de servicios válidos.
• Incentivo a la evasión. La creación de rangos exclusivos puede incentivar a actores fraudulentos a migrar hacia otros rangos de numeración o a utilizar esquemas de suplantación, sin una reducción real del fraude.
• Impacto operativo y de adopción. La migración de servicios existentes hacia nuevos rangos implica costos técnicos y operativos, tanto para PRST como para clientes empresariales, y requiere tiempos de adaptación.
• Limitada efectividad frente a fraude sofisticado. La medida resulta más efectiva para clasificar el tipo de llamada que para prevenir activamente el fraude, dado que no resuelve el problema de fondo relacionado con la trazabilidad del originador real.

Frente a la efectividad para la identificación y denuncia de fraudes, **SSC** considera que la creación de rangos exclusivos puede contribuir de manera parcial a la identificación del tipo de llamada por parte del usuario, pero no constituye una solución suficiente ni determinante para la prevención del fraude. Su efectividad depende de que se complemente con otros mecanismos, tales como etiquetado informativo, monitoreo de comportamiento, cooperación interoperatorial y trazabilidad técnica.

En conclusión, **SSC** considera que los rangos exclusivos de numeración para llamadas comerciales y publicitarias pueden aportar claridad y apoyo informativo al usuario, pero presentan limitaciones estructurales y riesgos de evasión, por lo que su adopción debería evaluarse como una medida complementaria, y no sustitutiva, dentro de un enfoque integral de mitigación del fraude en llamadas de voz.

TELEFÓNICA

Opina que la creación de rangos exclusivos (como un prefijo específico para ventas) presenta la ventaja teórica de facilitar al usuario la identificación de una llamada comercial. Sin embargo, **TELEFÓNICA** añade que, en la práctica, se presentan desafíos operativos significativos ya que implicaría una migración masiva de numeración para miles de empresas, generando costos elevados y confusión inicial. Además, este operador advierte que su efectividad para prevenir el fraude es limitada si no se controla el spoofing, toda vez que los delincuentes podrían simplemente enmascarar sus llamadas usando esos mismos prefijos exclusivos para engañar al usuario. Por tanto, sugiere que es más efectivo enfocar los esfuerzos en la autenticación del origen (validar quién llama) que en la segregación de la numeración (qué número usa).

TIGO

Considera que la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias ofrecería ventajas como facilitar a los usuarios la identificación del propósito de la llamada, reducir la confusión entre comunicaciones personales, institucionales y comerciales, permitir decisiones informadas sobre su atención, y mejorar la capacidad de denuncia frente a posibles fraudes. Adiciona que contribuiría a limitar el uso indebido de numeración ordinaria para fines comerciales y facilitaría la identificación institucional de proveedores y campañas específicas.

Entre los desafíos señala la definición y asignación adecuada de los rangos, la delimitación de su alcance, la adaptación técnica de redes y sistemas de facturación, el establecimiento de controles de acceso y mecanismos sancionatorios eficaces, la definición de obligaciones de registro e identificación de los usuarios de estos rangos y la migración operativa de las entidades hacia la nueva numeración.

ZANYA PINEDA

Menciona que la medida puede aportar beneficios marginales en términos de identificación visual para el usuario, pero no constituye una solución estructural ni suficiente para la prevención del fraude en servicios de voz. Esta medida parte de la premisa limitada que el fraude se origina principalmente desde llamadas etiquetadas como comerciales, cuando en la práctica los esquemas fraudulentos evolucionan constantemente y se adaptan rápidamente a cualquier restricción normativa, migrando hacia otros rangos de numeración, incluyendo numeración fija, móvil tradicional o incluso numeración internacional.

Añade que uno de los principales riesgos de esta medida es que desplaza el problema en lugar de resolverlo ya que los actores fraudulentos no dependen de un rango específico para operar. Por el contrario, su comportamiento se caracteriza por la flexibilidad técnica y la explotación de asimetrías regulatorias. En consecuencia, asegura que la asignación de rangos exclusivos podría generar una falsa sensación de seguridad, tanto para los usuarios como para los reguladores, mientras el fraude continúa manifestándose a través de otros esquemas de numeración menos vigilados.

Asegura que la medida implica costos operativos y técnicos relevantes para todos los actores del ecosistema de voz, ya que los operadores y proveedores de servicios deberían adaptar sistemas de enrutamiento, facturación, monitoreo y señalización, así como actualizar bases de datos de numeración y plataformas de atención al usuario. Estos costos no son menores y podrían impactar de manera desproporcionada a actores pequeños o medianos, generando barreras de entrada y afectando la competencia, sin una correlación directa con una reducción efectiva del fraude.

Por otro lado resalta que, desde la perspectiva del usuario final, existe también el riesgo de confusión y fatiga informativa, especialmente si la medida no va acompañada de una estrategia sólida de pedagogía y comunicación. La simple existencia de un rango exclusivo no garantiza que el usuario comprenda su significado, sepa cómo actuar frente a una llamada sospechosa o distinga entre una llamada comercial legítima y una fraudulenta. Sin educación clara y sostenida, el etiquetado por rango puede perder rápidamente su efectividad y convertirse en un elemento irrelevante para la toma de decisiones del usuario.

Señala que otro aspecto crítico es que esta medida no aborda el problema central de la trazabilidad y la responsabilidad en la cadena de la llamada. La numeración, por sí sola, no permite identificar con certeza al originador real del tráfico ni garantiza que el uso del número esté debidamente autorizado. En ausencia de controles adicionales sobre autenticación del origen, conservación de registros y cooperación entre actores, los rangos exclusivos pueden ser fácilmente explotados, suplantados o utilizados como fachada para actividades ilícitas.

Asimismo, añade que el riesgo de que la creación de rangos exclusivos derive en prácticas de bloqueo preventivo o discriminatorio, especialmente si los operadores móviles deciden tratar todo el tráfico proveniente de dichos rangos como intrínsecamente riesgoso. Este enfoque no solo afectaría llamadas comerciales legítimas (incluidas aquellas relacionadas con servicios esenciales como salud, educación o servicios financieros), sino que también podría vulnerar principios de proporcionalidad, neutralidad y libre prestación de servicios.

Finaliza indicando que, en términos regulatorios, la efectividad de los rangos exclusivos depende de su articulación con otras medidas complementarias, como esquemas de reporte por parte del usuario, plataformas de intercambio de alertas, estándares mínimos de monitoreo de tráfico y responsabilidades claras a lo largo de la cadena de intermediación. Sin este enfoque integral, los rangos exclusivos corren el riesgo de convertirse en una solución aislada, reactiva y fácilmente evadible.

RESPUESTA CRC:

A partir de los comentarios recibidos, se observa que la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias genera percepciones mixtas por parte de los agentes del sector. De una parte, existe coincidencia en que se trata de una medida de carácter principalmente informativo, cuyo aporte se orienta a facilitar la identificación del tipo de llamada por parte del usuario y a fortalecer su capacidad de tomar decisiones frente a la atención de comunicaciones, así como de reportar posibles usos indebidos. En este sentido, varios agentes destacan que la diferenciación de rangos podría contribuir a generar mayor claridad sobre el propósito de la llamada, apoyar los procesos de denuncia y ofrecer un marco más transparente para el control regulatorio del uso de la numeración.

No obstante, de manera transversal también se identifican desafíos relevantes asociados a su implementación y efectividad. En particular, se señala que la medida, al no abordar directamente aspectos como la autenticación del origen o la trazabilidad de la comunicación, tendría una capacidad limitada para prevenir el fraude, especialmente frente a esquemas sofisticados de suplantación o spoofing. Asimismo, varios agentes advierten sobre el riesgo de evasión, en la medida en que los actores fraudulentos podrían migrar hacia otros rangos de numeración o hacer uso indebido de los rangos asignados, sin que ello se traduzca necesariamente en una reducción efectiva del fenómeno.

Adicionalmente, se destacan implicaciones técnicas, operativas y económicas relevantes, tales como la necesidad de migraciones de numeración, adecuaciones en redes, sistemas de gestión, señalización y facturación, así como la definición de reglas de asignación, control y sanción. Estos elementos podrían implicar costos significativos para los distintos actores del ecosistema, así como retos de adopción y coordinación sectorial. De igual forma, se advierte que, desde la perspectiva del usuario, la efectividad de la medida dependería de procesos complementarios de pedagogía y comunicación, dado que la sola existencia de rangos diferenciados no garantiza su comprensión ni su uso efectivo en la toma de decisiones.

Con todo, los comentarios también permiten evidenciar que esta alternativa presenta beneficios potenciales en términos de empoderamiento del usuario y fortalecimiento de la confianza en el canal de voz, en la medida en que puede contribuir a ofrecer información más clara y accesible sobre la naturaleza de las comunicaciones recibidas. En efecto, la posibilidad de identificar de manera más inmediata el propósito comercial o publicitario de una llamada podría complementar otros mecanismos orientados a mejorar la transparencia del tráfico y a facilitar la interacción informada del usuario con los servicios.

En este contexto, y considerando tanto las ventajas como las limitaciones expuestas por los agentes, la CRC considera que la pertinencia de esta medida no debe determinarse de manera aislada, sino en el marco de una evaluación integral junto con las demás alternativas regulatorias identificadas. En consecuencia, la creación de rangos exclusivos de numeración será objeto de análisis bajo los criterios del Análisis de Impacto Normativo (AIN), con el fin de determinar su efectividad, eficiencia y proporcionalidad frente a otras medidas que persiguen objetivos similares, particularmente aquellas orientadas a suministrar mayor información al usuario y a fortalecer la confianza en el canal de voz. Este ejercicio permitirá establecer si la alternativa aporta un valor diferencial dentro del conjunto de medidas evaluadas o si sus beneficios resultan limitados frente a sus costos y riesgos de implementación.

- *¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la transparencia en las comunicaciones, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?*

ASOBANCARIA

Indica que podría mantenerse una alta exposición al fraude por vishing, además de generar un impacto operativo significativo. En su opinión, el etiquetado obligatorio de llamadas comerciales manteniendo la numeración actual podría tener impactos limitados en la mitigación del fraude, en particular frente a esquemas de vishing, dado que los actores maliciosos continuarían aprovechando la suplantación de numeración para engañar a los usuarios. Complementa en el sentido de indicar que la exposición al fraude podría mantenerse, al no resolverse de manera estructural los problemas de autenticación y trazabilidad del origen de las llamadas. Adiciona que esta medida podría generar un impacto operativo significativo para los actores del ecosistema, asociado a la adaptación de sistemas, procesos de marcación y gestión de excepciones, sin que ello se traduzca necesariamente en una reducción

proporcional del riesgo de fraude. Por esto, dice, el etiquetado de llamadas resulta más efectivo cuando se articula con otros controles, como mecanismos de validación del origen, autenticación de llamadas y filtrado del tráfico, en línea con el enfoque integral propuesto en el documento.

CLARO

Señala que el PCA o IT debería ser el responsable de identificar con el etiquetado cada uno de los mensajes enviados, pues es el que conoce el contenido de cada SMS.

PTC

Señala que prefijos en la numeración actual ayudarían a los operadores a identificar el origen, pero no a los usuarios. Agrega que el operador podría tomar acciones si cada prefijo corresponde a cada integrador y/o PCA y se evita tráfico mezclado. Concluye que lo más efectivo es que cada integrador y/o PCA tenga su numeración asignada.

SFC

Menciona que puede generar importantes beneficios en términos de seguridad, trazabilidad y confianza del usuario, dado que esta medida fortalecería la identificación del remitente, lo cual resulta fundamental para garantizar la confianza del usuario y mitigar riesgos asociados a la suplantación de marca y la intermediación no autorizada, al permitir un mayor control sobre el origen de los mensajes.

Asegura que uno de los beneficios más relevantes es la posibilidad de asignar un número único y verificable a cada remitente o campaña, lo que optimiza la identificación del emisor y reduce significativamente el riesgo de fraudes como el smishing, vishing y otros.

No obstante, esta transición implica desafíos importantes, entre ellos, la necesidad de adecuaciones tecnológicas por parte de operadores y proveedores, y para su implementación deberá contar con el acompañamiento técnico y campañas de pedagogía para los consumidores como para los actores del ecosistema.

SSC

Desde la perspectiva de **SSC**, la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual, presenta ventajas relevantes en términos de protección del usuario y transparencia, siempre que se diseñe bajo criterios técnicos claros, gobernanza adecuada y proporcionalidad.

Frente a las ventajas y posibles impactos positivos, menciona lo siguiente:

- Mayor transparencia para el usuario final. El etiquetado permite que el usuario identifique de manera inmediata la naturaleza de la llamada (por ejemplo, comercial, publicitaria o empresarial), sin necesidad de modificar la numeración ni de recurrir a bloqueos automáticos. Esto mejora la comprensión del contexto de la llamada y fortalece la confianza en las comunicaciones legítimas.
- Empoderamiento del usuario y prevención del fraude. Al brindar información clara y visible en el identificador de llamadas, el esquema facilita que el usuario tome decisiones

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

informadas sobre si atender o no una llamada, reduciendo la efectividad de esquemas de suplantación que se basan en generar ambigüedad o confianza indebida.
- Preservación de la numeración y continuidad del servicio. A diferencia de la creación de rangos exclusivos, el etiquetado permite mantener la numeración actual, evitando impactos operativos, costos de migración y afectaciones a la contactabilidad de servicios empresariales legítimos.
- Alineación con prácticas ya adoptadas por el ecosistema digital. El esquema es coherente con soluciones ampliamente utilizadas por los usuarios, como aplicaciones y funcionalidades de identificación de llamadas que ya incorporan etiquetas informativas y de verificación, lo que facilita su aceptación y comprensión.

En cuanto a los retos y desafíos a considerar, identifica lo siguiente:

- Definición y estandarización de las etiquetas. Resulta necesario establecer de forma clara y homogénea las categorías de etiquetado (por ejemplo, "llamada comercial", "empresa verificada", "no verificada"), así como los criterios objetivos para su asignación, evitando interpretaciones dispares entre operadores.
- Gobernanza y responsabilidad en la asignación de etiquetas. Debe definirse qué actor es responsable de asignar, validar, actualizar o retirar una etiqueta, así como los mecanismos de reclamación y corrección, para prevenir errores o afectaciones reputacionales a prestadores legítimos.
- Interoperabilidad técnica y experiencia de usuario. La efectividad del esquema depende de su correcta implementación en distintos dispositivos, sistemas operativos y redes, garantizando una experiencia de usuario consistente y comprensible.
- Riesgo de saturación informativa. Un uso excesivo o indiscriminado de etiquetas negativas podría generar desconfianza generalizada o fatiga en el usuario, por lo que el esquema debe equilibrar advertencias con etiquetas positivas y neutrales.

SSC considera que el etiquetado obligatorio, cuando se aplica de manera proporcional y estandarizada, contribuye de forma significativa a la protección del usuario y a la transparencia en las comunicaciones, al reducir la asimetría de información y permitir una gestión de confianza más efectiva, sin recurrir a medidas restrictivas que afecten de manera desproporcionada el tráfico legítimo.

TELEFÓNICA

Advierte que el etiquetado obligatorio (RCD - Rich Call Data) sobre la numeración actual es una alternativa superior a la segregación de rangos, pues permite a las empresas mantener sus números de contacto conocidos. Para este operador, la ventaja es que el usuario ve el nombre de la empresa o el motivo de la llamada en su pantalla, aumentando la confianza. Identifica como un reto la compatibilidad del parque de terminales ya que muchos teléfonos antiguos o de gama baja no tienen la capacidad nativa de mostrar esta información enriquecida sin una aplicación adicional. Añade que se requiere que la red soporte la transmisión de datos enriquecidos en la señalización, lo cual implica nuevamente la necesidad de redes IP.

TIGO

Señala que el etiquetado obligatorio de llamadas comerciales y publicitarias facilitaría la identificación inmediata del llamante por parte del usuario, obligaría al originador a declarar el propósito de la

comunicación y simplificaría los procesos de denuncia. No obstante, su implementación enfrenta retos técnicos y operativos, como la necesidad de mecanismos confiables para etiquetar señalización en redes IP y la limitada viabilidad en redes tradicionales, la falta de estandarización en la presentación de etiquetas, el riesgo de uso indebido o fraudulento de estas, la necesidad de procesos de registro y auditoría, y la posible saturación que reduzca su efectividad para el usuario. Además, indica que se requiere definir claramente su alcance y régimen sancionatorio. Finalmente, destaca que el etiquetado no sustituye mecanismos de autenticación como STIR/SHAKEN ni herramientas de filtrado o listas DNO, aunque puede actuar como medida complementaria.

ZANYA PINEDA

Menciona que esta medida puede constituir una herramienta relevante para fortalecer la transparencia en las comunicaciones de voz y la protección del usuario, siempre que su diseño responda a criterios de proporcionalidad, neutralidad tecnológica y respeto por los modelos legítimos de prestación del servicio. Este tipo de medida no actúa como un mecanismo de bloqueo ni de restricción del tráfico, sino como un instrumento informativo que traslada capacidad de decisión al usuario final, permitiéndole evaluar si desea o no atender la llamada.

Considera que, desde la perspectiva del usuario, el principal valor del etiquetado radica en la reducción de la asimetría de información. Al recibir una llamada claramente identificada como «Comercial», «Publicidad» o «Contacto empresarial», el usuario puede contextualizar la comunicación antes de contestar, sin que ello implique una presunción automática de fraude. Este enfoque resulta especialmente relevante en el servicio de voz, donde la simple visualización del número no ofrece información suficiente para distinguir entre una llamada legítima y una potencialmente abusiva o engañosa.

No obstante, asegura que el reto central de este esquema consiste en definir criterios uniformes, verificables e interoperables para la aplicación del etiquetado. La efectividad del modelo depende de que todos los actores del ecosistema (operadores móviles, proveedores de servicios de voz, integradores tecnológicos y originadores de llamadas) apliquen el etiquetado bajo estándares mínimos comunes, evitando interpretaciones discrecionales o prácticas inconsistentes que puedan generar confusión en el usuario o distorsiones en el mercado.

En este sentido, menciona que el etiquetado no debe quedar sujeto exclusivamente a la autodeclaración del originador ni a decisiones unilaterales del operador que termina la llamada, por lo que resulta necesario establecer mecanismos de validación progresiva, basados en relaciones contractuales, patrones de tráfico y reportes de usuarios, que permitan corregir usos indebidos del etiquetado sin recurrir a bloqueos generalizados ni sanciones automáticas. Este enfoque reduce el riesgo de falsos positivos y protege a actores legítimos que realizan comunicaciones comerciales lícitas, como entidades financieras, aseguradoras, empresas de servicios públicos o prestadores de salud.

Añade que, desde el punto de vista técnico, uno de los principales desafíos es garantizar que el etiquetado sea visible, comprensible y consistente en los distintos dispositivos y sistemas operativos, sin generar una experiencia de usuario alarmista o confusa.

Adicionalmente, considera necesario que el etiquetado obligatorio sea diseñado de forma que no se convierta en un mecanismo encubierto de estigmatización del tráfico comercial, ni en una barrera indirecta a la libre prestación de servicios de voz. En particular, debe evitarse que el etiquetado sea

utilizado como justificación para aplicar tratamientos degradados al tráfico, priorizaciones negativas o decisiones de bloqueo basadas únicamente en la categoría de la llamada, sin un análisis técnico individualizado.

Finalmente indica que, en términos regulatorios, esta medida puede aportar valor si se integra dentro de un ecosistema más amplio de gestión del riesgo, que incluya educación al usuario, canales eficaces de denuncia, plataformas de intercambio de alertas y responsabilidades distribuidas a lo largo de la cadena de la llamada. El etiquetado, por sí solo, no previene el fraude, pero sí mejora la capacidad del usuario para identificar patrones sospechosos y reportarlos, fortaleciendo los mecanismos de detección ex post.

RESPUESTA CRC:

A partir de los comentarios recibidos se identifican coincidencias y matices relevantes entre los agentes respecto a las ventajas, retos y posibles impactos asociados a la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para comunicaciones comerciales y publicitarias, manteniendo la numeración actual.

En términos generales, los comentarios evidencian una convergencia significativa en que el etiquetado de llamadas puede aportar beneficios en materia de transparencia y protección del usuario, en la medida en que permite proporcionar información adicional sobre la naturaleza de la llamada antes de que el usuario decida atenderla. En este sentido, se señala que el etiquetado puede fortalecer la identificación visible del originador o del propósito de la llamada, lo cual puede contribuir a mejorar la confianza en las comunicaciones legítimas y a facilitar procesos de denuncia o reporte cuando el usuario identifica comportamientos sospechosos.

Adicionalmente, algunos comentarios resaltan que una de las principales ventajas del etiquetado consiste en que permite mantener la numeración actual, evitando los costos y complejidades asociados a esquemas alternativos basados en la creación de rangos de numeración diferenciados o en procesos de migración masiva de números. No obstante, también se observa una coincidencia relevante en que el etiquetado obligatorio, por sí solo, tendría un alcance limitado frente a la mitigación del fraude, particularmente en escenarios asociados a suplantación de numeración o vishing. En efecto, varios comentarios advierten que, si no se acompaña de mecanismos robustos de autenticación del originador, validación de identidad y monitoreo del tráfico, el etiquetado podría no resolver de manera estructural los problemas de trazabilidad del origen de las llamadas. En este sentido, se plantea que su efectividad dependería de su articulación con otras medidas regulatorias o técnicas orientadas a fortalecer la integridad del identificador de llamadas y la gobernanza del tráfico de voz.

De igual manera, los comentarios recibidos coinciden en señalar diversos desafíos técnicos, operativos y de experiencia de usuario asociados a la implementación de este tipo de esquemas. Entre los principales retos identificados se destacan la necesidad de definir criterios claros y estandarizados para la asignación de etiquetas, la definición de mecanismos de gobernanza sobre quién es responsable de su asignación, validación y actualización, así como la necesidad de establecer procedimientos que permitan corregir errores o usos indebidos del etiquetado. Por otra parte, también se identifican consideraciones relacionadas con el diseño regulatorio del esquema, particularmente en lo relativo a evitar que el etiquetado genere efectos indeseados sobre el funcionamiento del mercado o sobre el tráfico legítimo. En este sentido, algunos aportes señalan que se debe evitar que se convierta en un

mecanismo indirecto de bloqueo o degradación del tráfico comercial legítimo, o que genere saturación informativa que reduzca su utilidad para el usuario.

En consideración con lo anterior, esta Comisión identifica que los comentarios de la consulta pública aportan insumos para la estructuración de las alternativas regulatorias, particularmente, en lo relacionado con la definición de esquemas de etiquetado que contemplen criterios claros de estandarización, mecanismos de gobernanza sobre la asignación de etiquetas, salvaguardas para evitar afectaciones al tráfico legítimo y su articulación con otros mecanismos de autenticación y control del tráfico. Así mismo, se resalta que los comentarios constituyen insumos técnicos para la evaluación de las alternativas regulatorias, en la medida en que permiten identificar aspectos críticos relacionados con la viabilidad técnica del esquema, los posibles impactos operativos para los actores del ecosistema, las dependencias tecnológicas asociadas a la arquitectura de las redes y los efectos potenciales sobre la experiencia del usuario.

- *¿Qué beneficios y riesgos identifica en la creación de un registro nacional único de números DNO? ¿Qué criterios deberían regir su actualización y acceso?*

ASOBANCARIA

Considera necesario contar con un control transversal de las listas DNO entre los distintos PRST, garantizando bloqueos oportunos y coordinados. Indica que el principal desafío radica en asegurar su aplicación efectiva y uniforme en todos los PRST.

CLARO

Señala que actualmente ingresa tráfico con millones de números origen diferentes diarios con un perfil de posible fraude, no considera que un control centralizado sea eficiente, dado que cada operador de LDI, podría tomar sus acciones locamente.

SSC

Desde la perspectiva de **SSC**, la creación de un registro nacional único de números de no originación (DNO) puede aportar beneficios relevantes para la mitigación del fraude en llamadas de voz, pero también conlleva riesgos técnicos y operativos que deben ser cuidadosamente gestionados mediante criterios claros de actualización, acceso y gobernanza.

Frente a los beneficios potenciales, menciona lo siguiente:

• Reducción de usos indebidos de numeración. Un registro nacional de DNO puede contribuir a evitar el uso fraudulento de numeración que no debería originar llamadas bajo ningún escenario legítimo, como rangos no asignados, numeración reservada o números identificados de manera consistente en eventos de fraude confirmado.
• Homogeneidad en la aplicación de controles básicos. La existencia de un registro único permitiría aplicar un criterio común y estandarizado entre los PRST, reduciendo asimetrías regulatorias y técnicas en la gestión de numeración claramente irregular.

• Apoyo a la trazabilidad y a la coordinación interoperatorial. El DNO puede servir como referencia compartida, facilitando la cooperación entre operadores y la respuesta coordinada frente a eventos de fraude reincidentes.

Frente a los riesgos y desafíos, plantea lo siguiente:

• Riesgo de falsos positivos con impacto sistémico. Al tratarse de un registro único y centralizado, errores en la inclusión de un número pueden generar bloqueos generalizados y afectar de manera desproporcionada tráfico legítimo, con impactos inmediatos en la prestación del servicio.
• Rigidez operativa y tiempos de reacción. Si los procesos de actualización no son ágiles, el registro puede volverse obsoleto o inefectivo, o impedir una reacción oportuna frente a nuevos esquemas de fraude.
• Incentivo a la evasión. Actores fraudulentos pueden adaptarse rápidamente, migrando a numeración distinta o a esquemas de suplantación más complejos, limitando la efectividad del DNO como única medida.
• Concentración de responsabilidades y riesgos. La centralización del registro implica mayores exigencias en materia de seguridad de la información, gobernanza y responsabilidad ante errores o usos indebidos.

En relación con los criterios para la actualización del registro, considera indispensable que la actualización del registro DNO se rija por criterios estrictos y objetivos, tales como:

• Inclusión limitada a numeración que objetivamente no debe originar llamadas, evitando incorporar números utilizados en servicios legítimos.
• Sustento técnico verificable para la inclusión de un número, basado en evidencia clara de uso indebido o fraude confirmado.
• Mecanismos de revisión periódica y expiración automática, que eviten inclusiones permanentes sin reevaluación.
• Procedimientos de corrección y exclusión ágiles, cuando se identifiquen errores o cambios en la condición del número.

En cuanto al acceso al registro, SSC considera que deben establecerse las siguientes salvaguardas:

• Acceso restringido a PRST y actores autorizados, exclusivamente para fines de prevención y mitigación del fraude.
• Registro y auditoría de consultas y actualizaciones, garantizando trazabilidad y responsabilidad.
• Prohibición expresa de usos comerciales o competitivos de la información.
• Cumplimiento de los principios de protección de datos, incluyendo minimización, seguridad y retención limitada.

SSC considera que un registro nacional único de DNO puede ser una herramienta útil como medida complementaria, siempre que su alcance sea estrictamente acotado, su actualización sea ágil y verificable, y su uso se enmarque en principios de proporcionalidad y protección del tráfico legítimo. En ningún caso debería entenderse como una solución única o sustitutiva de otros mecanismos como el monitoreo de comportamiento, la trazabilidad técnica y la cooperación inter operatoria.

TELEFÓNICA

Señala como beneficio la protección de números institucionales que solo deben recibir llamadas (como las líneas 018000 o PBX de atención al cliente), impidiendo que sean suplantados para realizar llamadas salientes fraudulentas. A su juicio, una lista DNO efectiva bloquearía de raíz el vishing que simula ser el banco llamando al cliente. Identifica como un riesgo la gestión de la lista, ya que, si un número legítimo es incluido por error, la empresa queda incomunicada hacia afuera. Sugiere que los criterios de actualización deben ser estrictos, permitiendo solo al asignatario del recurso solicitar la inclusión o exclusión, con validación de identidad fuerte. Finalmente, opina que el acceso de consulta debe ser en tiempo real para los operadores que cursan el tráfico, para poder bloquear las llamadas no autorizadas inmediatamente.

TIGO

Considera que la creación de un registro nacional único de números DNO presenta baja efectividad para la prevención del fraude, ya que restringe progresivamente el uso de la numeración, recurso escaso, y puede incentivar una mayor rotación de números utilizados por los defraudadores. Entre los principales riesgos se identifican la ineficiencia en el uso de los recursos de numeración y la aceleración de la sustitución de números asociados a actividades fraudulentas, lo que limita el impacto real de la medida.

ZANYA PINEDA

Menciona que la creación de un registro nacional único de números de no originación (DNO) puede aportar, en principio, coherencia, estandarización y coordinación institucional en la gestión del fraude en llamadas de voz. Un esquema centralizado permitiría consolidar información sobre numeración reportada como fraudulenta y establecer un marco común de referencia para todos los operadores y actores del ecosistema. Sin embargo, su efectividad real no depende de la existencia formal del registro, sino de cómo se alimenta, cómo se gobierna y, especialmente, cómo se aplica en la práctica por quienes controlan la terminación de las llamadas.

Añade que, desde una perspectiva técnica y operativa, el principal riesgo del DNO nacional es que repita las limitaciones estructurales ya observadas en el Registro Nacional de Números Excluidos (RNE). En ambos casos, el éxito del sistema descansa en la actuación diligente de los operadores móviles, quienes son los únicos que tienen la capacidad efectiva de impedir que una llamada se origine o se complete. Si los operadores no integran el DNO de manera obligatoria, automática y verificable en sus sistemas de enrutamiento y control de tráfico, el registro se convierte en una herramienta meramente declarativa, sin impacto real en la experiencia del usuario.

Indica adicionalmente que un DNO nacional plantea retos significativos en términos de actualización, trazabilidad y temporalidad de los reportes. En el servicio de voz, los esquemas de fraude se caracterizan por la alta rotación de numeración, el uso intensivo de SIM cards y la rápida mutación de los patrones de originación. En este contexto, un número puede ser utilizado de forma fraudulenta durante un período muy corto y, posteriormente, quedar inactivo o ser reasignado. Por ello, un DNO rígido, sin criterios claros de caducidad, revisión y depuración, puede generar bloqueos injustificados de tráfico legítimo, afectando derechos de usuarios finales y de terceros de buena fe.

En cuanto a los criterios de inclusión en el DNO, indica que es fundamental que estos se basen en reportes verificables y graduales, y no únicamente en denuncias aisladas o automatizadas, teniendo en cuenta que en el servicio de voz no es posible determinar ex ante el contenido de la llamada ni

calificarla como fraudulenta sin la intervención del usuario. Por lo tanto, añade que el DNO debe construirse a partir de evidencia posterior a la terminación de la llamada, validada mediante patrones repetitivos, análisis técnico del tráfico y corroboración interoperatoria. De lo contrario, se corre el riesgo de convertir el DNO en un mecanismo de censura preventiva del tráfico.

Asegura que otro aspecto crítico es la administración del registro, teniendo en cuenta que un DNO nacional requiere reglas claras sobre quién puede reportar, quién valida, quién decide la inclusión y exclusión de números, y bajo qué condiciones se pueden levantar las restricciones. En ausencia de procedimientos transparentes y garantistas, el registro puede convertirse en una herramienta discrecional que afecte la competencia, excluya actores legítimos del mercado o concentre aún más el control del tráfico en cabeza de unos pocos operadores dominantes.
Por otro lado, menciona que desde el punto de vista regulatorio el DNO no debe concebirse como una solución autónoma ni excluyente, sino como un componente más dentro de un esquema de mitigación del fraude basado en responsabilidades distribuidas a lo largo de toda la cadena. El enfoque de «lista negra» resulta insuficiente si no se acompaña de medidas estructurales en la asignación, comercialización e identificación de la numeración, especialmente en la fase inicial de entrega de SIM cards y recursos de numeración a usuarios y empresas.

Concluye advirtiendo que debe evitarse que el DNO nacional se utilice como un mecanismo para trasladar la carga del fraude hacia los actores intermedios o internacionales, ignorando que el problema se origina, en gran medida, en el descontrol histórico de la numeración móvil dentro del país. Un enfoque que solo actúa al final del flujo de la llamada (cuando está ya ha transitado por múltiples redes) resulta reactivo y limitado frente a la magnitud del fenómeno.

RESPUESTA CRC:

A partir de los comentarios recibidos, se observa que algunos agentes coinciden en que la creación de un registro nacional único de números de no originación (DNO) podría aportar beneficios para la mitigación del fraude en llamadas de voz, particularmente al permitir la identificación de numeración que no debería originar llamadas y la aplicación homogénea de controles entre los PRST. En este sentido, **ASOBANCARIA** destaca la necesidad de contar con un control transversal de las listas DNO entre los operadores, mientras que **SSC** y **ZANYA PINEDA** señalan que un registro centralizado podría contribuir a mejorar la coordinación intraoperatoria, la estandarización de criterios y la trazabilidad de numeración utilizada en esquemas de fraude. De manera complementaria, **TELEFÓNICA** identifica como beneficio la posibilidad de proteger numeración institucional que solo debería recibir llamadas, evitando su suplantación en esquemas de fraude como el vishing.

No obstante, se presentan divergencias respecto a la efectividad y conveniencia de un registro centralizado. Por un lado, **CLARO** considera que un esquema de control centralizado podría resultar ineficiente frente al volumen masivo de tráfico con numeraciones potencialmente fraudulentas, señalando que los operadores de larga distancia internacional podrían gestionar estas situaciones de manera local. En la misma línea, **TIGO** advierte que un registro DNO podría tener baja efectividad para la prevención del fraude, al incentivar la rotación constante de numeración utilizada por los defraudadores y generar restricciones adicionales sobre el uso de los recursos de numeración. Asimismo, **SSC** y **ZANYA PINEDA** advierten sobre riesgos asociados a la centralización del registro, como la posibilidad de falsos positivos con impactos sistémicos, rigidez en los procesos de actualización o problemas de gobernanza en la administración del sistema.

En cuanto a las propuestas regulatorias, los agentes plantean que, en caso de implementarse un registro DNO nacional, este debería contar con criterios estrictos de inclusión, actualización y administración, sustentados en evidencia técnica verificable de uso indebido o fraude confirmado, así como en mecanismos de revisión periódica, expiración automática y corrección de errores, como lo sugieren **SSC** y **TELEFÓNICA**. Asimismo, **SSC** y **ZANYA PINEDA** plantean la necesidad de establecer reglas claras de acceso, gobernanza y auditoría del registro, garantizando que su uso se limite a fines de prevención del fraude y evitando usos indebidos de la información. Finalmente, algunos agentes destacan que el registro DNO debería entenderse como una herramienta complementaria dentro de un esquema más amplio de mitigación del fraude, que incluya mecanismos de monitoreo del tráfico, trazabilidad técnica y cooperación inter operatoria.

En consideración con lo anterior, la CRC identifica que los comentarios recibidos en la consulta pública aportan insumos relevantes para la estructuración de las alternativas regulatorias, particularmente en lo relacionado con los beneficios y riesgos asociados a la creación de un registro nacional único de números DNO, así como con los criterios que podrían regir su actualización y acceso.

En ese sentido, la Comisión considera pertinente mantener dentro del análisis regulatorio la temática relacionada con la falta de estandarización en la aplicación de las listas de no originación, con el fin de evaluar las posibles alternativas regulatorias y contrastarlas con el escenario actual, en el marco del correspondiente Análisis de Impacto Normativo (AIN).

- *¿Qué ventajas, retos y posibles impactos identifica en la adopción de un esquema en el que cada PRST mantenga su propia lista de no originación (DNO), bajo un estándar mínimo obligatorio definido por la CRC? ¿De qué manera considera que esta medida podría contribuir a la protección contra el fraude y la suplantación en llamadas de voz, y qué desafíos técnicos, operativos o de coordinación deberían ser tenidos en cuenta para asegurar su efectividad y coherencia en Colombia?*

CLARO

Reconoce como principales ventajas la reducción significativa de fraudes y suplantaciones, ya que cada proveedor puede ajustar su lista según su tráfico y contexto, bloqueando números inbound-only o no asignados que suelen ser utilizados para suplantación. Asimismo, se genera una mayor flexibilidad operacional, al permitir la personalización de los controles con base en los perfiles de tráfico y los requisitos locales de cada operador, sin depender de un único registro central.

No obstante, reitera que los operadores de LDI, como responsables del tráfico, deberían contar localmente con sus propios mecanismos de control y gestión.

SSC

Desde la perspectiva de **SSC**, la adopción de un esquema en el que cada PRST administre su propia lista de no originación (DNO), bajo un estándar mínimo obligatorio definido por la CRC, presenta ventajas relevantes frente a un registro único centralizado, al tiempo que plantea retos técnicos, operativos y de coordinación que deben ser gestionados mediante lineamientos regulatorios claros.

Entre las principales ventajas, se destaca que la administración descentralizada de las listas DNO permite a cada PRST actuar de manera ágil y focalizada frente a eventos de fraude detectados en su propia red, reduciendo los tiempos de reacción y evitando la propagación automática de bloqueos a todo el ecosistema. Asimismo, este enfoque reduce el riesgo sistémico de falsos positivos, al limitar el impacto de eventuales errores de inclusión a la red del PRST que adopta la medida. Adicionalmente, facilita una mejor alineación con la realidad operativa de cada red, permitiendo integrar la DNO con otros mecanismos como el monitoreo de comportamiento, la trazabilidad técnica y la cooperación interoperatorial.

No obstante, la existencia de múltiples listas DNO también introduce retos relevantes. En particular, resulta necesario asegurar un nivel mínimo de coherencia interoperatorial, de manera que no se presenten tratamientos divergentes injustificados sobre la misma numeración. Asimismo, se requiere una adecuada gestión operativa y de gobernanza, que contemple procesos claros de inclusión, revisión, corrección y atención de reclamaciones, así como recursos técnicos suficientes para la administración continua de las listas.

Adicionalmente, SSC considera necesario advertir que este esquema puede verse afectado por asimetrías de mercado, especialmente en el caso de PRST con alta participación de mercado o posición dominante. En ausencia de salvaguardas regulatorias adecuadas, existe el riesgo de que las listas DNO sean utilizadas de forma excesiva o desproporcionada, generando bloqueos amplios que afecten tráfico legítimo o introduzcan distorsiones competitivas.

Por ello, resulta indispensable que el estándar mínimo definido por la CRC establezca criterios objetivos y restrictivos de inclusión, prohíba expresamente inclusiones masivas sin sustento técnico, y contemple obligaciones de trazabilidad, justificación y auditoría, así como mecanismos ágiles de revisión y corrección, con una supervisión regulatoria reforzada cuando se trate de PRST con alta participación de mercado.

En términos de contribución a la protección contra el fraude y la suplantación, SSC considera que las listas DNO por PRST pueden ser efectivas en la medida en que se utilicen de forma acotada y objetiva, enfocadas exclusivamente en numeración que no debe originar llamadas bajo ningún escenario legítimo, y se integren dentro de un enfoque de mitigación multicapa, complementario a otros mecanismos técnicos y operativos.

Para asegurar la efectividad y coherencia del esquema a nivel nacional, SSC considera necesario que la CRC defina, como mínimo: (i) un estándar obligatorio de criterios de inclusión y exclusión, evidencia técnica mínima y plazos de revisión; (ii) lineamientos de intercambio de alertas entre PRST sin imposición de replicación automática de listas; (iii) principios de proporcionalidad, reversibilidad y protección del tráfico legítimo; y (iv) reglas claras de protección de datos y auditoría.

SSC considera que un esquema de listas de no originación administradas por cada PRST, bajo un estándar mínimo definido por la CRC y acompañado de salvaguardas frente a asimetrías de mercado, constituye una alternativa más flexible, proporcional y operativamente viable que un registro nacional único, siempre que se diseñe con mecanismos efectivos de coordinación, control y supervisión.

TELEFÓNICA

Comenta que un esquema donde cada PRST gestiona su propia lista DNO bajo estándares mínimos ofrece la ventaja de la agilidad y la autonomía en la gestión de riesgos de su propia red. Añade que esto permite a cada operador proteger a sus clientes corporativos de manera directa sin depender de una base centralizada externa. Identifica la coherencia como un desafío, ya que, para que la protección sea sistémica, las listas deben estar sincronizadas o ser compartidas. Advierte que, aunque la lista sea local, debe existir un mecanismo de intercambio o consulta para que el bloqueo de no-originación sea respetado por todas las redes interconectadas.

TIGO

Considera que un esquema en el que cada PRST administre su propia lista de no originación (DNO) permitiría respuestas más ágiles y adaptadas a las particularidades de cada red, perfil de tráfico y base de clientes. Sin embargo, señala que su implementación enfrenta retos importantes, como la definición de un estándar mínimo que reduzca diferencias en criterios de inclusión y niveles de protección, la complejidad técnica para integrar consultas en tiempo real con sistemas de enrutamiento y rastreo, la necesidad de coordinación e interoperabilidad entre redes para evitar bloqueos inconsistentes y el riesgo de afectar llamadas legítimas.

ZANYA PINEDA

Indica que esta alternativa puede ofrecer mayor flexibilidad operativa y capacidad de reacción inmediata frente a eventos de fraude en llamadas de voz. Este modelo reconoce que los PRST son quienes cuentan con el control técnico directo sobre la oxigenación, el enrutamiento y la terminación de las llamadas, y por tanto están en mejor posición para implementar medidas dinámicas y ajustadas a los patrones reales de tráfico que observan en sus redes.

Menciona que, desde una perspectiva técnica, una DNO administrada por cada PRST permitiría respuestas más rápidas y contextualizadas, evitando los retrasos propios de esquemas centralizados que requieren validaciones múltiples antes de actuar. En un entorno de fraude de voz caracterizado por alta rotación de numeración, cambios constantes en rutas y uso intensivo de SIM cards, la capacidad de un operador para bloquear de manera ágil un número claramente abusivo puede reducir impactos inmediatos sobre los usuarios finales. Esta agilidad operativa constituye una de las principales ventajas del modelo descentralizado.

Sin embargo, añade que este esquema también plantea riesgos significativos de fragmentación, discrecionalidad y asimetría regulatoria si no se encuentra estrictamente delimitado por reglas claras y mecanismos efectivos de supervisión. En ausencia de un estándar mínimo robusto y de lineamientos homogéneos, cada PRST podría aplicar criterios distintos para incluir o excluir numeración en sus listas DNO, lo que derivaría en tratamientos dispares del mismo número dependiendo del operador que curse o termine la llamada, lo que puede generar inseguridad jurídica, afectar el tráfico legítimo y distorsionar la competencia en el mercado de voz.

Asegura que uno de los principales desafíos del modelo es evitar que las listas DNO por PRST se conviertan en herramientas de bloqueo preventivo excesivo, basadas en criterios internos poco transparentes o en presunciones no verificadas de fraude. Dado que en el servicio de voz no es posible calificar una llamada como fraudulenta antes de su terminación, la inclusión de un número en una DNO debería responder a patrones reiterados, reportes corroborados de usuarios y análisis técnico posterior, y no a eventos aislados o automatizados que puedan generar falsos positivos.

Añade que, desde el punto de vista regulatorio, la Comisión debería definir un estándar mínimo obligatorio que incluya, al menos: criterios objetivos de inclusión y exclusión de números, reglas de temporalidad y revisión periódica de las listas, mecanismos de trazabilidad de las decisiones adoptadas por cada PRST, y procedimientos claros para la atención de reclamaciones o solicitudes de levantamiento de bloqueos por parte de usuarios o terceros afectados. Sin estos elementos, el esquema descentralizado corre el riesgo de erosionar la confianza del ecosistema y de los usuarios finales.
Adicionalmente, asegura que la efectividad de las DNO por PRST depende de su articulación con un esquema nacional de reporte del usuario, que funcione como insumo común para todos los operadores. El usuario final es quien identifica en primera instancia la posible conducta fraudulenta, y su reporte debe constituir el punto de partida del análisis, sin que ello implique una inclusión automática del número en listas de no originación. La falta de un canal unificado de reporte puede llevar a duplicidades, inconsistencias y pérdida de información relevante para la detección de patrones más amplios de fraude.

Añade que otro riesgo relevante es que este modelo refuerce la concentración de poder de mercado en cabeza de los grandes operadores móviles, quienes cuentan con mayores capacidades técnicas y económicas para implementar sistemas avanzados de monitoreo y filtrado. Si no se establecen obligaciones de interoperabilidad y coordinación, los PRST dominantes podrían imponer de facto sus criterios al resto del ecosistema, afectando especialmente a actores más pequeños, integradores tecnológicos y proveedores legítimos de servicios de voz.

Finalmente indica que, en términos de protección al usuario, las listas DNO por PRST solo resultarán eficaces si se aplican bajo un enfoque proporcional y transparente, evitando bloqueos silenciosos o decisiones opacas que el usuario no pueda comprender ni cuestionar, por lo que la CRC debería exigir mecanismos mínimos de rendición de cuentas, como reportes periódicos sobre la gestión de las DNO, estadísticas de números bloqueados, tiempos de permanencia y resultados en términos de reducción efectiva del fraude.

RESPUESTA CRC:

Desde la perspectiva de **CLARO**, la principal ventaja de que cada PRST administre su propia lista de no originación (DNO) radica en la reducción significativa del fraude y la suplantación mediante el bloqueo focalizado de numeración inbound-only o no asignada, así como en la flexibilidad operativa para adaptar los controles al perfil de tráfico de cada red. Esta posición se alinea de manera directa con la intención de la CRC de diseñar alternativas regulatorias proporcionales y técnicamente viables, que reconozcan la heterogeneidad operativa de los PRST y eviten los cuellos de botella propios de esquemas centralizados.

El argumento refuerza la alternativa planteada por la Comisión, en la medida en que demuestra que la descentralización puede incrementar la efectividad antifraude sin introducir rigideces regulatorias. No obstante, al enfatizar que los operadores de LDI deben contar con mecanismos locales de control, el comentario también sugiere la necesidad de precisar responsabilidades en la cadena internacional, lo que implica que la alternativa debe mantenerse, pero complementarse con reglas claras de atribución de responsabilidad.

Desde **SSC** se plantea una visión más estructural, destacando que la administración descentralizada de las DNO permite respuestas ágiles y focalizadas, reduce el riesgo sistémico de falsos positivos y facilita la integración con otros mecanismos de mitigación como el monitoreo de comportamiento y la trazabilidad técnica. Este enfoque coincide plenamente con la intención de la CRC de promover esquemas multicapa de mitigación del fraude, evitando soluciones únicas y rígidas. Sin embargo, **SSC** introduce un análisis crítico relevante al advertir que la multiplicidad de listas puede generar incoherencias interoperatoriales, asimetrías de mercado y riesgos de uso excesivo por parte de PRST con alta participación.

Este argumento no desvirtúa la alternativa, pero sí evidencia que su efectividad depende críticamente del diseño del estándar mínimo. En consecuencia, la posición de SSC conduce a mantener la alternativa, pero modificarla incorporando salvaguardas explícitas de proporcionalidad, auditoría, trazabilidad y supervisión reforzada, especialmente frente a operadores dominantes.

TELEFÓNICA aporta una visión centrada en la autonomía y la agilidad, señalando que la gestión local de DNO permite a cada PRST proteger directamente a sus clientes corporativos sin depender de una base centralizada. Este argumento es coherente con la intención de la CRC de fortalecer la capacidad preventiva de los operadores y reducir los tiempos de reacción frente al fraude. No obstante, **TELEFÓNICA** identifica como desafío crítico la necesidad de coherencia sistémica, advirtiendo que, para que la protección sea efectiva, debe existir algún mecanismo de intercambio o consulta entre redes.

Este comentario confirma que la alternativa no puede concebirse como un conjunto de listas aisladas, sino como un esquema descentralizado coordinado. En consecuencia, el impacto del argumento deriva en un ajuste a la alternativa para incorporar mecanismos mínimos de interoperabilidad que aseguren consistencia sin imponer replicación automática.

TIGO coincide en resaltar la agilidad y la adaptación al perfil de cada red como ventajas del esquema, lo cual refuerza la intención de la CRC de privilegiar soluciones operativamente realistas. Sin embargo, introduce consideraciones técnicas relevantes al señalar la complejidad de integrar consultas en tiempo real con sistemas de enrutamiento y rastreo, así como el riesgo de afectar llamadas legítimas si los criterios no son homogéneos. Este argumento pone de presente que la alternativa, aunque conceptualmente es adecuada, requiere un estándar mínimo suficientemente preciso para evitar disparidades técnicas y operativas. Por tanto, el impacto del comentario es reafirmar que la alternativa debe mantenerse, pero con un nivel de especificidad técnica mayor en su diseño normativo a la hora de la evaluación.

La posición de **ZANYA PINEDA** ofrece un análisis particularmente alineado con la lógica de la CRC al reconocer que los PRST, por su control directo del enrutamiento y la terminación, están en mejor posición para implementar medidas dinámicas frente a un fraude de voz altamente cambiante. Este argumento refuerza la racionalidad de la alternativa descentralizada y su coherencia con el principio de eficacia regulatoria. Sin embargo, también introduce una advertencia crítica al señalar los riesgos de fragmentación, discrecionalidad, inseguridad jurídica y distorsión competitiva si no existen reglas homogéneas.

Desde la intención de la CRC, este análisis subraya que la alternativa no puede operar sobre la base de presunciones automáticas de fraude, ni convertirse en un mecanismo de bloqueo preventivo

excesivo. En este sentido la alternativa debe mantenerse, pero condicionarse estrictamente a criterios objetivos.

En conjunto, los argumentos de **CLARO**, **SSC**, **TELEFÓNICA**, **TIGO** y **ZANYA PINEDA** convergen en que el esquema de DNO por PRST es coherente con la intención de la CRC de diseñar una medida antifraude flexible, proporcional y operativamente viable, especialmente frente a la dinámica del fraude en llamadas de voz. Al mismo tiempo, los comentarios evidencian que, sin un estándar mínimo robusto, la alternativa podría generar efectos contrarios a los buscados, como bloqueos injustificados, asimetrías de mercado o pérdida de confianza. En consecuencia, la alternativa definitiva será ajustada reforzando su diseño normativo para asegurar coherencia, transparencia, protección del tráfico legítimo y supervisión efectiva.

8.2.6 Sobre las temáticas enfocadas en la educación de la ciudadanía

8.2.6.1 Subtemática 1: Acciones educativas

ANDESCO

Propone que la CRC lidere campañas pedagógicas y coordine estrategias con otras entidades públicas bajo el principio de colaboración interinstitucional, para elevar la capacidad ciudadana de identificar fraudes por mensajes o llamadas y promover canales efectivos de denuncia. Además, al referirse a instrumentos como el portal y el sistema de trazabilidad de PQR asociados a esta sección, **ANDESCO** llama la atención sobre la necesidad de que la CRC valore sus capacidades operativas para administrar información con estándares robustos de seguridad de la información y tratamiento de datos personales, procurando que estas iniciativas no se traduzcan en nuevas obligaciones técnicas u operativas adicionales para los PRST, o en esquemas que concentren en ellos cargas que deberían distribuirse entre actores del ecosistema.

ANDI

En relación con las necesidades de educación y fortalecimiento de capacidades ciudadanas, la **ANDI** llama la atención de la ausencia de una propuesta que ponga en cabeza de la CRC una obligación de realizar campañas educativas a los ciudadanos para prevenir el fraude a través de mensajes o llamadas. A juicio de la **ANDI**, debe ser la CRC quien, en coordinación con diferentes entidades del Estado, imparta medidas educativas, haciendo consciente al ciudadano del riesgo que se genera por la mala asignación, y de las medidas que tiene para denunciar el mal uso por parte de dichos asignatarios.

ASOBANCARIA

Considera necesario fortalecer campañas conjuntas entre la CRC y el sector financiero orientadas a la prevención del fraude por ingeniería social, integradas en aplicaciones bancarias, SMS y otros canales digitales, con mensajes claros y consistentes que refuercen la creación y gestión de contraseñas seguras, la identificación de intentos de suplantación y el uso responsable de llamadas, enlaces y solicitudes de información. En opinión de **ASOBANCARIA**, estas iniciativas educativas deben concebirse como un complemento directo de los controles técnicos y de monitoreo previstos para los servicios de SMS y voz, de manera que refuercen su efectividad y contribuyan a una reducción integral

del riesgo de fraude. Asimismo, destaca la necesidad de implementar acciones de educación masiva y sostenida, incluyendo medios tradicionales como televisión y radio, así como medios digitales, desarrolladas de manera coordinada, intersectorial y continua, conforme a los lineamientos regulatorios.

ASOMÓVIL

Comparte la importancia de fortalecer la educación al usuario mediante acciones de prevención, alfabetización digital y mejora de los mecanismos de reporte. No obstante, advierte que estas campañas solo serán efectivas si se diseñan e implementan con una coordinación interinstitucional amplia, que articule esfuerzos públicos y privados, incluidas autoridades, entidades financieras y canales de denuncia. Añade que este componente pedagógico debe complementarse con consecuencias efectivas para los actores que facilitan o habilitan el fraude.

CCE

Menciona que le llama la atención la ausencia de una propuesta que ponga en cabeza de la CRC una obligación de realizar campañas educativas a los ciudadanos para prevenir el fraude a través de mensajes o llamadas, y considera que la CRC es el ente, coordinado con diferentes entidades del estado, que debe impartir medidas educativas, haciendo consciente al ciudadano del riesgo que se genera por la mala asignación, y de las medidas que tiene para denunciar el mal uso por parte de dichos asignatarios.

CCIT

En materia de educación al usuario, la **CCIT** considera que el documento de alternativas omite una línea de acción que debería recaer en la CRC: campañas educativas a los ciudadanos para prevenir el fraude por mensajes o llamadas. Propone que estas campañas se adelanten de forma coordinada con otras entidades del Estado y que estén orientadas a (i) sensibilizar sobre los riesgos asociados al uso indebido de recursos de identificación y (ii) visibilizar los mecanismos disponibles para denunciar el mal uso por parte de asignatarios. En su enfoque, la prevención no debe descansar exclusivamente en controles tecnológicos, sino también en reducir asimetrías de información del usuario frente a prácticas fraudulentas recurrentes.

CLARO

Manifiesta que ha adelantado campañas educativas dirigidas a sus usuarios, pero sin que se evidencie una efectividad clara en la reducción del fraude. En este sentido, considera innecesario imponer nuevas obligaciones pedagógicas a los PRST, PCA e IT, sin que se adelante un análisis de impacto normativo (AIN).

El operador solicita que la CRC asuma directamente el liderazgo de campañas educativas masivas, coordinadas con otras entidades del Estado, utilizando medios de amplia difusión y evitando trasladar cargas administrativas adicionales a los agentes regulados.

HABLAME

Respalda la educación ciudadana como componente de mitigación, pero condiciona su efectividad y legitimidad a que los mensajes educativos sean gratuitos no solo para el usuario final, sino también para integradores, PCA y operadores, sin cargos de acceso entre agentes. Desde su perspectiva, al tratarse de comunicaciones de interés público vinculadas con seguridad, deberían clasificarse regulatoriamente como tráfico de interés general sin costo para evitar desincentivos a su despliegue masivo.

Adicionalmente, manifiesta que el COLCERT como autoridad central de decisión antifraude debería mantener un portal público con tipologías, casos activos, URLs y patrones detectados, y desarrollar campañas permanentes para que el ciudadano sepa que puede consultar y reportar allí mensajes sospechosos, reduciendo la intermediación de operadores y el riesgo de decisiones subjetivas. Con ello, **HABLAME** sugiere integrar educación, reporte y respuesta técnica en un mismo circuito institucional, con un objetivo explícito de elevar confianza y disminuir la exposición de usuarios a campañas fraudulentas sin degradar el tráfico legítimo.

PTC

Destaca que ya cuenta con una estrategia de concientización dirigida a clientes, en desarrollo de la cual envía recomendaciones de seguridad por mensajes de texto y, cuando identifica amenazas potenciales, emite comunicados oportunos para alertar y proteger usuarios. Asimismo, menciona un programa de "Alerta en línea" orientado a brindar recomendaciones de seguridad de la información a menores en colegios del país.

SFC

Considera fundamental que las campañas se desarrollen bajo un esquema de comunicación unificada entre las autoridades y los actores del sector. Menciona que más allá de formular recomendaciones generales sobre los riesgos asociados a los servicios móviles, estas iniciativas deben visibilizar prácticas fraudulentas que afectan directamente el patrimonio del ciudadano. En ese sentido, propone articular los contenidos de la CRC con los programas de educación financiera de la **SFC** y de los gremios bancarios, reforzando mensajes claros y consistentes, como que ninguna entidad financiera solicita claves ni información sensible a través de llamadas o mensajes de texto.

Propone articular las medidas de educación ciudadana con los programas de educación financiera ya existentes, así como avanzar en la creación de un portal centralizado y dinámico que consolide información sobre campañas fraudulentas detectadas. Adicionalmente, se destaca la necesidad de caracterizar previamente a la población objetivo, con el fin de diseñar estrategias de comunicación más efectivas.

TELEFÓNICA

Reafirma su compromiso con campañas de sensibilización al usuario, pero considera que la creación de sistemas centralizados de trazabilidad de PQR o portales de denuncia administrados por la CRC debe evaluarse con prudencia. Lo anterior, ya que, dice, centralizar el detalle de las reclamaciones de fraude conlleva riesgos de seguridad de la información y duplicidad de funciones con los canales de atención de los operadores y las entidades financieras.

En complemento de lo anterior, **TELEFÓNICA** dice que la lucha contra el fraude trasciende la esfera regulatoria técnica, por lo que el bloqueo de un número es una medida de contención, pero no de solución definitiva si no hay judicialización. Por ello, **TELEFÓNICA** sugiere que el esfuerzo institucional se enfoque en fortalecer las mesas de trabajo operativas con la Fiscalía General de la Nación, la Policía Nacional y el sector bancario, estableciendo protocolos ágiles para que la evidencia técnica preservada por los operadores pueda ser utilizada eficazmente en la persecución penal de las estructuras delictivas.

TIGO

Reconoce la importancia de la educación del usuario como un pilar fundamental en la mitigación del fraude, pero advierte que las campañas educativas realizadas por los operadores no han demostrado una efectividad clara y medible.

En consecuencia, considera que imponer nuevas obligaciones pedagógicas a los PRST, PCA e IT genera cargas administrativas adicionales sin un retorno evidente para el usuario. En su lugar, plantea que la CRC, en coordinación con otras entidades del Estado, como el ColCERT, la Fiscalía General de la Nación y a la Policía Nacional, debe liderar directamente las campañas educativas masivas, utilizando medios de amplia difusión y no trasladando esta responsabilidad a los agentes regulados. Además, sugiere la articulación con organizaciones internacionales tales como GSMA para alimentar la lista de campañas fraudulentas de manera tal que si alguna modalidad de fraude aún no ha llegado a Colombia se logre actuar anticipadamente en la socialización y preparación de los usuarios ante el potencial riesgo.

Señala que los PRST cumplen un papel que responde a un mero transportador de tráfico, por lo que escapa de su control y dominio combatir un problema social que debe ser atendido por el Estado mismo.

U. EXTERNADO

Le parece acertado complementar el andamiaje regulatorio con medidas no regulatorias como: (i) campañas de educación digital que habiliten a los usuarios a reconocer llamadas y mensajes maliciosos; (ii) protocolos de cooperación intersectorial y traceback con autoridades (Policía Judicial, MinTIC) y sector financiero, bajo MOU y mesas técnicas; y (iii) sandboxes regulatorios para pilotar soluciones innovadoras (analítica de tráfico, reputación, etiquetado enriquecido, autenticación por RCD), con evaluación en entorno controlado. En el plano internacional, la GSMA Fraud & Security Group (FASG) promueve justamente esquemas de cooperación e intercambio de señales y estándares mínimos de seguridad para operadores, su adopción en Colombia facilitaría convergencia técnica y buenas prácticas.

RESPUESTA CRC:

ANDESCO, **ANDI, ASOMÓVIL**, **CCIT**, **CLARO**, **TELEFÓNICA**, **CCE** y **TIGO** coinciden en que sea la CRC quién lidere las campañas pedagógicas o de educación y que, además, coordine con otras entidades públicas, bajo el principio de colaboración interinstitucional, estos espacios o herramientas de sensibilización para que los ciudadanos tengan la capacidad de identificar fraudes por mensajes y llamadas de voz, mientras que **HABLAME** propone que sea el ColCERT la autoridad central de decisión antifraude, y en consecuencia el administrador del portal público de campañas para que el ciudadano

sepa que puede consultar y reportar allí mensajes sospechosos, reduciendo la intermediación de operadores y el riesgo de decisiones subjetivas.

CLARO señala que cualquier medida debería estar acompañada de un análisis de impacto normativo (AIN) y **TELEFÓNICA** propone ampliar las acciones de divulgación a otros actores del ecosistema digital y evaluar su impacto mediante indicadores como la reducción del fraude, encuestas de percepción y análisis del tráfico bloqueado.

En esa línea, la **UNIVERSIDAD EXTERNADO** propone una coordinación permanente entre CRC-MinTIC-SIC- sector financiero y KPIs de desempeño. En el mismo sentido, la **SFC** propone articular los contenidos de la CRC con los programas de educación financiera de la SFC y de los gremios bancarios, reforzando mensajes claros y consistentes, como que ninguna entidad financiera solicita claves ni información sensible a través de llamadas o mensajes de texto.

En complemento de lo anterior, la **SFC** sugiere la articulación de las medidas de educación ciudadana con los programas de educación financiera ya existentes, así como avanzar en la creación de un portal centralizado y dinámico que consolide información sobre campañas fraudulentas detectadas, actuaciones administrativas de recuperación de códigos cortos y demás información relevante sobre la materia. En igual sentido, **ASOBANCARIA** sugiere el fortalecimiento de campañas conjuntas entre la CRC y el sector financiero orientadas a la prevención del fraude por ingeniería social, integradas en aplicaciones bancarias, SMS y otros canales digitales.

Analizados los comentarios recibidos, la CRC considera necesario que exista coordinación y liderazgo entre los distintos agentes involucrados y el sector, de manera que se definan con claridad las responsabilidades específicas asociadas a las acciones de educación y prevención. Esto, bajo el contexto de que las responsabilidades no pueden ser delegadas ni trasladadas a terceros cuando correspondan a funciones propias dentro de la cadena de valor de los servicios tradicionales de SMS y voz, e incluso bajo el marco de asignación de los recursos de identificación.

En línea con lo anterior, y tomando los comentarios remitidos por Universidad Externado y la SFC frente a la necesidad de educación, formación y desarrollo, la CRC considera pertinente también complementar la alternativa propuesta en el sentido de fijar medidas específicas que atiendan la necesidad de promover la fuerza laboral en ciberseguridad.

La obligación de implementar programas de formación interna en materia de prevención del fraude cibernético se fundamenta en la necesidad de fortalecer las capacidades organizacionales de los agentes que intervienen en la prestación de servicios móviles y en el ecosistema de mensajería A2P. Diversos marcos internacionales reconocen que la gestión efectiva de los riesgos de ciberseguridad y fraude no depende exclusivamente de controles tecnológicos, sino también del conocimiento, preparación y conducta de los equipos responsables de la operación, atención al usuario, cumplimiento regulatorio y gestión comercial.

En particular, NIST SP 800-50 Rev. 1[42] sugiere que los programas de aprendizaje en ciberseguridad y privacidad deben gestionarse bajo un enfoque de ciclo de vida, orientarse al cambio de

[42] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Building an Information Technology Security Awareness and Training Program. Special Publication 800-50 Revision 1. Gaithersburg: NIST, 2003. Disponible en: https://csrc.nist.gov/pubs/sp/800/50/r1/final

comportamiento, articularse con la gestión del riesgo y contar con métricas y mecanismos de evaluación para su mejora continua.

En el mismo sentido, ISO/IEC 27001:2022[43] e ISO/IEC 27002:2022[44] reconocen la formación, sensibilización y entrenamiento en seguridad de la información como controles relevantes para asegurar que el personal y las partes interesadas comprendan sus responsabilidades en la protección de la información y en el cumplimiento de políticas y procedimientos aplicables a sus funciones.

Esta medida también resulta consistente con la política pública colombiana en materia de seguridad digital. El CONPES 3854[45] plantea el fortalecimiento de capacidades de múltiples partes interesadas para identificar, gestionar, tratar y mitigar riesgos de seguridad digital, mientras que el CONPES 3995 busca fortalecer capacidades en seguridad digital de ciudadanos, sector público y sector privado, así como promover la adopción de modelos, estándares y marcos de trabajo en la materia.

Así mismo, la Estrategia Nacional de Seguridad Digital 2025-2027[46] identifica la falta de cultura efectiva en seguridad digital y la necesidad de desarrollar fuerza laboral en ciberseguridad como desafíos relevantes para consolidar un entorno digital seguro, confiable y resiliente.

En el ámbito sectorial, la GSMA[47][48] ha señalado que los fraudes móviles aprovechan no solo vulnerabilidades técnicas, sino también mecanismos de ingeniería social dirigidos a inducir a las personas a realizar transacciones o entregar información personal, por lo cual la prevención exige acciones coordinadas de *awareness*, guías, innovación y cooperación de la industria móvil.

Por lo anterior, la CRC considera razonable exigir que PRST y asignatarios de recursos de identificación del ecosistema A2P cuenten con programas periódicos de formación interna que cubran modalidades

[43] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Ginebra: ISO, 2022. Disponible en: https://www.iso.org/standard/27001

[44] Especialmente el control 6.3 de la norma ISO 27002, subraya la necesidad de que las organizaciones implementen programas de concienciación, educación y capacitación en seguridad de la información para garantizar que los empleados y las partes interesadas pertinentes comprendan sus responsabilidades en materia de seguridad y puedan proteger eficazmente los activos de información.
Fuentes:
1. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Ginebra: ISO, 2022. Disponible en: https://www.iso.org/standard/75652.html
2. ISMS.ONLINE. ISO 27002 Control 6.3: Information Security Awareness, Education and Training. Brighton: ISMS.online, s.f. Disponible en: https://www.isms.online/iso-27002/control-6-3-information-security-awareness-education-and-training/

[45] DNP. Documentos CONPES de confianza y seguridad digital. Bogotá D.C.: DNP, s.f. Disponible en: https://dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

[46] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MinTIC). La Estrategia Nacional de Seguridad Digital llega para enfrentar las crecientes amenazas cibernéticas. Bogotá D.C.: MinTIC, 2025. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403023:La-Estrategia-Nacional-de-Seguridad-Digital-llega-para-enfrentar-las-crecientes-amenazas-ciberneticas

[47] GSM ASSOCIATION (GSMA). Fraud and Scams: Keeping consumers safe from fraud and scams. Londres: GSMA, 2025. Disponible en: https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf

[48] GSM ASSOCIATION (GSMA). Fraud and scams: protecting consumers and communications networks. Documento presentado ante el Body of European Regulators for Electronic Communications (BEREC). Bruselas, 2025. Disponible en: https://www.berec.europa.eu/system/files/2025-05/2.%20GSMA.pdf

de fraude, obligaciones regulatorias, procedimientos de detección y reporte, protocolos de atención al usuario y protección de datos personales, asegurando cobertura sobre las áreas funcionales que tienen mayor incidencia en la prevención, detección, gestión y mitigación del fraude.

Con base en los anteriores comentarios, se complementarán las alternativas relacionadas con la educación a la ciudadanía, en el sentido de incluir medidas con ese enfoque que son comunes para servicios SMS y voz, y otras independientes para SMS y voz respectivamente, así:

1. **Medidas educativas o pedagógicas comunes para SMS y voz:**

    a. La CRC elaborará un documento que contenga tips, recomendaciones, guías o consejos para que los ciudadanos lo puedan consultar en un micrositio que se creará en la página web de la Comisión y que será difundido por los distintos canales de comunicación que usa la Comisión, con la finalidad de poner en conocimiento o educar al público en general acerca de la identificación de SMS o llamadas de voz con fines presuntamente fraudulentos.

    Con un objetivo similar, pero dirigido a entidades públicas, se elaborará un documento de consulta exclusiva para esas entidades estatales que será compartido en un canal creado para esos efectos.

    b. De manera correlativa, se establecería la obligación a cargo de los asignatarios y operadores de difundir el mencionado micrositio de la CRC en sus respectivas páginas web para masificar la consulta por parte de los ciudadanos.

    c. Los asignatarios y los operadores tendrían la obligación de desarrollar campañas pedagógicas para la prevención de fraude, en la periodicidad y los términos que la Comisión definiría en la regulación. De manera concreta, la Comisión definirá un hashtag para hacerle seguimiento a esas campañas pedagógicas.

    Tal como lo propuso **ASOBANCARIA**, las campañas a desarrollar deberían incluir varios medios de comunicación, ser masivas y sostenidas en el tiempo; inclusive contemplando insumos necesarios para la educación financiera, tal como lo propuso la **SFC**.

    Bajo esta alternativa, estos agentes también tendrán la obligación de capacitar a sus equipos internos en la forma en la que se definirá en la regulación.

    d. La CRC promovería espacios interinstitucionales con todas las entidades involucradas e interesadas en la prevención del fraude para crear sinergias y aunar esfuerzos en materia pedagógica y educativa. Además, se evaluará la participación de organizaciones internacionales con esos mismos propósitos y efectos.

2. **Medidas educativas o pedagógicas para los servicios de SMS:**

    a. La Comisión promovería la difusión pública de sus actuaciones administrativas de recuperación, de modo que se facilite la participación de cualquier tercero interesado, en los términos de los artículos 37 y 38 de la Ley 1437 de 2011, Código de

Procedimiento Administrativo y de lo Contencioso Administrativo. Esto ayudaría a que cualquier interesado se vincule a los trámites administrativos de recuperación de recursos de identificación para los fines que correspondan, entre otros, aportar y solicitar pruebas. Lo anterior garantizaría un mayor nivel de transparencia y, además, facilitaría a la Comisión conta con elementos de juicio adicionales para adoptar sus decisiones.

Esta difusión se realizaría en un micrositio específico de la página web de la Comisión que se crearía para estos efectos, en el cual la ciudadanía en general podría conocer el inicio y resultado de las actuaciones administrativas descritas.

b. La Comisión evaluará la posibilidad de incluir en la regulación una exigencia para los asignatarios de códigos cortos para SMS y USSD, según la cual deberán incluir en sus contratos con clientes del sector financiero la carga contractual de que los referidos clientes inscriban, en el portal web que la CRC crearía para estos efectos, los códigos cortos que usan para soportar sus servicios de mensajería, información que podrá ser consultada por el público en general en el micrositio específico creado para estos efectos.

3. Medidas educativas o pedagógicas para los servicios de voz:

a. La Comisión evaluará la posibilidad de incluir en la regulación una exigencia para los PRST, según la cual deberán incluir en sus contratos con clientes del sector financiero la carga contractual de que los referidos clientes inscriban, en la plataforma web que la CRC crearía para estos efectos, aquella numeración E.164 geográfica o no geográfica que usan para soportar sus servicios de llamadas de voz, información que podrá ser consultada por el público en general en el micrositio específico creado para estos efectos.

4. Medidas de formación interna en materia de prevención del fraude.

a. La Comisión evaluará la posibilidad de incluir en la regulación una exigencia para los PRST, PCA e IT según la cual deberán implementar programas de formación interna en materia de prevención del fraude cibernético dirigidos a sus equipos de trabajo, cubriendo unos contenidos mínimos.

Finalmente, los comentarios presentados por los operadores y demás agentes interesados en relación con las problemáticas asociadas a la creación de sistemas centralizados de trazabilidad de PQR o de portales de denuncia administrados por la CRC, entre ellos los planteados por **COMCEL, TELEFÓNICA y ANDESCO**, serán debidamente considerados en el análisis regulatorio.

En particular, dichas observaciones, junto con las demás consideraciones relevantes formuladas en respuesta a la consulta, serán evaluadas en el proceso de análisis de las alternativas regulatorias, con el fin de determinar de manera fundamentada si la alternativa propuesta debe mantenerse, ajustarse o prescindirse de ella

Respuesta a las preguntas de la consulta frente a las temáticas enfocadas en la educación de la ciudadanía

Frente a las respuestas recibidas a las preguntas formuladas sobre esta temática, a continuación, se presenta un resumen de los principales planteamientos realizados por los participantes. Sin perjuicio de lo anterior, se destaca que la mayoría de estos aportes ya fueron analizados en la Sección 8.2.6 del presente documento; no obstante, algunas respuestas incluían elementos específicos de relevancia que fueron abordados en el marco de la respectiva pregunta.

Lo anterior se presenta con el propósito de consolidar los aspectos más relevantes expuestos por los participantes y facilitar su análisis integral en la Sección 8.2.6, en la cual se desarrollan las consideraciones relacionadas con la educación a la ciudadanía en materia de prevención del fraude, incorporando tanto los aportes derivados del formulario de consulta como la evaluación de las alternativas regulatorias asociadas a esta temática.

- ¿Qué acciones voluntarias (no regulatorias) adelanta actualmente su organización o conoce usted en el mercado para informar a los usuarios sobre riesgos de fraude? ¿Son efectivas? ¿Tienen métricas de impacto?

CLARO

Señala que realiza monitoreo y bloqueo de llamadas de forma automática, basado en diferentes comportamientos como: llamadas de corta duración; alto volumen de llamadas desde un mismo número A; llamadas internacionales con número A usando el country Code de Colombia +57, este bloqueo es parcial para casos de numeración móvil por la afectación que se pueda presentar para usuarios de roaming; llamadas entrantes internacionales con numeración fija colombiana está bloqueado al 100%.

En cuanto a mensajería expone que existen controles y bloqueos por volúmenes; y que, desde el área de fraude y el área de comunicaciones de la compañía se realizan actividades tipo campañas por diferentes canales (Web, mensajería, redes sociales etc.), informando a los usuarios sobre el fraude cibernético, por lo que, concluye que cualquier nueva obligación genera cargas económicas, operativas y técnicas que implican el desarrollo y mantenimiento de nuevas plataformas, por lo que, señala que cualquier nueva regla debe tener un Análisis de Impacto Normativo (AIN).

SFC

Menciona que desde esa entidad se adelantan de manera permanente campañas pedagógicas y recomendaciones de seguridad dirigidas al consumidor financiero, utilizando canales como la página web y redes sociales para alertar sobre nuevas modalidades de fraude.

Estas acciones se complementan con los programas de educación financiera que por normativa deben implementar las entidades vigiladas por esta Superintendencia, las cuales deben contender aspectos relacionados con la seguridad en el uso de los productos, protección a la información personal, prevención de fraudes, entre otros elementos, que al final permitan al consumidor contar con herramientas para propender por una mejor experiencia de sus productos en el marco de un ambiente de seguridad en las transacciones.

TELEFÓNICA

El operador presentó una respuesta consolidada a todas las preguntas relacionadas con la temática de educación a la ciudadanía.

En concreto, **TELEFÓNICA** ratifica su compromiso continuo con la pedagogía, evidenciado en las campañas voluntarias que ha desplegado en sus canales digitales y centros de experiencia para alertar sobre modalidades como smishing y vishing. Sin embargo, este operador considera que la efectividad de estas acciones no puede recaer exclusivamente en los operadores de telecomunicaciones, ya que es imperativo que las obligaciones de divulgación pedagógica se extiendan de manera vinculante a los agregadores, integradores tecnológicos (IT) y proveedores de contenidos y aplicaciones (PCA), dado que gran parte del fraude suplanta a entidades financieras y comercios cuyos servicios son el gancho para el engaño.

Respecto de la propuesta de crear un "Portal de la CRC" que centralice listas de números reportados y campañas fraudulentas, **TELEFÓNICA** dice que valora la intención de transparencia, pero advierte sobre retos operativos críticos para su viabilidad, toda vez que la actualización de la información debe ser en tiempo real para ser útil, lo cual requiere automatización y no procesos manuales de carga. Añade que es fundamental aclarar el modelo de financiación de dicho portal, pues los costos de su desarrollo y mantenimiento no deben ser trasladados a los proveedores de redes.

En lo que respecta a la creación de un sistema centralizado de trazabilidad de peticiones, quejas y recursos (PQR) administrado por la CRC, **TELEFÓNICA** expresa una preocupación técnica y jurídica significativa, ya que centralizar bases de datos con el detalle de las reclamaciones de fraude de todos los usuarios del país conlleva riesgos elevados de seguridad de la información (creación de un honeypot o punto único de falla) y desafíos complejos en materia de protección de datos personales (habeas data). Así, considera que la trazabilidad es necesaria, pero esta debe realizarse mediante reportes estandarizados y agregados que los operadores envíen a la autoridad, y no mediante la entrega de la gestión de las PQR a un sistema centralizado, el cual podría burocratizar la atención y exponer la privacidad de los ciudadanos. Finaliza en el sentido de decir que la métrica de éxito de la estrategia educativa no debe ser solo el volumen de denuncias, sino el alcance efectivo y la reducción de la tasa de éxito de los intentos de fraude, medida a través de encuestas de percepción y análisis de tráfico bloqueado.

TIGO

Indica que actualmente se desarrollan campañas voluntarias de educación y sensibilización dirigidas a los usuarios para prevenir el fraude cibernético. No obstante, considera que su efectividad es difícil de medir de manera directa, dado que este tipo de iniciativas tienen un carácter masivo y preventivo que impide establecer una relación causal entre la exposición a una campaña específica y la evitación de un fraude determinado. Agrega que la información sobre eventos de fraude proviene generalmente de reportes posteriores, lo que limita la posibilidad de atribuir resultados concretos a acciones pedagógicas y puede generar estimaciones imprecisas o sesgadas.

RESPUESTA CRC:

CLARO destaca la posible implementación de mecanismos técnicos de monitoreo y bloqueo automático de llamadas y mensajes con patrones sospechosos como medida complementaria de mitigación, aunque advierte que cualquier nueva obligación regulatoria debería estar precedida de un Análisis de Impacto Normativo (AIN). Por su parte, **TIGO** señala que la efectividad de las campañas

puede ser difícil de medir debido a su carácter preventivo y masivo; **TELEFÓNICA** propone ampliar las acciones de divulgación a otros actores del ecosistema digital, como agregadores, integradores tecnológicos (IT) y proveedores de contenidos y aplicaciones (PCA), así como evaluar su impacto mediante indicadores como la reducción en la tasa de éxito del fraude, encuestas de percepción o análisis del tráfico bloqueado; mientras que la **SFC** indica que estas iniciativas pueden complementarse con los programas de educación financiera que deben implementar las entidades vigiladas, orientados al uso seguro de productos financieros, la protección de la información y la prevención de fraudes.

Considerando lo anterior, la CRC tendrá en cuenta los aportes recibidos y remite a la Sección 8.2.6 del presente documento, en la cual se desarrollan de manera integral las acciones relacionadas con la educación a la ciudadanía en materia de prevención del fraude. Este análisis se adelanta bajo un enfoque de simplificación normativa, orientado a articular las distintas iniciativas y responsabilidades existentes dentro de un marco común, privilegiando medidas de divulgación, sensibilización y coordinación institucional que resulten proporcionales y efectivas, evitando al mismo tiempo la incorporación de nuevas obligaciones regulatorias cuando no se evidencie un valor agregado claro frente a las herramientas ya disponibles.

- ¿Qué cargas técnicas y económicas representaría para los PRST, los IT y los PCA implementar obligaciones de divulgación pedagógica frente al fraude cibernético?

CLARO

Expone que se presentarían múltiples cargas, tales como la creación de las campañas, ya sean vía SMS o por otros medios, el valor de la transmisión de la misma, más la implementación de los reportes de campañas que la CRC plantea imponer, crear y actualizar contenidos, habilitar canales informativos (web, apps, IVR, SMS) y ajustar sistemas y procesos internos. También señala que se requieren recursos humanos para gestión y reporte, y concluye que, aunque generan una carga moderada, contribuyen a reducir incidentes y fortalecer la confianza del usuario.

Solicita a la CRC evaluar primero la efectividad de la suspensión provisional, fortalecer los procesos de recuperación y articulación sectorial, y realizar un Análisis de Impacto Normativo antes de implementar la medida propuesta. Solo si este análisis demuestra que el fraude persiste y no puede ser controlado con las herramientas actuales tendría sentido considerar nuevos desarrollos técnicos. Dado los retos y tiempos de implementación, la medida no se considera viable, especialmente porque la problemática ya se ha mitigado en gran parte con la suspensión provisional aplicada por la CRC.

TIGO

Señala que la implementación de obligaciones de divulgación pedagógica frente al fraude cibernético implica costos técnicos y económicos significativos, ya que requiere capacidad instalada permanente, incluyendo procesos definidos para campañas, equipos especializados en comunicación y diseño, y plataformas tecnológicas de difusión. No obstante, considera que los agentes deben mantener autonomía para diseñar sus estrategias según sus capacidades. Asimismo, destaca que la alternativa de «Pedagogía y lista de campañas más denunciadas» permitiría focalizar acciones preventivas con base en riesgos reales, optimizando recursos y evitando cargas uniformes, por lo que se perfila como una medida flexible y costo-eficiente para la mitigación del fraude.

- Frente a la alternativa de divulgación pedagógica por parte de PRST, PCA e IT ¿Qué tipo de contenidos deberían ser obligatorios? (ejemplos reales, guías de prevención, alertas recientes, recomendaciones prácticas, etc.)

CLARO

Considera que esta obligación debe estar en cabeza de la CRC y de otras instituciones del estado. Es necesario recordar que el código corto es asignado por la CRC. En este sentido, debe tener un mínimo de diligencia frente al asignatario de la misma.

SFC

Menciona que, para la definición del canal más adecuado para divulgar las estrategias de educación, recomienda realizar un estudio previo que caracterice a la población que será destinataria de los programas de educación. Esto en la medida que, a partir de su diagnóstico, las estrategias de educación podrían causar un mayor impacto al estar diseñadas a la medida y de acuerdo con los perfiles y necesidades de los consumidores.

TIGO

Considera que es más efectivo adoptar un enfoque flexible de divulgación pedagógica basado en herramientas dinámicas como guías de prevención, casos reales anonimizados, alertas sobre nuevas modalidades de fraude, recomendaciones prácticas y mensajes de autocuidado digital, en lugar de contenidos rígidos u obligatorios. Señala que este esquema permitiría adaptar las estrategias de comunicación a la evolución constante del fraude, facilitando respuestas oportunas y focalizadas según el tipo de riesgo, el público objetivo y el canal de difusión, lo que fortalecería la prevención, optimizaría el impacto de las campañas y evitaría limitar la innovación y la capacidad de adaptación.

- Frente a la alternativa de divulgación pedagógica por parte de PRST, PCA e IT ¿Cuál considera es el canal más apropiado para esta divulgación? (ejemplo: SMS masivos, mensajes en facturas, Landing pages, Push notifications en apps, etc.)

CLARO

Considera que esta obligación debe estar en cabeza de la CRC y de otras instituciones del Estado. Señala que el código corto es asignado por la CRC, por lo que debe tener un mínimo de diligencia frente al asignatario de la misma. Concluye que el medio debería ser definido por la CRC, pero recomienda información en su página web, y propagandas en canales abiertos.

TIGO

Señala que no existe un canal único óptimo para la divulgación pedagógica, ya que su efectividad depende de una estrategia multicanal articulada según el tipo de mensaje, el nivel de urgencia y el perfil del usuario. Indica que los canales directos como SMS masivos, mensajes en facturas y notificaciones push son adecuados para alertas inmediatas, mientras que herramientas como landing pages permiten ampliar información y centralizar contenidos pedagógicos. Asimismo, manifiesta que

las redes sociales facilitan mayor alcance y segmentación. Considera que este enfoque complementario permite reforzar mensajes, adaptarlos a los hábitos de los usuarios y maximizar la efectividad de las acciones de prevención.

- Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, ¿Qué nivel de detalle debería tener la información publicada para ser útil sin generar nuevas vulnerabilidades? (ejemplo: números reportados, patrones o modus operandi, ejemplos de mensajes fraudulentos, etc.)

CLARO

Considera inútil la medida, dado que a su juicio el usuario generalmente no conoce ni consulta este tipo de medidas, por lo que su implementación terminaría generando una carga adicional para los PRSTM. Además, implicaría diversos retos operativos y económicos, como el desarrollo y mantenimiento de un portal, su integración con sistemas internos, la actualización permanente de datos y mecanismos de seguridad, costos de infraestructura tecnológica, contratación de personal para administración y soporte, así como gastos asociados a campañas de divulgación. Concluye que existen riesgos de seguridad y filtración de datos personales al centralizar la información en un portal.

TIGO

Considera que el portal de campañas más denunciadas debe publicar información con un nivel de detalle suficiente para alertar y educar a usuarios y agentes del sector, sin exponer elementos que puedan ser aprovechados por actores fraudulentos. Para ello, sugiere incluir de forma agregada y dinámica códigos cortos, numeraciones o rangos asociados a fraudes, descripciones generales del modus operandi sin revelar aspectos técnicos sensibles, ejemplos ilustrativos anonimizados de mensajes o llamadas fraudulentas y recomendaciones claras para identificar señales de alerta. Señala que este enfoque permitiría fortalecer la prevención y la capacidad de respuesta sin generar nuevas vulnerabilidades.

RESPUESTA CRC:

Frente a los comentarios recibidos, **CLARO** señala que la implementación de un portal podría no resultar útil y advierte que su desarrollo implicaría cargas operativas y económicas adicionales para los operadores. Por su parte, **TIGO** propone que, en caso de implementarse, el portal publique únicamente información agregada y no sensible, como códigos cortos o rangos asociados a fraude, descripciones generales del modus operandi, ejemplos anonimizados de mensajes fraudulentos y recomendaciones de prevención, con el fin de informar y alertar a los usuarios sin generar nuevas vulnerabilidades.

Analizados estos planteamientos, la CRC acoge las consideraciones presentadas por los agentes y reconoce la importancia de que, en caso de desarrollarse una herramienta de este tipo, esta se estructure bajo criterios que garanticen su robustez, confiabilidad y adecuada gestión de la información, evitando la divulgación de datos sensibles que puedan ser utilizados de manera indebida.

En ese sentido, la CRC tendrá en cuenta las consideraciones mencionadas y remite a la Sección 8.2.6 del presente documento, en la cual se desarrollan los elementos expuestos por **CLARO** y **TIGO**, con

el propósito de abordar de manera integral las acciones de educación y divulgación de información a la ciudadanía en materia de prevención del fraude. Lo anterior se realiza bajo un enfoque de simplificación normativa, procurando articular estas iniciativas se encuentren bajo un denominador común que permita fortalecer las acciones de prevención y educación dirigidas a los usuarios, sin generar cargas regulatorias innecesarias.

- Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, ¿Qué beneficios concretos considera que traería este portal para los usuarios y agentes del sector?

RESPUESTAS:

CLARO

No considera beneficio alguno sobre esta alternativa.

SFC

Considera que la implementación de un portal centralizado de campañas denunciadas traería beneficios concretos al crear un frente común de información en tiempo real. Para el usuario, funcionaría como una herramienta de consulta rápida para verificar la legitimidad de un mensaje sospechoso, reduciendo la asimetría de información que los delincuentes aprovechan.

Para los agentes del sector y las entidades financieras, este portal se convertiría en un insumo de información colaborativa, permitiendo identificar y replicar rápidamente las nuevas tipologías de fraude detectadas por otros actores. No obstante, este portal debe garantizar una actualización inmediata y ser de fácil acceso, evitando que se convierta en un repositorio estático y fortalezca la capacidad de autoprotección del consumidor financiero.

TIGO

Considera que un portal que consolide las campañas de fraude más denunciadas ofrecería beneficios tanto para los agentes del sector como para los usuarios. Señala que, para los PRST, PCA e IT, representaría un insumo estratégico y actualizado que facilitaría la identificación oportuna de modalidades de fraude en circulación, permitiendo diseñar acciones pedagógicas focalizadas y alinear esfuerzos de prevención con base en una fuente común, confiable y basada en denuncias reales. Indica que, para los usuarios, el portal brindaría acceso a información clara y actualizada que permitiría reconocer patrones de fraude, identificar señales de alerta y adoptar medidas preventivas, fortaleciendo la cultura de autoprotección y la confianza en las estrategias de mitigación.

- Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, en caso de que aplique, ¿qué cargas técnicas y económicas representaría para su organización implementar estas obligaciones?

RESPUESTAS:

CLARO

Expone que la implementación de esta medida implicaría diversos retos operativos y económicos, entre ellos el desarrollo y mantenimiento del portal, su integración con sistemas internos, la actualización periódica de la información y de los mecanismos de seguridad para evitar vulnerabilidades, los costos asociados a la infraestructura tecnológica, la contratación de personal para su administración y soporte, así como los gastos derivados de campañas de divulgación dirigidas a los usuarios.

TIGO

Señala que la alternativa 2 de la temática «Acciones educativas que aumenten el conocimiento de los usuarios», en donde se propone que la CRC creará y administrará un portal que incluya la lista con las campañas más denunciadas ante esta entidad los agentes del sector incluidos los PRST, los PCA y los IT tendrían como única responsabilidad la consulta de dicho portal, sin contar con injerencia alguna en su diseño, operación o implementación técnica.

- ¿Considera viable técnica y operativamente crear un sistema de trazabilidad centralizado de PQR relacionadas con fraude por mensajes de texto o llamadas? Justifique su respuesta.

RESPUESTAS:

CLARO

Expone que la medida propuesta generaría una carga adicional para los PRSTM, quienes ya gestionan las PQR de los usuarios. En su lugar, se propone establecer un mecanismo mediante el cual, cuando un PRSTM detecte un SMS con contenido presuntamente fraudulento, solicite al PCA la verificación de la veracidad de la información, con copia a la CRC, y con obligación de respuesta en un plazo máximo de dos horas. Si el PCA no valida el contenido, el PRSTM podría bloquear el envío de los mensajes y la CRC iniciar una investigación administrativa de oficio.

TIGO

Considera que la creación de un sistema centralizado de trazabilidad de PQR sobre fraude en llamadas y mensajes tendría como finalidad servir de herramienta de divulgación, prevención y mitigación. Sin embargo, estima que este objetivo puede lograrse mediante mecanismos más simples y costo-eficientes, como un portal que consolide las campañas más denunciadas. Este último permitiría difundir información relevante sin incurrir en los altos costos técnicos, operativos y económicos asociados a un sistema de trazabilidad, ni enfrentar retos de interoperabilidad, estandarización de datos y protección de información sensible. Por esta razón indica que el portal informativo se percibe como una alternativa más viable técnica y operativamente, al cumplir el mismo propósito con menores cargas y complejidades.

- ¿Qué variables o campos considera debería contener este sistema de trazabilidad para permitir análisis útiles?

RESPUESTAS:

CLARO

Expone que no es viable el sistema de trazabilidad, en la medida que solo cargaría más a los PRSTM quienes son los que reciben las PQR de los usuarios.

- ¿Qué riesgos de seguridad o privacidad considera deben ser tenidos en cuenta al centralizar la información de PQR relacionadas con fraude?

RESPUESTAS:

CLARO

Considera que la medida no es viable, ya que implica múltiples riesgos, entre ellos la posible exposición de datos personales al tratarse de PQR centralizadas de varios actores, el acceso no autorizado al sistema y el robo de información, así como la potencial vulneración de los sistemas de los involucrados al concentrar la información en un solo punto. Además, su implementación debería alinearse estrictamente con las leyes de protección de datos personales.

PTC

PTC sugiere considerar los controles de seguridad de la información introducidos en la ISO 27001

TIGO

Advierte que la centralización de información de PQR sobre fraude implica riesgos significativos de seguridad y privacidad, dado que estos registros pueden contener datos personales y sensibles, lo que aumenta la posibilidad de accesos no autorizados, filtraciones o usos indebidos. Asimismo, señala que existen riesgos asociados a la integridad y calidad de la información, ya que errores en su registro o actualización podrían generar alertas imprecisas y afectar la confianza en el sistema. Finalmente, indica que la interoperabilidad entre plataformas de distintos agentes plantea desafíos adicionales en materia de estándares de seguridad, trazabilidad de accesos y asignación de responsabilidades ante eventuales incidentes.

RESPUESTA CRC:

CLARO y **TIGO** advierten riesgos asociados a la exposición de datos personales, accesos no autorizados, filtraciones de información y vulneración de los sistemas al concentrar datos en un único punto, además de desafíos en integridad, calidad de la información e interoperabilidad entre plataformas. Como propuestas, **PTC** sugiere adoptar controles de seguridad de la información basados en la norma ISO 27001, mientras que **CLARO** enfatiza que cualquier implementación debe alinearse estrictamente con la normativa de protección de datos personales, evidenciando que el principal reto radica en garantizar altos estándares de seguridad, trazabilidad y gobernanza de la información para evitar nuevas vulnerabilidades.

Respecto de lo antes expuesto, la CRC tendrá encuentra las consideraciones mencionadas y remite a la Sección 8.2.6 del presente documento, con el propósito de desarrollar los elementos previamente expuestos por **CLARO** y **TIGO** bajo el propósito de realizar en esa sección el análisis y las

consideraciones relacionadas con la educación a la ciudadanía en materia de prevención del fraude, desde una perspectiva integral y de alcance general, lo anterior, procurando su articulación bajo un denominador común que permita configurar el mejor escenario posible para fortalecer las acciones de prevención y educación dirigidas a los usuarios.

- ¿Qué componentes debería incluir estrategia educativa conjunta entre la CRC, los agentes regulados y otras entidades competentes? (por ejemplo: campañas nacionales, identificación de patrones emergentes, material didáctico para usuarios, indicadores de éxito, etc.)

RESPUESTAS:

CLARO

Propone que la CRC implemente campañas nacionales masivas de prevención mediante la difusión en medios tradicionales y digitales para alertar sobre fraudes, la publicación de informes periódicos sobre nuevas modalidades y su impacto en los usuarios, así como la elaboración de material didáctico accesible para todas las edades, como guías prácticas, videos, infografías y simulaciones. Asimismo, propone capacitar a los actores involucrados y establecer protocolos de atención y prevención, promover la colaboración entre entidades para unificar estrategias educativas que faciliten la comprensión del usuario y desarrollar canales interactivos, como portales web, redes sociales y aplicaciones, para la emisión de alertas y la recepción de denuncias.

SFC

Considera que la estrategia educativa conjunta debería incluir campañas coordinadas entre autoridades, operadores y entidades financieras; alertas oportunas sobre las modalidades de fraude que estén circulando; material educativo claro y accesible para distintos tipos de usuarios; y mecanismos de seguimiento que permitan medir su efectividad, como la reducción de casos y el aumento en el reporte ciudadano.

En todo caso, sugiere que el esquema normativo y regulatorio que se defina incorpore lineamientos dirigidos a que todos los actores adopten programas de educación efectivos, dirigidos a la adecuada utilización de estas herramientas.

TIGO

Propone que la estrategia educativa conjunta sea coordinada centralmente por la CRC para maximizar su impacto y reducir cargas operativas para los PRST. Señala que esta debería incluir campañas nacionales de alcance general diseñadas con apoyo de autoridades competentes, basadas en información agregada sobre modalidades de fraude. Asimismo, sugiere que la identificación de patrones emergentes se realice de forma centralizada y que la CRC disponga un repositorio común de material didáctico estandarizado reutilizable por los agentes regulados. Finalmente, recomienda que los indicadores de éxito se basen en métricas agregadas de alcance y difusión, permitiendo una estrategia coherente, costo-eficiente y sustentada en la coordinación interinstitucional, donde los PRST actúen principalmente como canales de divulgación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

8.2.7 Sobre las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

8.2.7.1 Reincidencia (códigos cortos)

ANDESCO

Afirma que existe una omisión relevante: la CRC no habría atendido la solicitud –planteada reiteradamente por diversos actores– de permitir expresamente la terminación de contratos de acceso con PCA/IT reincidentes en el envío de SMS fraudulentos. Sostiene que, en la práctica, aun cuando se recupere un código corto involucrado, el mismo PCA/IT puede continuar el envío fraudulento mediante otros códigos, lo cual perpetúa el daño al usuario y reduce la eficacia de las medidas. Por ello, **ANDESCO** considera que una habilitación clara para terminar la relación contractual con reincidentes fortalecería incentivos de cumplimiento y evitaría trasladar injustificadamente al operador el riesgo de continuidad del fraude.

En línea con lo anterior, **ANDESCO** recalca que la asignación de códigos cortos es competencia directa de la CRC y que, por tanto, la Comisión debería realizar un escrutinio más exhaustivo de solicitantes (calidades, antecedentes, condiciones de uso) para disminuir el riesgo ex ante, en vez de corregirlo después mediante exigencias tecnológicas costosas para PRST.

ANDI

Sostiene que la CRC no respondió al comentario expreso realizado por diferentes actores con el cual se solicitó que la CRC permitiera la terminación de contratos con PCA/IT abiertamente reincidentes en el envío de SMS con contenido fraudulento. En su opinión, esta situación ha permitido que los PCA/IT, una vez notificados de la recuperación del código corto, utilicen los demás códigos asignados para enviar a través de dicho código los mensajes fraudulentos, y continuar con el fraude.

Adicionalmente, la **ANDI** advierte sobre la importancia de aclarar que el encargado de asignar la numeración corta es la CRC. En este sentido, dice, la CRC debe hacer una evaluación exhaustiva de los solicitantes de la numeración, en donde constate las calidades, condiciones, y demás requisitos que permitan dar tranquilidad del uso que se va a dar al potencial asignatario de la numeración, y no trasladar con posterioridad el problema a los PRSTM quienes se ven obligados a implementar medidas tecnológicas para evitar el envío de mensajes con contenido fraudulento. Para la **ANDI**, si la asignación del código corto se hace de manera consciente, a un usuario que la utiliza de manera adecuada, este tipo de problemas no se presenta. Por el contrario, si se evidencia que la numeración no está siendo bien utilizada, la consecuencia debe ser la recuperación de los códigos cortos mal utilizados, y no volver a asignar hasta tanto demuestre que implementó medidas que evidencien su buen uso.

En coherencia con lo anterior, la **ANDI** sintetiza una ruta de actuación previa a nuevas medidas: (i) evaluar el efecto de la suspensión provisional, (ii) permitir terminación de contratos con reincidentes, (iii) endurecer filtros de asignación, (iv) habilitar bloqueo preventivo de SMS/llamadas cuando haya indicios de fraude y, solo después, (v) realizar el AIN de las medidas restantes.

ASOBANCARIA

Sugiere que los esquemas de gestión de reincidencia contemplen consecuencias automáticas y progresivas frente a conductas reiteradas, así como mecanismos de seguimiento periódico que permitan evaluar su efecto disuasivo y ajustar las medidas cuando sea necesario.

En opinión de **ASOBANCARIA**, es importante promover la integración del sector financiero con los sistemas administrados por la CRC para el reporte de campañas fraudulentas, numeración sospechosa y otros eventos relevantes, bajo esquemas interoperables y estandarizados. Asimismo, **ASOBANCARIA** advierte que es necesario avanzar hacia mecanismos de bloqueo preventivo e inmediato de los recursos reportados por fraude, con criterios homogéneos, trazabilidad adecuada y procedimientos de revisión claramente definidos.

En complemento de lo anterior, **ASOBANCARIA** considera conveniente la incorporación de penalizaciones claras frente al uso indebido y la reincidencia en la utilización de recursos de identificación. Adicionalmente, **ASOBANCARIA** sugiere la implementación de controles específicos frente a modalidades como el SIM swapping, mediante verificaciones reforzadas en los procesos de cambio de SIM, el uso de autenticación multifactor, biometría o estándares como FIDO2, así como la generación de alertas preventivas al usuario y la aplicación de bloqueos temporales de originación A2P hasta la culminación de las validaciones correspondientes, dada la relevancia de la red móvil como factor crítico de autenticación para múltiples servicios financieros.

Para finalizar, **ASOBANCARIA** sugiere que las soluciones que desarrolle la Comisión se deben diseñar bajo un enfoque interoperable y API-ready, de forma que la información generada pueda ser consumida de manera preventiva por las entidades en sus procesos de gestión de fraude, monitoreo y toma de decisiones. En este mismo sentido, **ASOBANCARIA** considera que se debe evaluar la incorporación de una alternativa adicional consistente en la exigencia de procesos de KYC por parte de los operadores móviles para la verificación de la identidad de los usuarios que soliciten la reexpedición de SIMs o adquisición de nuevas líneas, medida que ha sido adoptada en otros países y que podría contribuir de manera significativa a la prevención del fraude desde el origen del servicio.

ASOMÓVIL

Insiste en la necesidad de que el marco regulatorio incorpore una respuesta más severa frente a la reincidencia de los PCA e integradores tecnológicos involucrados en fraudes cursados a través de redes móviles. En particular, plantea que la sola recuperación del código corto no constituye una consecuencia suficiente ni materialmente disuasiva, pues no afecta de manera real a los agentes que facilitan o permiten la conducta y, en la práctica, puede ser asumida como un costo menor del negocio ilícito.

Desde esa perspectiva, propone habilitar expresamente a los PRSTM para terminar las relaciones contractuales con los reincidentes, con fundamento en el principio de buena fe contractual y en la necesidad de impedir que ciertos actores continúen utilizando la infraestructura de mensajería para fines fraudulentos. Asimismo, solicita complementar esta medida con un régimen específico para reincidentes que contemple consecuencias escalonadas y efectivas, tales como multas proporcionales al daño causado, la prohibición temporal o definitiva de recibir nuevas asignaciones de numeración y, en casos de persistencia, la pérdida del registro como proveedor de contenidos. Incluso, sugiere

establecer un periodo de "mora" para la entrega de nuevos códigos cortos a quienes hayan defraudado la confianza regulatoria.

CCE

Sostiene que la CRC no responde al comentario expreso realizado por diferentes actores con el cual solicitó que la CRC permitiera la terminación de contratos con PCA/IT abiertamente reincidentes en el envío de SMS con contenido fraudulento. Enfatiza en que esta situación ha permitido que, una vez recuperado un código corto por uso indebido, los mismos continúen ejecutando prácticas fraudulentas mediante otros códigos asignados, lo que evidencia una falla del enfoque correctivo vigente y una ineficacia del régimen disuasivo actual.

Considera que la reincidencia en el uso indebido de códigos cortos no está siendo abordada de manera efectiva por el régimen vigente. Insiste en que la recuperación aislada del recurso no genera un desincentivo real y permite la continuidad del fraude.

Por ello, propone que la CRC incorpore consecuencias más severas y estructurales frente a los reincidentes, incluyendo la imposibilidad de acceder nuevamente a recursos de numeración hasta tanto se demuestre la adopción de medidas correctivas reales.

Sobre la asignación de códigos cortos, indica que el encargado de asignar la numeración corta es la CRC y que en este sentido debe hacer una evaluación exhaustiva de los solicitantes de la numeración, en donde constate las calidades, condiciones, y demás requisitos que permitan dar tranquilidad del uso que se va a dar al potencial asignatario de la numeración, y no trasladar con posterioridad el problema a los PRSTM quienes se ven obligados a implementar medidas tecnológicas para evitar el envío de mensajes con contenido fraudulento.

Sugiere que si la CRC evidencia que la numeración no está siendo bien utilizada, la consecuencia debe ser la recuperación de los códigos cortos mal utilizados, y no volver a asignar hasta tanto demuestre que implementó medidas que evidencien su buen uso. En concreto, la **CCE** solicita que se implementen procesos más cuidadosos/estrictos frente a los solicitantes de recursos de numeración.

CCIT

Señala que la CRC no habría dado respuesta a una petición reiterada por actores del ecosistema, que es permitir la terminación de contratos de acceso con PCA/IT "abiertamente reincidentes" en el envío de SMS con contenido fraudulento. Explica que la relevancia práctica de esta medida deviene de que, en ausencia de esa posibilidad, cuando se recupera un código corto, el PCA/IT notificado podría continuar la conducta usando otros códigos asignados, con lo que la recuperación del recurso no corta el ciclo de reincidencia. Por ello, pide incorporar expresamente esta herramienta como parte del set regulatorio de control del recurso y de contención de daño al usuario.

Adicionalmente, la **CCIT** enfatiza la responsabilidad de la CRC como autoridad de asignación de numeración corta: pide "procesos más cuidadosos/estrictos" y una evaluación exhaustiva de solicitantes (calidades, condiciones y requisitos), de modo que el riesgo de fraude se reduzca desde la puerta de entrada del recurso. En coherencia con ello, propone que, si se evidencia uso indebido, la consecuencia sea recuperar los códigos cortos mal utilizados y no volver a asignarlos hasta que el potencial asignatario demuestre medidas que evidencien buen uso. El propósito de esta postura es

evitar que fallas de asignación y control ex post se traduzcan en cargas tecnológicas generalizadas sobre PRST, por lo que reitera que, tras evaluar la efectividad de la suspensión o bloqueo provisional, la CRC debería realizar el AIN de las restantes medidas antes de convertirlas en mandatos obligatorios

CLARO

Insiste en que la reincidencia debe tener consecuencias estructurales. Considera indispensable que el régimen incorpore obligaciones y sanciones específicas frente a los asignatarios reincidentes, más allá de la simple recuperación del recurso.

HABLAME

En materia de códigos cortos y su uso para mitigación del fraude, **HABLAME** destaca el papel funcional de los integradores tecnológicos para asegurar interoperabilidad y velocidad del mercado, y plantea que el esquema vigente de códigos cortos debe preservarse. Su preocupación central es que medidas que conduzcan al "retiro total" de un código corto por contenidos asociados a múltiples originadores desconocen la realidad operativa del A2P. En su lugar, **HABLAME** propone focalizar acciones sobre originadores específicos, y que los bloqueos se adopten previa orden judicial o administrativa competente, evitando sanciones amplias que terminen afectando campañas legítimas**.**

En cuanto a la identificación de reincidentes mediante el uso de códigos cortos, la posición de **HABLAME** se alinea con un enfoque de consecuencias selectivas y trazables sobre responsables identificables, más que sobre el recurso en abstracto.

TELEFÓNICA

Considera que la recuperación aislada de códigos cortos es insuficiente frente a la reincidencia. Propone definir criterios objetivos para configurar la reincidencia y habilitar consecuencias estructurales, como la terminación del contrato de acceso y la inhabilitación para recibir nuevos recursos, centrando la sanción en la persona jurídica y no solo en el recurso.

En particular, **TELEFÓNICA** considera que la regulación resultante de este proyecto debe incluir como medida prioritaria, una habilitación expresa y un marco de protección jurídica ("puerto seguro") que faculte a los operadores para realizar bloqueos preventivos inmediatos de tráfico, códigos cortos o numeración internacional ante la detección técnica de patrones anómalos o reportes consistentes de fraude. En concreto, **TELEFÓNICA** la normativa debe permitir actuar con celeridad para detener la conducta lesiva en tiempo real, difiriendo las etapas de revisión de fondo, descargos y eventual reactivación para un momento posterior al bloqueo.

TIGO

Respalda la necesidad de introducir consecuencias claras frente a la reincidencia en el uso indebido de códigos cortos, señalando que la simple recuperación del recurso resulta insuficiente como mecanismo disuasivo. Considera necesario que el régimen incorpore sanciones estructurales que recaigan sobre el asignatario reincidente, y no únicamente sobre el recurso.

Señala que la efectividad de esta medida sería limitada si se orienta únicamente a sancionar o imponer restricciones a la razón social que incurre en el uso indebido, puesto que, en la práctica, ese enfoque

puede ser fácilmente eludible mediante la creación de una nueva personería jurídica, con lo cual se neutraliza el propósito correctivo y preventivo de esta medida. En este sentido, solicita que la medida contemple a los representantes legales, de forma que las consecuencias se activen cuando se evidencie continuidad en la conducta a través de distintas personas jurídicas donde participan los mismos representantes legales que han participado en empresas ya catalogadas como reincidentes.

Respuesta CRC:

Para efectos de dar respuesta a los anteriores comentarios, estos se clasificaron en dos grandes asuntos. Por un lado, las consecuencias de la reincidencia para los PCA/IT y, por el otro, el procedimiento de asignación de códigos cortos vigente.

En relación con lo primero es menester recordar que, en el documento de alternativas regulatorias publicado por la Comisión, de manera expresa la CRC sí respondió el comentario de la **ANDI** sobre reincidencia en los siguientes términos:

> «En relación con la propuesta de **ANDI** de facultar a los PRSTM para terminar contratos con PCA e IT reincidentes en conductas fraudulentas, esta Comisión resalta que el análisis integral de las condiciones que determinan la relación de acceso entre PRSTM y PCA/IT, establecidas en el Capítulo 2 del Título IV de Resolución CRC 5050 de 2016, para el uso de las redes para la prestación de servicios de mensajería corta, así como las obligaciones y responsabilidades de cada una de las partes, si bien excede el alcance planteado para el actual proyecto regulatorio, esto no implica que de los análisis adelantados se pueda concluir la necesidad de establecer consecuencias puntuales ante casos de reincidencia».

Por lo tanto, no es cierto, como lo afirman varios agentes, que la CRC haya omitido los comentarios sobre reincidencia. Si bien en su momento se consideró que la medida contra reincidentes desbordaba el objeto del proyecto, es igualmente cierto que **ANDESCO**, **ANDI**, **CCIT**, **CCE**, **TIGO**, **CLARO**, **TELEFÓNICA**, **ASOBANCARIA** y **ASOMÓVIL** concuerdan en que se deben establecer consecuencias estructurales para los PCA/IT reincidentes. A modo de ejemplo, proponen que se habilite de forma expresa al operador para terminar los contratos suscritos con los PCA/IT reincidentes. En efecto, señalan que la recuperación de un código corto no es suficiente en la práctica, toda vez que el PCA o el IT puede continuar operando con otros códigos cortos asignados, lo que perpetúa el daño al usuario y reduce la eficacia de las medidas. Por esta razón, a juicio de estos agentes, la Comisión debe incluir consecuencias disuasorias en la regulación.

En virtud de la importancia y utilidad de los comentarios frente a este punto de la reincidencia, la CRC considera conveniente proponer e introducir como medida la posibilidad de que los PRST puedan suspender provisionalmente la relación de acceso con los PCA/IT en aquellos casos en que a estos agentes la CRC les haya recuperado por segunda vez un código corto por las causales de uso diferente al de la asignación, de remisión de contenidos en nombre de terceros sin su autorización o de incumplimiento de las normas sobre RNE.

En aquellos casos, los PRST podrán suspender temporalmente –por un mes– dicha relación de acceso en forma unilateral, para lo cual deberán informar tanto a la CRC como a la SIC sobre las medidas adoptadas para minimizar los efectos de tal suspensión en los usuarios. En la misma línea, se propone incluir la posibilidad de que los PRST puedan solicitar a la CRC autorización para la terminación definitiva cuando se recupere por tercera vez un código corto por las causales indicadas a un PCA/IT.

Así, en estos casos, ante una nueva reincidencia –tercera recuperación de código corto por parte de la Comisión–, el PRST con quien dicho PCA/IT tiene una relación de acceso podría iniciar un trámite de desconexión definitiva ante la CRC con el fin de que esta Comisión autorice tal terminación.

La razonabilidad y proporcionalidad de esta medida se halla, en primer lugar, en que con ella se persigue un fin constitucional y regulatoriamente relevante, que no es otro más que garantizar la seguridad de los usuarios y preservar la confianza en los servicios de mensajes cortos de texto (SMS), en un contexto específico de incremento de la criminalidad materializada por medio de este servicio. En efecto, la medida se apoya en un criterio objetivo y verificable –la segunda y tercera recuperación de un código corto por causales asociadas a uso indebido– lo que evita que la actuación del PRST dependa de valoraciones subjetivas sobre el contenido del mensaje.

En este sentido, la desconexión temporal y la terminación definitiva resultan adecuadas para interrumpir la continuidad del riesgo y prevenir que usuarios del PRST reciban contenidos fraudulentos desde agentes que ya han demostrado, en más de una ocasión, incapacidad o falta de controles para asegurar el uso correcto de los códigos.

Aunado a lo anterior, la introducción de la posibilidad de suspensión por parte de los PRST y la posibilidad de autorizar la terminación de la relación de acceso en forma definitiva permitiría cerrar las brechas de eficacia que persisten si únicamente se mantiene como herramienta regulatoria la recuperación del código corto específico.

Ciertamente, la recuperación de un código corto puntual puede llegar a ser insuficiente para contener el fenómeno en cuestión cuando el PCA/IT puede continuar el envío de tráfico riesgoso a través de otros códigos dentro de la misma relación de acceso. Así, en principio, el mes de desconexión provisional operaría como un mecanismo de contención eficaz y, al mismo tiempo, como un incentivo para que el PCA/IT adopte correctivos verificables en sus procesos internos de control, trazabilidad y autorización de campañas.

Finalmente, la posibilidad de dar por terminada la relación de acceso en forma definitiva, previa autorización de la CRC, fortalecería aún más el propósito superior de garantizar la seguridad de los usuarios. Este enfoque contribuye a gestionar el riesgo sin trasladar a los PRST una carga imposible de asumir (como convertirse en árbitros del carácter fraudulento del contenido) y reduce, adicionalmente, la exposición del operador a controversias o acciones litigiosas derivadas de permitir el curso de tráfico evidentemente riesgoso.

De esta forma, la prerrogativa propuesta en cabeza de los PRST se considera proporcional porque, en todo caso, el impacto económico para el PCA/IT tiene un límite claro, como quiera que la suspensión es temporal, solo procede ante reincidencia (no ante hechos aislados) y la consecuencia más intensa, la terminación definitiva, no se activa automáticamente, sino que exige una tercera recuperación y, además, la autorización de la CRC, lo que introduce un control efectivo y, en consecuencia, evita el riesgo de arbitrariedad por parte de los PRST. Así las cosas, la ponderación entre las ventajas y desventajas que implica la medida resulta positiva, pues la posible afectación al negocio de los PCA/IT se justificaría por el propósito superior de prevenir daños a los usuarios y de reforzar la integridad del sistema.

Ahora bien, en línea con la medida planteada, también se propone la inclusión de dos nuevas causales de oposición a ser invocadas por los PRST ante una solicitud de acceso por parte de PCA/IT a quienes

se les haya previamente terminado una relación de acceso con ocasión de la constatada reincidencia en materia de recuperación de códigos cortos. Así, en primer lugar, se incluirá la posibilidad de que todo aquel PRST, en virtud de cuya solicitud se haya autorizado la terminación de una relación de acceso por motivos de reincidencia en la recuperación de códigos cortos, pueda negarse a otorgar el nuevo acceso durante un (1) año a dicho PCA/IT contado a partir de la terminación definitiva autorizada por la CRC. Y, en segundo lugar, se incluirá como causal para oponerse al acceso que el PCA/IT cuya relación de acceso se terminó definitivamente no haya tomado medidas suficientes para prevenir el envío de mensajes de contenido fraudulento por medio de los códigos cortos a él asignados.

Por otra parte, estos mismos actores coinciden en que la CRC debe reforzar o robustecer el proceso de asignación de códigos cortos mediante diferentes medidas ex ante, en procura de que las cargas tecnológicas no se trasladen a los PRST. A su turno, **HABLAME** expone que la medida del retiro de un código corto desconoce la realidad operativa del ecosistema A2P, en el cual un mismo recurso puede ser utilizado por múltiples originadores, y propone un enfoque focalizado orientado a identificar y sancionar originadores específicos, y sugiere que los bloqueos se adopten previa orden judicial o competente para evitar afectaciones indebidas a campañas legitimas.

Al respecto, esta Comisión destaca la utilidad de los comentarios enfocados a reforzar, ajustar o revisar los requisitos o requerimientos para la asignación de recursos de identificación como lo son los códigos cortos. Sobre el particular, y de conformidad con la definición contenida en la Resolución CRC 5050 de 2016, se debe recordar que la asignación de un recurso de identificación es la «Autorización concedida por el administrador de los recursos de identificación a un solicitante para utilizar un determinado recurso de identificación, bajo la observancia de unos propósitos y condiciones especificadas. La asignación de dichos recursos confiere exclusivamente el derecho de uso, pero no otorga derecho de propiedad sobre los mismos, ni tendrá costo alguno para los asignatarios».

Lo anterior implica que si bien la CRC, como administrador de los recursos de identificación, autoriza el uso de los recursos, ello no significa que tal autorización permita el uso indiscriminado o sin límites de los recursos de identificación, motivo por el cual es apenas lógico que dicha autorización pueda ser rescindida por medio de la recuperación del recurso cuando se acredite su uso indebido o, en términos generales, por fuera de lo permitido en la regulación general sobre la materia.

Bajo esta lógica, vale traer a colación el artículo 6.1.1.5. de la Resolución CRC 5050 de 2016, que regula de manera concreta la asignación de los recursos de identificación y, además, el artículo 6.1.1.6. de la misma resolución que dispone las obligaciones regulatorias del Administrador de los Recursos de Identificación y, en adición, de los asignatarios de esos recursos. Así las cosas, la Comisión propone la incorporación de nuevos requerimientos para la asignación y, además, de nuevas obligaciones para los asignatarios, como se expone a continuación:

a. Nuevos requisitos de asignación:

- Según lo dispuesto en el numeral 6.4.2.1.3. del artículo 6.4.2.1 de la Resolución CRC 5050 de 2016 actualmente es requisito para la asignación la «descripción detallada del servicio que se prestará a través del código corto solicitado donde se especifique, como mínimo, lo siguiente: i) La indicación de si se trata de un contenido o aplicación; ii) La descripción del contenido o de aplicación a ofrecer al usuario; iii) El procedimiento de interacción con el usuario».

En tal sentido, se modificará ese numeral para que sea requisito, además de lo anterior, que la descripción específica del contenido o funcionalidad ofrecida al usuario tenga en cuenta la categoría del contenido y las actividades operativas específicas asociadas a la prestación del servicio, lo que deberá incluir la identificación del origen del mensaje y los mecanismos que permiten su trazabilidad a lo largo del flujo de comunicación hasta la notificación al usuario final.

- El solicitante del recurso deberá informar en detalle las medidas de control y herramientas tecnológicas que serán empleadas por parte del PCA y su integrador tecnológico (según aplique) para prevenir fraudes o usos indebidos a través del envío de mensajes SMS o USSD mediante los códigos cortos solicitados, precisando su aplicación según la modalidad correspondiente.

- El solicitante deberá aportar certificado de existencia y representación legal vigente, expedido con no más de noventa (90) días, en el que conste que la matricula legal está vigente. Además, certificado de existencia y representación legal vigente del integrador tecnológico, en caso de aplicar.

b. Nuevas obligaciones:

Dentro del artículo 6.1.1.6. Resolución CRC 5050 de 2016, que consagra las obligaciones del administrador de recursos de identificación y de los asignatarios de esos recursos, se incluirán las siguientes obligaciones:

i) El asignatario de los recursos deberá contar con la autorización de terceros cuando tales recursos sean utilizados para enviar contenido en nombre de esos terceros.

ii) En el evento en que un PCA asignatario pretenda cambiar el integrador tecnológico contratado para el uso de un determinado código corto asignado, deberá informar previamente ante la CRC para efectos de modificar las condiciones iniciales de asignación.

iii) En Los asignatarios que estén obligados a contar con matrícula mercantil en los términos del Código de Comercio deberán mantenerla debidamente actualizada en los términos ordenados por el artículo 33 del Código de Comercio. De no estar actualizada la CRC puede recuperar los códigos cortos que tenga esa sociedad asignada.

En complemento de lo anterior, la Comisión identificó la necesidad de revisar, desde un enfoque de simplificación, las normas sobre RNE y la forma de simplificar algunas de ellas para que la SIC pueda tener acceso a los documentos, pruebas o insumos que reposan en la CRC, en el marco del trámite de recuperación de códigos cortos, con la finalidad de que las competencias de la SIC puedan ejercerse con mayores elementos de juicio en lo que respecta al seguimiento del cumplimiento de las disposiciones relacionadas con el RNE.

Por último, es importante advertir que los comentarios relacionados con la implementación de controles específicos frente a modalidades como el SIM swapping, verificaciones reforzadas en los procesos de cambio de SIM, el uso de autenticación multifactor, biometría o estándares como FIDO2,

así como la generación de alertas preventivas al usuario y la aplicación de bloqueos temporales de originación y la exigencia de procesos de KYC fueron abordadas, respondidas o consideradas en capítulos precedentes de este documento, ya que escapan al ámbito de la simplificación.

8.2.7.2 Cesión/transferencia

CLARO

Expone que debe mantenerse el Statu Quo, dado que la cesión o transferencia de códigos cortos tal como lo propone la CRC, no resulta adecuada en la medida en que termina desvirtuando el objetivo regulatorio de corregir conductas indebidas asociadas al uso de códigos cortos, pues esta figura permite a actores sancionados recuperar indirectamente su capacidad operativa, debilitando el efecto disuasivo del régimen de administración, y generando una ventaja para esos actores frente a quienes si cumplen las reglas, afectando la equidad competitiva y reduciendo la efectividad de los mecanismos de control y sanción definidos por el regulador.

TIGO

El operador se opone a flexibilizar la cesión o transferencia de códigos cortos, al considerar que esta figura puede desvirtuar el objetivo regulatorio y facilitar que actores sancionados recuperen indirectamente su capacidad operativa. En este sentido, propone mantener el statu quo y restringir estas figuras para preservar el efecto disuasivo del régimen. En este sentido, solicita prohibir expresamente dichas prácticas de préstamo o uso por terceros, puesto que el «préstamo» o habilitación informal, sumado a la utilización de un mismo código para múltiples marcas o clientes, termina por diluir la trazabilidad y la atribución de responsabilidades frente al contenido, el origen del tráfico y la atención
de reclamaciones.

TELEFÓNICA

Apoya la imposición de restricciones severas a la cesión o transferencia de recursos de identificación, exigiendo validación bajo los mismos estándares de asignación original (KYC reforzado) y prohibiendo esquemas de subarriendo o reventa que faciliten la elusión regulatoria.

Admiten cesión con condiciones (mantener condiciones iniciales, trazabilidad y restricciones).

SFC

Considera importante preservar una trazabilidad estricta en la asignación de códigos cortos y recursos de numeración, en particular aquellos utilizados para comunicaciones masivas. En ese sentido, insiste en que los procesos de simplificación mantengan exigencias robustas de «Conozca a su Cliente» (KYC) para los agregadores de mensajes, con el fin de evitar que estos recursos sean utilizados por estructuras criminales amparadas en el anonimato.

Respuesta CRC:

CLARO opina que no se debería permitir la cesión o transferencia de los códigos cortos sin controles estrictos y solicita que se mantenga el statu quo. **TIGO** añade que la flexibilización de la figura de la

cesión o transferencia permite que actores a quienes se les han recuperado códigos cortos recuperen indirectamente su capacidad operativa, por lo que solicita prohibir expresamente dichas prácticas de préstamo o uso por terceros. **TELEFÓNICA** apoya la imposición de restricciones severas a la cesión o transferencia bajo los mismos estándares de la asignación inicial, pero adiciona que debería prohibirse el subarriendo o reventa de los códigos cortos. Finalmente, la **SFC** sugiere que se preserve una trazabilidad estricta en la asignación de códigos cortos y recursos de numeración, en particular aquellos utilizados para comunicaciones masivas.

Con base en esos comentarios, como se indicó antes, la Comisión recuerda que el parágrafo del artículo 6.1.1.5 de la Resolución CRC 5050 de 2016 de manera expresa dispone que los recursos de identificación no pueden ser objeto de venta o comercialización y, además, tampoco pueden ser cedidos o transferidos, excepto cuando el Administrador de los Recursos de Identificación lo autorice de manera expresa, de oficio o a solicitud de parte, para lo cual el nuevo asignatario deberá cumplir los requisitos de asignación correspondientes. Finalmente, en el caso de emitirse una autorización expresa de cesión o transferencia de los derechos de uso de los recursos de identificación, el nuevo asignatario adquiere todas las obligaciones sobre los recursos de identificación cedidos o transferidos.

Así, si bien la Comisión considera que la regulación es lo suficientemente clara en el evento de la cesión o transferencia de los recursos de identificación, en cuanto a sus implicaciones y obligaciones, frente a los códigos cortos para SMS y USSD, lo cierto es que con base en los comentarios recibidos por los interesados, y sobre la base de que las reglas en materia de cesión de códigos pueden ser optimizadas para efectos de aumentar la eficacia de la regulación sobre esta materia, se procederá a proponer como medida regulatoria la prohibición de la cesión o transferencia de estos recursos de identificación.

8.2.7.3 Suspensión de tráfico en actuación administrativa

ANDESCO

Pide que la CRC realice un análisis actualizado del impacto de la medida de suspensión provisional, resaltando que fue promovida por PRSTM, que su implementación no requirió modificación regulatoria y que habría reducido de manera significativa los casos escalados a PCA para validación de contenido. Con base en ello, **ANDESCO** plantea que la CRC debe verificar si las medidas adicionales son realmente necesarias o podrían ser redundantes frente a herramientas ya eficaces.

ANDI

Comenta que no se encuentra un análisis actualizado que revise la medida adelantada por la CRC planteada en el numeral 7.4.3 TEMÁTICA 3: Suspensión del tráfico cursado a través de un código corto, en el marco de una actuación administrativa, dentro del documento objeto de estudio. Para la ANDI, esta simple medida, que con tanta insistencia solicitaban los PRSTM, fue aplicada por la CRC sin que fuera necesaria una modificación regulatoria, disminuyó considerablemente los casos escalados a los PCA para validación de contenido de mensajes con contenido presuntamente fraudulento.

Desde esa evidencia operativa, la **ANDI** propone que la CRC analice con detalle los efectos que ya han tenido las herramientas vigentes, particularmente el bloqueo provisional de mensajes de texto asociados a investigaciones por uso indebido, mecanismo que, según los resultados operativos, ha

reducido considerablemente la problemática. Para la **ANDI**, Este dato evidencia que medidas focalizadas, basadas en control de numeración y gestión del recurso, pueden generar impactos contundentes sin necesidad inmediata de imponer cargas tecnológicas adicionales. A su juicio, el AIN permitiría determinar si estas acciones existentes deben consolidarse, ajustarse o complementarse, evitando duplicidad de obligaciones o inversiones innecesarias.

ASOMÓVIL

En relación con la suspensión del tráfico cursado a través de un código corto, ASOMÓVIL considera que la medida prevista por la CRC debe articularse y complementar las disposiciones ya incorporadas en la Resolución CRC 7811 de 2025, de modo que permita una reacción ágil frente al tráfico fraudulento y reduzca afectaciones masivas a los usuarios. A su juicio, la suspensión del tráfico, por sí sola, resulta insuficiente si no se inserta en un esquema más amplio que cierre efectivamente el ciclo del fraude y evite que los infractores continúen operando mediante rotación de numeración, cambio de operador o uso de filiales e intermediarios.

Por ello, además de respaldar mecanismos de bloqueo o suspensión con mayor celeridad, propone fortalecer los controles de asignación de numeración mediante un enfoque preventivo basado en evaluación de riesgo del solicitante, considerando antecedentes de cumplimiento y vínculos relevantes. En esa lógica, la suspensión del tráfico debe operar como una medida complementaria de un sistema más robusto, en el que la reincidencia tenga consecuencias reales sobre la permanencia en el ecosistema y se envíe una señal clara de intolerancia frente al fraude reiterado.

CCE

Sostiene que no se encuentra un análisis actualizado que revise la medida adelantada por la CRC planteada en el numeral 7.4.3 TEMÁTICA 3: Suspensión del tráfico cursado a través de un código corto, en el marco de una actuación administrativa, dentro del documento objeto de estudio, pese a que dicha medida ha demostrado, en la práctica, una reducción significativa de los casos escalados por fraude.

En consecuencia, solicita que la CRC analice con detalle los efectos que ya han tenido las herramientas vigentes, particularmente el bloqueo provisional de mensajes de texto asociados a investigaciones por uso indebido, mecanismo que según los resultados operativos ha reducido considerablemente la problemática. Este dato evidencia que medidas focalizadas, basadas en control de numeración y gestión del recurso, pueden generar impactos contundentes sin necesidad inmediata de imponer cargas tecnológicas adicionales. Todo lo anterior, en opinión de la CCE, con el fin de determinar si las demás medidas propuestas son necesarias.

CCIT

En sus comentarios, la **CCIT** solicita un análisis actualizado sobre la "suspensión del tráfico cursado a través de un código corto, en el marco de una actuación administrativa", indicando que habría sido aplicada por la CRC sin requerir modificación regulatoria y que habría tenido un efecto positivo al reducir considerablemente los casos escalados a los PCA para validación de contenido presuntamente fraudulento. La **CCIT** plantea que medir ese efecto es condición para decidir si las demás medidas propuestas son necesarias o si resultasen redundantes frente a una herramienta ya operativa.

CLARO

Expone que se debe mantener el Stau Quo, dado que la situación actual salvaguarda al usuario y lo pone como centro de la actuación de la CRC. Señala que sin ser una medida regulatoria da alivio a la problemática planteada, lo que a su juicio deja en evidencia que la regulación solo debe imponerse cuando sea necesaria. Adicional que con solo una medida administrativa de la CRC se logró en gran medida dar soluciones a la problemática planteada. Finalmente concluye que esta medida sumada a la posibilidad de terminar contrato con operadores reincidentes da solución en su totalidad a la problemática planteada. Adicionalmente, señala que no es viable que la suspensión de tráfico se imponga en cualquier momento de la actuación administrativa.

TELEFÓNICA

Solicita que se otorgue a los PRST una facultad expresa, con puerto seguro regulatorio, para suspender preventivamente el tráfico asociado a un código corto ante patrones técnicos de fraude, priorizando la protección del usuario y garantizando el debido proceso de forma posterior.

TIGO

Destaca como uno de los principales aciertos regulatorios recientes la suspensión provisional del tráfico de códigos cortos al inicio de la actuación administrativa, medida que, según su experiencia operativa, ha generado reducciones significativas en los reportes de fraude.

En consecuencia, considera que esta herramienta debe mantenerse y consolidarse, y que la regulación solo debe imponerse cuando sea estrictamente necesaria, evitando duplicidades o cargas adicionales injustificadas.

Solicita que la medida también deberá contemplar la posibilidad de suspender temporalmente el tráfico si se detecta un presunto uso ineficiente de un recurso de identificación asignado. Recomienda que, para robustecer su eficacia frente al fraude, se incorpore de forma expresa una causal de recuperación del recurso de identificación asociada a actividades fraudulentas cuando existan presuntos indicios de uso indebido del recurso soportados en las quejas o reportes allegados a la Comisión.

Además, solicita que la suspensión temporal del tráfico asociado al código corto vinculado en la actuación administrativa sea obligatoria y exigible para todos los actores de la cadena, desde el PCA, su Integrador Tecnológico en caso de tenerlo, y demás intermediarios que participen en el encaminamiento del tráfico, hasta el PRST, de manera que se eviten vacíos de implementación o interpretaciones fragmentadas que permitan que el tráfico continúe cursándose por algún eslabón.

De igual forma, señala que para que esta medida sea efectiva, es necesario que la CRC establezca un tiempo máximo de atención a la denuncia o reporte hecho ante un posible fraude que no supere las 24 horas para el acto de apertura de la actuación administrativa que permita realizar la suspensión del código corto y del tráfico que está cursando por dicho código, de forma preventiva hasta tanto se resuelva por completo la misma.

Respuesta CRC:

ANDESCO, CCIT, CCE y la **ANDI** solicitan a la CRC que realice un análisis del impacto de la medida de suspensión provisional ya que, a su juicio, no requirió de modificación regulatoria y habría reducido de manera significativa los casos escalados a PCA para validación de contenido fraudulento. Esto con la intención de evaluar si las medidas adicionales son necesarias. Por su parte, **ASOMÓVIL**, **CLARO** y **TIGO** sostienen que la medida de suspensión del tráfico de códigos cortos al inicio de la actuación administrativa ha sido altamente efectiva para reducir el fraude, por lo que debería consolidarse y complementarse con facultades adicionales.

Bajo este contexto, y en relación con los comentarios de **ANDESCO**, **CCIT**, **CCE**, **ANDI**, **ASOMÓVIL**, **CLARO** y **TIGO**, es importante recordar que el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016 regula el procedimiento de recuperación de los recursos de identificación. Esta disposición fue modificada de manera expresa por el artículo 94 de la Resolución CRC 7811 de 2025 al incluir el Parágrafo 3°. Según esta disposición, en las actuaciones administrativas de recuperación de códigos cortos iniciadas por las causales señaladas en los numerales 6.4.3.2.2., 6.4.3.2.8. y 6.4.3.2.9. del artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, la CRC puede ordenar, en el acto de apertura de la actuación administrativa, la suspensión temporal del uso del recurso de identificación. Dicha suspensión se mantendrá durante el trámite administrativo y no podrá exceder un plazo máximo de seis (6) meses. Por lo tanto, queda claro que la facultad que hoy en día ejerce la CRC en el marco de los trámites administrativos descritos está expresamente consignada en el artículo mencionado.

Una vez realizada esta precisión, la CRC concuerda con **ANDESCO**, **CCIT**, **CCE**, **ANDI**, **ASOMÓVIL**, **CLARO** y **TIGO** en el sentido de afirmar que la medida de suspensión provisional ha sido efectiva y que, además, debe ser robustecida y/o complementada. Por lo tanto, se propone incluir en las respectivas medidas de simplificación propuestas que la prerrogativa de suspensión provisional podrá ser ordenada no solo al inicio de las actuaciones de recuperación sino en cualquier etapa del trámite siempre y cuanto se trate de la recuperación de códigos cortos iniciadas por las causales señaladas en los numerales 6.4.3.2.2., 6.4.3.2.8. y 6.4.3.2.9. del artículo 6.4.3.2. de la Resolución CRC 5050 de 2016.

A su turno, **TELEFÓNICA** solicita que se otorgue a los PRST una facultad expresa para suspender preventivamente el tráfico asociado a un código corto ante patrones técnicos de fraude. Frente al comentario de **TELEFÓNICA** es menester indicar que la facultad de suspensión preventiva o provisional del tráfico por parte del PRST, en el marco del contrato con los respectivos PCA/IT, ya fue abordada en la respuesta a los comentarios sobre la temática de reincidencia de este capítulo.

Ahora bien, en atención al comentario de **INALAMBRIA** en el que propone la focalización para no afectar el tráfico legitimo masivo, procede afirmar que la medida propuesta por la CRC en este capítulo, según la cual la facultad de la Comisión para suspender provisionalmente el tráfico en cualquier estado de la actuación administrativa y, en particular, delimitado a unas causales precisas, ya estaría focalizando los efectos de la medida que eventualmente se adopte en los trámites administrativos de recuperación de recursos de identificación.

Para finalizar, y producto de todos los comentarios descritos, la Comisión considera relevante complementar las medidas hasta ahora propuestas en el sentido de modificar el trámite administrativo de recuperación de los recursos de identificación regulado en el artículo 6.1.1.8. de la Resolución CRC de 2016, no solo en relación con la facultad de la Comisión de decretar la suspensión del tráfico, sino también para efectos de introducir en el inicio del trámite una publicación del acto administrativo de

inicio durante un plazo particular para efectos de promover y garantizar la participación de cualquier tercero interesado, en los términos de los artículos 37 y 38 del CPACA.

Esto garantizaría, de manera efectiva, que cualquier interesado se vincule a los trámites administrativos de recuperación de recursos de identificación para los fines que correspondan, especialmente para aportar y solicitar pruebas. Lo anterior garantizará un mayor nivel de transparencia y, además, le permitirá a la Comisión contar con elementos de juicio adicionales para adoptar decisiones.

8.2.7.4 Vigencia y actualización

CLARO

Considera que imponer nuevas obligaciones periódicas de actualización de información a los asignatarios contraviene el principio de simplificación regulatoria. A su juicio, corresponde a la CRC identificar de oficio las inconsistencias y proceder con la recuperación del recurso cuando sea necesario, sin trasladar obligaciones a los actores cumplidos.

INALAMBRIA

Favorecen causal de recuperación por no actualización RPCAI/RUES y suspensión preventiva por incumplimiento de actualización.

TELEFÓNICA

Considera esencial la obligación de mantener actualizada la información del asignatario y propone que la falta de actualización o imposibilidad de contacto sea causal autónoma de recuperación inmediata del recurso, depurando asignaciones inactivas o «zombis».

TIGO

Considera indispensable que la renovación esté acompañada de una verificación del nivel de utilización efectiva del recurso, dado que en algunos casos se ha identificado que se cursa un volumen mínimo de mensajes únicamente para evitar la pérdida del recurso. Por ello, resulta pertinente que el proceso de renovación incluya criterios objetivos de utilización (por ejemplo, umbrales mínimos sostenidos, consistencia del tráfico, evidencia de la marca asociada y del modelo de operación), de manera que la
asignación se mantenga únicamente cuando exista un uso real, verificable y acorde con la finalidad del código corto.

Respuesta CRC:

INALAMBRIA y **TELEFÓNICA** coinciden en que los asignatarios deben tener obligaciones claras de actualización de su información Registro de Proveedores de Contenidos y Aplicaciones e Integradores tecnológicos (RPCAI) y la matrícula mercantil en el Registro Único Empresarial y Social (RUES) administrado por la Cámara de Comercio, así como una consecuencia por no cumplir con ese mandato, como puede ser la recuperación del código corto. Por su parte, **CLARO** considera que corresponde a la CRC identificar las inconsistencias o desactualizaciones y, en esa medida, proceder a recuperar el

código corto cuando corresponda. Para **TIGO** es fundamental que la renovación esté acompañada de una verificación del nivel de utilización efectiva del recurso, dado que en algunos casos se ha identificado que se cursa un volumen mínimo de mensajes únicamente para evitar la pérdida del recurso.

Con base en estos comentarios, para la Comisión es importante recordar que el artículo 6.4.3.2. de la Resolución CRC 5050 de 2016 contempla las causales de recuperación de la numeración de códigos cortos para SMS y USSD. En particular, el numeral 6.4.3.2.1. del mencionado artículo dispone como una de las causales el que un asignatario incumpla alguna de las obligaciones generales definidas en el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la Resolución CRC 5050 de 2016. Con ese contexto claro, como se indicó anteriormente en este documento, se propone incluir nuevas obligaciones para los asignatarios de los recursos de identificación, entre ellas, la obligación de mantener actualizados dichos registros. Por lo tanto, el incumplimiento de esa obligación específica se convertiría, al mismo tiempo, en una causal de recuperación. Además de lo anterior, los asignatarios que estén obligados a contar con matrícula mercantil en los términos del Código de Comercio deberán mantenerla debidamente actualizada en los términos ordenados por el artículo 33 del Código de Comercio. Así, de no estar actualizada la CRC puede recuperar los códigos cortos que tenga esa sociedad asignada.

Ahora bien, producto de los comentarios analizados en esta sección, la Comisión considera relevante complementar las medidas planteadas en el sentido de:

- Incluir una nueva causal de recuperación de la numeración de códigos cortos para SMS y USSD, en el evento en el que el asignatario se encuentre en la imposibilidad de continuar ejerciendo su objeto social, por ejemplo, cuando entra en estado de liquidación judicial o voluntaria.

- Modificar el numeral 6.4.3.1.3. del artículo 6.4.3.1. de la Resolución CRC 5050 de 2016, para que disponga que los códigos cortos implementados no deberán reportar ausencia de tráfico en periodos consecutivos iguales o superiores a seis (6) meses y no a doce (12) meses, ya que el plazo actualmente no es óptimo para efectos de la evaluación de la utilización eficiente del recurso de identificación correspondiente. Bajo ese mismo sentido, se modificaría la causal de recuperación establecida en el numeral 6.4.3.2.4. del artículo 6.4.3.2. en relación con el periodo referenciado.

Respuesta a las preguntas de la consulta frente a las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

Los interesados respondieron una serie de preguntas formuladas por la Comisión en la consulta pública en relación con esta temática asociada al Régimen de Administración de Recursos de Identificación. Si bien la Comisión resalta la importancia y utilidad de esas respuestas, lo cierto es que la gran mayoría de las respuestas se subsumen en las reflexiones que ya fueron expuestas por la CRC en líneas precedentes en este mismo numeral 8.2.7**.** Por lo tanto, a continuación, se resumirán las respuestas recibidas, pero la Comisión únicamente se pronunciará respecto de aquellas que planteen elementos nuevos o diferentes que no hayan sido previamente abordados.

Reincidencia en el uso indebido de recursos de identificación para el envío de SMS.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Desde la perspectiva de prevención de contactos fraudulentos a los usuarios, ¿qué elementos del régimen de administración de recursos de identificación para el envío de SMS deberían ser revisados o simplificados para prevenir su uso indebido? Explique detalladamente las razones que justifican dicha revisión.

CLARO

Señala como elementos clave de la administración mecanismos de suspensión preventiva ante indicios de fraude, terminación de contratos por reincidencia, mayor diligencia y la validación de los asignatarios de la numeración.

TELEFÓNICA

El operador presentó una respuesta consolidada a todas las preguntas relacionadas con la temática del régimen de administración de recursos de identificación, bajo el enfoque de simplificación.

En primer lugar, **TELEFÓNICA** dice que respalda la adopción de medidas más estrictas para controlar el acceso y uso de los códigos cortos, identificando la reincidencia como el punto crítico a resolver. Opina que es indispensable que la regulación defina criterios objetivos y taxativos para configurar la "reincidencia" (por ejemplo, la comisión reiterada de conductas fraudulentas en un periodo determinado), y que dicha calificación habilite consecuencias contundentes, como la terminación unilateral del contrato de acceso o interconexión y la "muerte comercial" del asignatario para acceder a nuevos recursos de numeración. En su sentir, la simple recuperación del código es insuficiente, pues el actor infractor migra a otro recurso o utiliza un tercero para continuar la práctica.

Frente a la figura de la suspensión preventiva del tráfico, **TELEFÓNICA** solicita que se otorgue a los operadores una facultad expresa y un "puerto seguro" regulatorio que les permita bloquear de manera inmediata el tráfico de un código corto ante la detección técnica de patrones anómalos o reportes de fraude consistentes, sin necesidad de agotar un proceso administrativo previo ante la CRC. Añade que la protección del usuario requiere acción en tiempo real, puesto que esperar a la apertura formal de una investigación por parte del regulador otorga una ventaja temporal inaceptable a los defraudadores. En su opinión, esta suspensión debe estar acompañada de un protocolo de notificación ágil al asignatario para garantizar su derecho de defensa a posteriori, pero priorizando siempre el cese de la afectación al usuario.

En lo que respecta a la cesión o transferencia de recursos, **TELEFÓNICA** apoya la imposición de restricciones severas, ya que el mercado secundario de códigos cortos sin control ha facilitado que recursos asignados legítimamente terminen en manos de actores no verificados. En concreto, propone que toda cesión deba ser notificada y validada nuevamente bajo los mismos estándares de asignación original (KYC reforzado), prohibiendo expresamente el subarriendo o reventa de capacidad de envío a terceros no identificados.

Para terminar, y en relación con la actualización de la información en el registro, **TELEFÓNICA** opina que es una obligación esencial del asignatario mantener sus datos de contacto y uso vigentes. Propone que la falta de actualización o la imposibilidad de contactar al responsable del código sea causal suficiente y autónoma para la recuperación inmediata del recurso por parte de la CRC, saneando así la base de datos de asignaciones "zombis" que suelen ser instrumentalizadas para el fraude. A su juicio, cualquier medida adicional de simplificación normativa debe tener como límite la trazabilidad,

ya que no se debe simplificar requisitos de entrada si ello implica perder la capacidad de identificar quién está detrás de cada mensaje que llega a los colombianos.

TIGO

Propone revisar el régimen de administración de recursos de identificación para fortalecer la trazabilidad y prevenir su uso indebido, estableciendo la asignación de un único código corto o numeración E.164 por marca y prohibiendo expresamente su préstamo o uso por terceros. Sugiere definir obligaciones de acceso y responsabilidades tanto para PCA como para IT en su calidad de asignatarios, incorporar controles específicos de prevención de fraude, tales como firewalls, medidas de conocimiento del cliente (KYC) y bloqueo de tráfico sospechoso, y establecer consecuencias claras frente a la reincidencia, aplicables tanto a las personas jurídicas como a sus representantes legales.

RESPUESTA CRC:

TIGO propone que, en el marco del régimen de administración de recursos de identificación, se establezca que la asignación del código corto debe estar atado a una marca en particular y que se prohíba de manera expresa su préstamo o uso por terceros. Al respecto, en las medidas precisadas en líneas precedentes, en esta misma sección 8.2.7, la Comisión ya abordó la posibilidad de incluir en la regulación requisitos adicionales para la asignación de los recursos de identificación, así como obligaciones complementarias y adicionales para los asignatarios.

Además, también se propuso la posibilidad de prohibir la cesión del código corto. En complemento de lo anterior, la Comisión también precisó que hoy en día no está permitida la cesión o transferencia de un código corto sin la aprobación previa de la CRC. Sobre esa base, es importante también subrayar que en la sección 8.2.6 se propuso la posibilidad de crear un micrositio en el que se hará público, según las particularidades allí expuestas, los códigos cortos y las marcas asociadas a ellos. Por lo tanto, y en caso de que la regulación que expida la CRC contemple las medidas descritas, la Comisión considera que las ideas propuestas por **TIGO** no son necesarias, sin perjuicio de lo cual la CRC las tendrá en el radar para la eventual definición y complementación de las alternativas escogidas.

- En relación con la detección de uso indebido del recurso de identificación, ¿qué criterios adicionales a los expuestos considera necesarios para determinar que un asignatario está haciendo un uso indebido del recurso de identificación? Describa y fundamente cada criterio propuesto.

CLARO

Propone como criterios adicionales, los siguientes indicadores de uso indebido del recuso de identificación:

- Recurrencia de patrones de tráfico atípicos (altas tasas de envío, horarios inusuales o remitentes no declarados), que sugieren intención de ocultar campañas irregulares;

- Incumplimiento reiterado de solicitudes de información o de requerimientos de trazabilidad, que afecta la capacidad de supervisión y utilización del código por terceros no autorizados, lo que demuestra falta de controles internos del asignatario.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

• Concentración de mensajes hacia rangos internacionales inusuales o números aleatorios y así evitar smishing.

TIGO

Propone criterios adicionales para identificar el uso indebido de recursos de identificación, entre ellos: la desviación del propósito autorizado del código corto; la asociación recurrente con PQR o denuncias por fraude; el uso de códigos o numeración no asignados directamente por la CRC; la ausencia de mecanismos de control, trazabilidad y gestión de incidentes por parte del asignatario; la reasignación o cesión no autorizada del recurso a terceros; y la retención de múltiples códigos con tráfico mínimo para evitar su pérdida sin que exista un uso legítimo. Señala que estos criterios se fundamentan en la necesidad de preservar la trazabilidad, la responsabilidad del asignatario y el uso eficiente de los recursos de identificación.

RESPUESTA CRC:

La CRC considera que los criterios expuestos por **TIGO** y **CLARO**, para efectos de detectar el uso indebido del recurso de identificación, son insumos técnicos útiles que serán tenidos en cuenta por la Comisión, ya sea para incorporarlos eventualmente en la regulación o, en su defecto, para acogerlos como criterios internos de verificación en el marco del trámite administrativo correspondiente de recuperación de códigos cortos, previo a la expedición del acto administrativo que corresponda.

- Respecto a las medidas correctivas, ¿qué restricciones adicionales a las previstas actualmente, considera pertinente aplicar a los asignatarios que incurren en uso indebido del recurso de identificación para SMS? Explique en detalle las razones de cada restricción sugerida.

CLARO

Expone que, la CRC, como entidad encargada de asignar la numeración corta, debería realizar una evaluación exhaustiva de los solicitantes para asegurar el uso adecuado de estos códigos y evitar trasladar posteriormente a los PRSTM la carga de implementar medidas tecnológicas para prevenir mensajes fraudulentos. Asimismo, si se evidencia un uso indebido reiterado por parte de PCA/IT, plantea la necesidad de permitir la terminación de los acuerdos de acceso con infractores reincidentes, dado que una asignación adecuada desde el inicio reduciría a su juicio significativamente estos problemas.

TIGO

Propone que, en un esquema de código corto único por marca, se faculte a los PRST para suspender temporalmente el tráfico asociado al recurso de identificación involucrado en presuntas campañas fraudulentas, mientras se verifica con el agregador el contenido y origen de la comunicación. Asimismo, sugiere que, en casos de reincidencia en conductas fraudulentas, se impongan restricciones más severas, como la inhabilidad de la personería jurídica y de sus representantes legales para acceder a nuevos recursos de identificación, con el fin de reforzar el efecto disuasivo y prevenir la reutilización indebida del sistema.

- Con base en su experiencia, ¿cuáles de las medidas actualmente contempladas en la regulación sobre la recuperación de códigos cortos considera efectivas y cuáles no? Por favor sustente su respuesta indicando, cuando sea posible, ejemplos o casos que respalden su argumento.

CLARO

Considera que existe una falta de criterios claros para la reincidencia y actualmente no se aplican sanciones progresivas, lo que permite que algunos actores continúen incurriendo en conductas indebidas sin consecuencias significativas e incluso accedan a nuevos códigos. Expone que, ante el aumento de los fraudes, la CRC debería implementar mecanismos que permitan tramitar y responder en tiempos más cortos para evitar mayores afectaciones a los usuarios, así como mantener actualizada la plataforma del SIGRI y la publicación de resoluciones, con el fin de facilitar la consulta y validación de los recursos de numeración asignados y recuperados.

TIGO

Señala que algunos criterios actuales para la recuperación de códigos cortos presentan limitaciones en su efectividad. En particular, señala que el requisito de tráfico mínimo durante doce meses ha permitido que empresas mantengan múltiples códigos con volúmenes marginales de mensajes solo para evitar su pérdida, lo que evidencia un uso ineficiente del recurso. Asimismo, considera que el criterio de tráfico para un único usuario por más de tres meses perdería pertinencia en un esquema de código corto único por marca. Indica que, frente a las causales de recuperación, se considera poco efectiva la relacionada con el uso distinto al autorizado, debido a la ausencia de mecanismos de supervisión y auditoría preventiva sobre PCA e IT, lo que incrementa el riesgo de usos indebidos.

Asimismo, manifiesta que la principal restricción opera cuando la CRC no permite la terminación de los contratos o acuerdos de acceso por esta causal.

Cesión o transferencia de recursos

- En relación con la cesión o transferencia de recursos de identificación, ¿considera que deberían mantenerse las condiciones iniciales de asignación cuando un recurso de identificación sea cedido o transferido? Por favor, explique las razones que fundamentan su respuesta.

CLARO

Expone que la cesión o transferencia de recursos de identificación no resulta adecuada porque desvirtúa el objetivo regulatorio de corregir conductas indebidas en el uso de códigos cortos. Sostiene que permitirla facilitaría que PCA o IT que perdieron estos recursos por incumplimientos los recuperen indirectamente a través de otros actores, manteniendo en la práctica su capacidad operativa. esto debilita el efecto disuasivo de la medida, genera ventajas injustificadas frente a quienes cumplen las reglas y reduce la efectividad de los mecanismos de control y sanción del regulador.

TIGO

Considera que las condiciones iniciales de asignación de los recursos de identificación deben mantenerse en casos de cesión o transferencia, dado que forman parte del acto administrativo que

define el alcance y finalidad del recurso, garantizando estabilidad jurídica y evitando usos indebidos. No obstante, indica que la autoridad competente debe verificar que el nuevo titular cumpla los requisitos técnicos, operativos y jurídicos exigidos, y podrá ajustar excepcionalmente dichas condiciones cuando existan cambios normativos, tecnológicos o de interés público, respetando los principios de legalidad, proporcionalidad y seguridad jurídica.

- Para autorizar la cesión de un código corto, ¿qué tipo de documentación, validación previa o requisitos formales adicionales deberían exigirse a la persona jurídica que recibirá el código corto? Detalle y explique cada elemento propuesto.

CLARO

Sostiene que no es pertinente la cesión de códigos cortos.

TIGO

Señala que adicional a los elementos exigidos en el artículo 6.4.2.2 «Procedimiento de asignación de la numeración de códigos cortos para SMS y USSD» es importante validar que el cesionario, tanto la persona jurídica como el representante legal, en el momento de la solicitud de la cesión del código corto no estén involucrados en una investigación administrativa que aún no haya concluido; de ser el caso no se le debería permitir el trámite de cesión del código corto.

- Con base en su experiencia, ¿considera que para códigos cortos debería prohibirse la cesión de estos recursos? ¿Qué aspectos considera que la regulación debe priorizar para mitigar estos riesgos? Justifique su respuesta.

CLARO

Afirma que debería prohibirse la cesión de códigos corto, dado que a su juicio la cesión aumenta el riesgo de uso indebido y dificulta la trazabilidad del responsable, lo que facilita fraudes.

TIGO

Considera que la problemática no se origina en la cesión formal de códigos cortos, sino en prácticas informales de préstamo o habilitación de su uso por terceros sin registro ni cambio de titularidad, lo que diluye la trazabilidad y dificulta la asignación de responsabilidades. Por ello, propone prohibir expresamente el uso de códigos cortos y numeración asociada por parte de terceros distintos al asignatario, exigiendo que cualquier cesión se realice conforme al procedimiento formal definido por la CRC y con el cumplimiento de los requisitos correspondientes.

- Respecto a la cesión o transferencia de recursos de identificación, ¿considera que la CRC debe imponer condiciones para mantener la asignación de un código corto, tal como validar el estado o vigencia de la matrícula mercantil de la razón social que solicita un código corto? Por favor, sustente su respuesta.

CLARO

Considera que no se deben imponer condiciones para mantener la asignación del código corto, más allá del cumplimiento de su debido uso.

TIGO

Considera que la CRC puede imponer condiciones para mantener la asignación de códigos cortos en casos de cesión o transferencia, siempre que estén orientadas a verificar la capacidad jurídica del solicitante y la correcta administración del recurso. Entre estas, estima razonable validar la vigencia de la matrícula mercantil para confirmar la existencia legal y responsabilidad del cesionario. Asimismo, sugiere exigir la verificación de la representación legal, la aceptación formal de las condiciones regulatorias, la coherencia entre el objeto social y el uso previsto del código, la revisión de antecedentes por uso indebido del recurso y la obligación de informar si el código será utilizado por terceros, como integradores tecnológicos.

Suspensión preventiva del tráfico

- En relación con la suspensión preventiva del tráfico asociado a un código corto, ¿qué condiciones o supuestos deberían considerarse para habilitar la aplicación de esta medida durante el desarrollo o inicio de la actuación administrativa para la eventual recuperación del recurso? Por favor, explique su respuesta.

CLARO

Sostiene que una medida operativa, aplicada sin necesidad de modificación regulatoria, tal como la suspensión provisional de tráfico logró reducir significativamente el fraude. No obstante, señala que aún falta analizar la viabilidad de terminar contratos entre PCA y PRSTM cuando exista recuperación reiterada de códigos cortos por uso indebido.

TIGO

Propone incorporar como causal expresa de recuperación del recurso la existencia de indicios de actividades fraudulentas sustentados en quejas o reportes presentados ante la Comisión. Asimismo, sugiere que la suspensión preventiva del tráfico asociado al código corto sea obligatoria para todos los actores de la cadena de provisión, desde los PCA e intermediarios hasta los PRST, evitando vacíos en su aplicación. Adicionalmente, se recomienda establecer un plazo máximo, no superior a tres días hábiles, para atender denuncias, iniciar la actuación administrativa y efectuar la suspensión del código y del tráfico asociado.

- Desde su experiencia, ¿cuáles serían los principales beneficios de aplicar una suspensión preventiva del tráfico en casos de presunto uso indebido vinculados a un código corto? Explique sus razones.

CLARO

Sostiene que son múltiples los beneficios de suspender provisionalmente el tráfico en caso de presunto indebido uso, siendo el más importante que los usuarios no van a volver a recibir mensajes con contenido presuntamente fraudulento. Así mismo, la CRC va a iniciar una actuación administrativa y

va a poder recuperar el código corto, el cual a futuro podrá ser asignado nuevamente a un PCA o IT que cumpla con los requisitos regulatorios sobre SMS.

TIGO

Considera que la suspensión preventiva del tráfico asociado a códigos cortos con indicios de uso indebido permite mitigar de forma inmediata posibles daños a los usuarios, evitando la continuidad de comunicaciones fraudulentas mientras se realizan las verificaciones correspondientes. Adicionalmente, constituye una herramienta eficaz para contener riesgos reputacionales y preservar la confianza en los servicios de mensajería y en el ecosistema de telecomunicaciones. Agrega que, al tratarse de una medida temporal y focalizada, basada en criterios objetivos, se entiende como un mecanismo de gestión del riesgo que no implica prejuzgamiento y que es compatible con el debido proceso.

- En cuanto a los posibles impactos, ¿qué riesgos, limitaciones o efectos no deseados podrían derivarse de la aplicación de una suspensión preventiva del tráfico durante el desarrollo o inicio de la actuación administrativa? Detalle y explique los elementos que considere relevantes.

CLARO

Expone que el usuario debe ser el enfoque de la regulación, en este sentido, sostiene que se encuentra acertada la medida de la CRC de suspender provisionalmente el uso del código corto al inicio de una actuación administrativa.

TIGO

Advierte que la suspensión preventiva del tráfico puede generar riesgos si no se aplican criterios objetivos y claramente definidos, por lo que debe sustentarse en evidencias verificables de uso indebido del recurso, como el empleo del código corto para fines distintos a los autorizados. Asimismo, señala la necesidad de que la CRC precise la duración de la suspensión y los plazos para iniciar la actuación administrativa correspondiente, con el fin de evitar afectaciones indebidas y garantizar seguridad jurídica en su aplicación.

- Sobre las garantías del debido proceso, ¿qué elementos considera adicionales para establecer la medida de suspensión del tráfico durante el desarrollo o inicio de la actuación administrativa en casos de presunto uso indebido del código corto? Describa y explique los pasos que considere adecuados.

CLARO

Señala que como mínimo se debe contar con una notificación previa al presunto infractor sobre la medida y sus motivos.

TIGO

Propone que la medida de suspensión preventiva incorpore garantías claras de debido proceso, estableciendo de forma expresa las circunstancias objetivas que la habilitan, como volúmenes atípicos de PQR, evidencia técnica de suplantación o reincidencia en conductas fraudulentas. Recomienda que

la suspensión se formalice mediante acto administrativo motivado que precise hechos, fundamentos técnicos y jurídicos, alcance, duración y condiciones para su levantamiento. Finalmente, destaca la necesidad de un marco operativo claro que permita a los PRST ejecutar la medida con agilidad sin afectar las garantías procesales.

Actualización y trazabilidad de información

- Sobre la actualización de información, ¿considera que debe incluirse como causal de recuperación de los recursos asignados el incumplimiento en la actualización de los datos en las bases de la CRC, como el RPCAI, conforme al Registro Único Empresarial y Social (RUES) de la sociedad asignataria? Por favor, justifique su respuesta.

CLARO

Sostiene que la mejor medida a imponer es la suspensión provisional, sumada a la posibilidad de bloquear por identificar mensajes con contenido presuntamente fraudulentos, cuando los sistemas de alerta evidencien de un posible fraude, y la autorización de parte de la CRC de terminar contratos con PCA/IT reincidentes en la recuperación de códigos cortos por indebido uso – uso fraudulento.

TIGO

Considera pertinente incluir como causal de recuperación de recursos de identificación el incumplimiento en la actualización de datos en las bases de la CRC conforme a la información del RUES, dado que esta medida fortalece la legitimidad, trazabilidad y responsabilidad del asignatario. La actualización permanente de la información permite verificar la existencia jurídica, representación legal y capacidad operativa del titular del recurso, facilitando las funciones de control y supervisión. Por el contrario, la desactualización de datos debilita la exigibilidad de responsabilidades y puede propiciar escenarios de uso indebido o intermediación irregular.

- ¿Considera que la CRC debería incorporar una causal específica de recuperación de códigos cortos que permita suspender de manera preventiva la autorización de uso cuando el asignatario no actualice la información conforme con el Registro Único Empresarial Social (RUES)? Por favor, justifique su respuesta.

CLARO

Afirma de forma categórica que, si el PCA/IT asignatario de numeración no ha actualizado su RUES, si se puede impedir la asignación de nuevos códigos cortos; y que, esta actualización se debe evidenciar al momento de la solicitud.

TIGO

Considera pertinente que la CRC incorpore como causal de recuperación la suspensión preventiva del uso de códigos cortos cuando el asignatario no mantenga actualizada su información conforme al RUES, dado que esta medida refuerza la legitimidad y trazabilidad del titular del recurso. La desactualización dificulta la identificación de responsables, limita la capacidad de reacción ante abusos y aumenta el riesgo de usos indebidos por terceros. Por ello, la suspensión preventiva se entiende

como un mecanismo razonable de gestión del riesgo orientado a la protección de usuarios y del ecosistema de mensajería, más que como una medida sancionatoria.

- ¿Considera que la CRC debería establecer alguna medida regulatoria adicional en los eventos en los que exista conducta reincidente ante el uso indebido de códigos cortos? Por favor, justifique su respuesta.

CLARO

Señala que la CRC debería permitir la terminación de los acuerdos o contratos con PCA o IT reincidentes. Expone que esta medida sumada con la suspensión temporal del uso de códigos cortos en casos de reincidencia soluciona de raíz la problemática presentada.

TIGO

Considera que la CRC debe adoptar medidas regulatorias adicionales frente a conductas reincidentes en el uso indebido de códigos cortos, dado que estas evidencian incumplimientos sistemáticos y deficiencias en la gestión del recurso. En este sentido, propone como medida proporcional la inhabilitación temporal del representante legal responsable para solicitar nuevos códigos cortos, con un carácter preventivo y disuasivo que incentive una administración responsable del recurso. Según su criterio esta medida permitiría focalizar la responsabilidad en el actor directamente involucrado, evitando afectar de manera desproporcionada las operaciones legítimas de la empresa.

RESPUESTA CRC:

TIGO propone como medida proporcional la inhabilitación temporal del representante legal responsable para solicitar nuevos códigos cortos, con un carácter preventivo y disuasivo que incentive una administración responsable del recurso. Al respecto, la Comisión considera que esa medida no tendría un efecto práctico y eficaz en contra de la lucha contra el fraude, toda vez que la sociedad de la cual esa persona es representante legal tendría la posibilidad de actuar por vía de otro representante legal o simplemente reemplazarlo. Por lo tanto, una medida como la propuesta no será acogida por la Comisión.

- ¿Qué consecuencias regulatorias adicionales considera adecuadas en caso de que los asignatarios no actualicen su información según lo estipulado? Por favor, justifique su respuesta.

CLARO

Señala que la propuesta regulatoria no resuelve de manera efectiva la problemática identificada y, por el contrario, impone una carga administrativa y operativa significativa a los asignatarios de numeración. Sostiene que la medida más eficaz consiste en la suspensión provisional de los códigos cortos cuando se evidencie su uso presuntamente fraudulento, complementada con la facultad de bloquear mensajes que los sistemas de alerta identifiquen como potencialmente fraudulentos. Asimismo, resalta como necesario que la CRC autorice la terminación de contratos con aquellos PCA o IT que reincidan en el uso indebido de la numeración y en la recuperación reiterada de códigos cortos por prácticas fraudulentas.

TIGO

Considera pertinente que la CRC incorpore una causal específica de recuperación de códigos cortos que permita suspender de manera preventiva la autorización de uso cuando el asignatario no mantenga actualizada su información conforme al Registro Único Empresarial y Social (RUES). Esta medida fortalece la legitimidad y trazabilidad del titular del recurso, elementos esenciales para la gestión operativa y la prevención de usos indebidos asociados a fraudes a través de mensajes de texto.

8.3. Comentarios del sector a las alternativas sobre remuneración de mensajes cortos de texto en comunicaciones A2P

En el marco del proyecto «Esquemas de Remuneración Mayorista de Redes Móviles» se recibieron diversos comentarios relacionados con la propuesta de actualización de los cargos de terminación de SMS, en particular frente a sus posibles implicaciones en materia de competencia, sostenibilidad del servicio y riesgos asociados al fraude cibernético. No obstante, tras su revisión, la CRC identificó que una parte significativa de estos comentarios se encontraban directamente relacionados con aspectos que trascendían la definición de cargos mayoristas y que estaban asociados a la necesidad de establecer medidas integrales para la mitigación del fraude cibernético a través de servicios de mensajería.

En este contexto, y considerando que dichos aspectos son objeto de análisis específico en el presente proyecto regulatorio, orientado a la identificación de medidas para mitigar el fraude cibernético por medio de servicios de telecomunicaciones, la CRC consideró pertinente trasladar esos comentarios para su evaluación en este escenario.

En relación con la diferenciación entre los mercados de mensajería A2P y P2P, los comentarios destacan que ambos segmentos presentan características estructurales, modelos de negocio y dinámicas competitivas sustancialmente distintas, lo que justificaría un tratamiento regulatorio diferenciado. En particular, se argumenta que el segmento A2P opera en un entorno B2B (Business to Business) con múltiples actores, operadores, integradores y empresas, y además señalan que enfrenta competencia directa de servicios OTT como aplicaciones de mensajería instantánea, lo que limitaría la necesidad de intervención en precios. En este sentido, varios agentes proponen la desregulación del mercado A2P o la adopción de esquemas de libre negociación, al considerar que existen condiciones suficientes para la formación eficiente de precios.

La mayoría de los interesados, encabezados por gremios como Asobancaria, Asomóvil y los PRSTM coinciden en señalar que la reducción del cargo de terminación de SMS a niveles cercanos a cero podría generar efectos adversos en materia de fraude cibernético. En particular, advierten que tarifas significativamente bajas disminuyen las barreras económicas para el envío masivo de mensajes, facilitando la ejecución de prácticas fraudulentas como el smishing, el abuso de códigos OTP, el tráfico automatizado y el call pumping. En este contexto, argumentan que la rentabilidad de este tipo de actividades ilícitas depende del costo marginal de envío, por lo que una reducción sustancial del cargo incrementaría los incentivos para su proliferación. Asimismo, señalan el riesgo de incremento de tráfico

gris proveniente de integradores con bajos estándares de verificación, así como posibles afectaciones al ecosistema digital y al sector financiero.

Adicionalmente, los comentarios señalan que la caída proyectada del cargo de terminación (cercana al 97%) compromete la sostenibilidad del servicio y desincentiva la inversión en infraestructura y modernización tecnológica. En particular, advierten que esta situación podría afectar el despliegue y fortalecimiento de soluciones orientadas a la prevención, detección y mitigación del fraude cibernético

Ahora bien, con base en los comentarios recibidos, la CRC consideró pertinente diferenciar el análisis entre dos servicios de mensajería que presentan características técnicas, económicas y competitivas claramente distintas. En consecuencia, se abordó de manera separada: (i) el servicio de mensajería entre personas (P2P) y (ii) el servicio de mensajería de aplicaciones a personas (A2P).

En relación con el servicio de SMS P2P, en el marco del proyecto «Esquemas de Remuneración Mayorista de Redes Móviles» se actualizó el valor de remuneración aplicable a la terminación de estos mensajes en redes móviles, con base en la metodología de LRIC puro derivada del «Modelo de Costos Empresa Eficiente Móvil 2025». Como resultado de este ejercicio, el cargo de terminación se fijó en $0,03 pesos constantes de 2026 por SMS, el cual entró en vigor a partir del 1 de abril de 2026.

Por su parte, en lo que respecta al servicio de mensajería A2P, la CRC decidió mantener el esquema de remuneración vigente en esa oportunidad y trasladar el análisis de este segmento al presente proyecto regulatorio, reconociendo sus particularidades en términos de uso, estructura de mercado y riesgos asociados, especialmente en materia de fraude cibernético.

En este sentido, la Comisión definió una estrategia regulatoria compuesta por dos fases complementarias. La primera está orientada a la evaluación y eventual adopción de medidas regulatorias y técnicas para prevenir y mitigar el fraude cibernético mediante servicios móviles, incluyendo aquellas aplicables al ecosistema de mensajería SMS A2P. La segunda estará enfocada en el análisis económico y competitivo del mercado de mensajería SMS A2P y en la evaluación de alternativas regulatorias relacionadas con su esquema de remuneración, incorporando los resultados, costos, inversiones, beneficios e impactos derivados de las medidas antifraude que resulten adoptadas en la primera fase.

Una de las razones principales para adoptar esta decisión de dividir este proyecto en dos fases es que, a juicio de la Comisión, se requiere contar con información actualizada sobre la prestación del servicio de mensajería SMS A2P, sus condiciones operativas, económicas y comerciales, razón por la cual se requirió esta información a algunos agentes del mercado por vía de requerimiento de información[49].

En consecuencia, los comentarios recibidos en relación con la remuneración del servicio SMS A2P serán considerados como insumo para el desarrollo de esta segunda fase regulatoria, la cual será objeto de un documento independiente de propuesta regulatoria, con el fin de evaluar las distintas alternativas regulatorias y definir una propuesta para la remuneración de la terminación de mensajes SMS A2P, que considere tanto las condiciones de competencia como también los incentivos adecuados para la inversión, la eficiencia, la mitigación de riesgos en el ecosistema digital y la información que fue solicitada por la Comisión por vía del requerimiento de información mencionado.

[49] CRC. Requerimiento de información No. 2026-024. Información relacionada con la remuneración de mensajes cortos de texto en comunicaciones A2P. Número de radicado 2026200867 del 3 de junio de 2026.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9. EVALUACIÓN DE LAS ALTERNATIVAS DE SOLUCIÓN

9.1. Metodología de evaluación de alternativas

En esta sección se exponen las metodologías de los enfoques de evaluación de alternativas utilizados en esta propuesta, a saber: Análisis de Decisión Multicriterio, Análisis de Costo-Efectividad, Análisis de Costos Administrativos y Simplificación normativa.

9.1.1 Metodología de Análisis Multicriterio

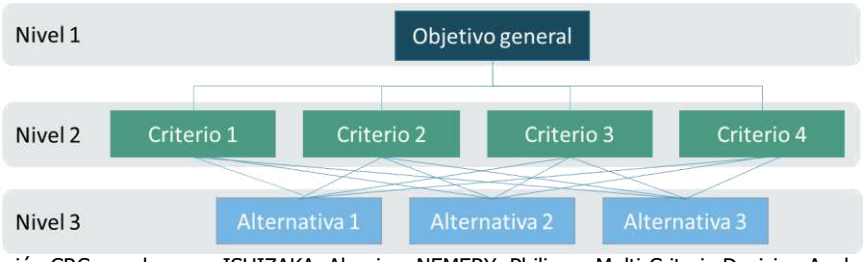
El proceso de AIN requiere del uso de una metodología que permita analizar los impactos potenciales de las alternativas propuestas para resolver el problema o problemas identificados. Este tipo de análisis parte del reconocimiento de que los problemas a ser estudiados son complejos, debido a que para llevar a cabo un examen integral debe considerarse una gran variedad de aspectos tanto cuantitativos como cualitativos y que, principalmente estos últimos, abarcan elementos que no siempre es posible medir con exactitud plena. Este tipo de análisis permite incluir todos estos aspectos a la hora de valorar las diferentes soluciones que fueron propuestas para resolver el problema identificado.

Vale la pena mencionar que el análisis multicriterio es una de las metodologías más usadas en la evaluación de políticas públicas y en los procesos de toma de decisiones[50]. La posibilidad de incluir dentro de los criterios, simultáneamente, tanto aspectos cuantificables, como aspectos no cuantificables, requiere un grado de análisis detallado y riguroso que considere tanto los intereses de los diferentes agentes que tengan injerencia sobre las temáticas de estudio, como las consecuencias directas e indirectas que posiblemente surjan de la aplicación de las diferentes medidas.

En el desarrollo del análisis multicriterio existen diversas técnicas de estimación, siendo el Proceso de Análisis Jerárquico (AHP por sus siglas en inglés) una de las más usadas en la literatura[51]. Esta metodología, desarrollada por Saaty (1977-1980), parte de la descomposición de la temática o problemática a analizar, en un esquema jerárquico como el que se describe en la Ilustración 12. Así, el primer nivel del problema corresponde al objetivo principal de la decisión; el segundo nivel representa los criterios frente a los cuales se van a evaluar las alternativas o soluciones para lograr el objetivo, los cuales, cabe mencionar, pueden a su vez componerse de subcriterios; y el último nivel representa las alternativas que serán sujetas a evaluación.

[50] DEAN, Marco. Multi-criteria analysis. En: Advances in Transport Policy and Planning [En Línea]. Vol 6. 2020. Niek Mouter. p. 165-224. ISBN 9780128208212. Disponible en: https://www.sciencedirect.com/science/article/pii/S2543000920300147
[51] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT: LONDON. Communities and Local Government. Multi-criteria analysis: a manual [En Línea]. Londres: 2009., 168 pp. ISBN: 978-1-4098-1023-0. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191506/Multcrisis_analysis_a_manual.pdf

Ilustración 12. Estructura del proceso jerárquico de análisis



Fuente: Elaboración CRC, con base en ISHIZAKA, Alessio y NEMERY, Philippe. Multi-Criteria Decision Analysis. Methods and Software. 2013. El nivel 2 puede descomponerse en varios subniveles dependiendo de la cantidad de subcriterios que compongan el criterio.

La técnica del AHP busca construir, mediante un proceso analítico, una representación de la «curva de utilidad de los criterios y alternativas»[52]. Esta técnica se basa en las leyes de la psicofísica para establecer escalas de evaluación relativas[53], a partir de comparaciones directas, segmentando el análisis por pares, para determinar los grados de preferencia mediante un proceso matemático[54]. Esta técnica, además, permite evaluar las alternativas a la luz de criterios que no tengan ningún grado de preferencia previa al análisis, buscando minimizar sesgos de percepción o prejuzgamiento.

De acuerdo con el Departamento para Comunidades y Gobierno Local del Reino Unido[55], la implementación de un análisis multicriterio debe cumplir las siguientes fases:

i. Descripción del contexto de decisión, identificando el problema, los objetivos generales y específicos y los agentes involucrados.
ii. Identificación y desarrollo de las alternativas de solución al problema establecido.
iii. Identificación de los criterios y subcriterios.
iv. Construcción de la matriz de comparación entre criterios de evaluación para establecer su importancia relativa con el fin de generar sus respectivos ponderadores.
v. Valoración de la consistencia de los resultados encontrados en la matriz de ponderadores.
vi. Evaluación del desempeño de las alternativas de solución para cada uno de los criterios establecidos, para posteriormente calcular el desempeño general de la alternativa con base en los ponderadores establecidos.
Presentación y análisis de los resultados.

La metodología de Análisis Multicriterio descrita fue utilizada para evaluar las alternativas regulatorias propuestas para las siguientes temáticas:

[52] ISHIZAKA, Alessio y NEMERY, Philippe. Multi-Criteria Decision Analysis. Methods and Software: Wiley, 2013. ISBN: 978-1-119-
97707-9
[53] DOLDÁN, Félix. Métodos de decisión basados en criterios cualitativos: una comparación entre los métodos AHP y REMBRANT. 1999. Universidad de La Coruña.
[54] SAATY, Thomas L. Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process [en línea]. En: RACSAM - Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas. RACSAM, septiembre de 2008. vol. 102, no 2. pp 251-318. Disponible en: https://link.springer.com/article/10.1007/BF03191825
[55] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT: LONDON. Op. Cit., p. 50.

Eje de temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

- Temática 1: Falta de identificación clara del remitente en SMS A2P
- Temática 3: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

Eje de temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

- Temática 2: Falta de una instancia de coordinación para la articulación y el intercambio de alertas
- Temática 3: Falta de lineamientos específicos para monitoreo y etiquetado de tráfico
- Temática 4: Falta de estandarización en la aplicación de listas de no originación (DNO)

Eje de temáticas enfocadas en la educación de la ciudadanía

- Temática 1: Acciones educativas que aumenten el conocimiento de los usuarios

Los resultados de la aplicación de la metodología multicriterio se encuentran desarrollados en la sección 9.2 de presente documento, de forma correspondiente para cada una de las temáticas, con excepción de aquellas en donde se aplica la metodología de Análisis de Costo-Efectividad y el enfoque de simplificación regulatoria.

Adicionalmente, con el propósito de fortalecer la robustez metodológica del análisis multicriterio y reducir potenciales sesgos en la evaluación de las alternativas regulatorias, la CRC implementó una estrategia de valoración dual basada en la participación de dos grupos internos de trabajo con enfoques complementarios:

- El primer grupo correspondió al equipo técnico encargado de la construcción de las propuestas regulatorias, cuya evaluación se enfocó en aspectos de coherencia normativa, proporcionalidad y alineación con los objetivos de política pública.

- El segundo grupo estuvo conformado por expertos en gestión de recursos de identificación, seguridad de redes y control de fraude, quienes evaluaron las alternativas desde una perspectiva técnica y operativa asociada a autenticación, trazabilidad, riesgos de implementación y capacidades de monitoreo, así como un experto asesor externo de la CRC.

La consolidación del resultado final se realizó mediante una agregación ponderada de ambas valoraciones, asignando un peso del 33% al grupo de construcción regulatoria y un 67% al grupo técnico especializado, conforme a la siguiente expresión:

$$Puntaje\ final_i = (0{,}33 \times Evaluación\ Regulatoria_i) + (0{,}67 \times Evaluación\ Técnica_i)$$

Esta estrategia permitió incorporar perspectivas complementarias dentro del proceso de evaluación, mejorar la consistencia técnica de los resultados y disminuir el riesgo de sobrevaloración de alternativas regulatorias con limitaciones operativas o tecnológicas.

9.1.2 Metodología de Análisis de Costo-Beneficio (ACB)

El ACB es una metodología para evaluar la viabilidad social o privada de proyectos o intervenciones, al sopesar los costos frente a los beneficios implícitos valorados en unidades monetarias.[56] Como fue mencionado en la sección anterior, a diferencia del Análisis Costo Efectividad (ACE), el ACB compara los costos con los beneficios monetizados, mientras que el ACE relaciona los costos con unidades relevantes de efectividad sin monetizar los resultados. Sin embargo, el ACB y el ACE son casi equivalentes cuando respaldan las decisiones de asignación de recursos.[57]

En el contexto del análisis del impacto regulatorio, el ACB y el ACE son similares en términos de evaluar las implicaciones de las intervenciones, pero difieren significativamente en sus enfoques, objetivos y los tipos de resultados que miden. El objetivo del ACB es determinar si los beneficios de una intervención superan sus costos, proporcionando así un beneficio neto que contribuye a la toma de decisiones. El ACB traduce todos los resultados en términos monetarios, lo que permite una comparación directa de diversos impactos[58], mientras que en el ACE estos deben ser transformados y ponderados para poder ser sumados.

En el contexto en que el ACB se desarrolla para bienes o servicios que tienen un mercado establecido se hace necesario considerar las formas funcionales tanto para la demanda como para la oferta, para lo cual se pueden emplear modelos econométricos, a partir de los cuales se establecen tanto las cantidades como los precios de equilibrio, y posteriormente se calculan los excedentes del consumidor y del productor. Con base en este insumo, se calculan los beneficios netos para cada una de las alternativas regulatorias evaluadas según sus efectos sobre la función de oferta y sobre los atributos que caracterizan a la demanda del bien o producto.

Cuando la evaluación se desarrolla en un horizonte temporal de varios años, los costos se actualizan mediante el cálculo del Valor Presente Neto (VPN), utilizando una tasa social de descuento, conforme a la siguiente expresión:

$$VPN = \sum_{t=0}^{T} \frac{(B_t - C_t)}{(1+r)^t}$$

Donde:

B_t: representa los beneficios estimados en el periodo t
$C_{t:}$ administrativos y operativos asociados a la medida regulatoria en el periodo t
r: la tasa social de descuento, que para este caso se usó el valor del WACC calculado por la CRC, 11,57%[59]
T: Horizonte temporal, en este caso 3 años dada la posibilidad de proyección de los beneficios económicos de las medidas regulatorias

[56] Yasui, S. (2005). A Critical Review of the Traditional Methodology of Cost-Benefit Analysis and a Proposed Alternative. Human and Ecological Risk Assessment: An International Journal, 11(2), 411–432. https://doi.org/10.1080/10807030590925795
[57] Phelps, C. E.; Mushlin, A. I. (1991). On the (Near) Equivalence of Cost-Effectiveness and Cost-Benefit Analyses. International Journal of Technology Assessment in Health Care. 7, 12 – 21. https://api.semanticscholar.org/CorpusID:21346648
[58] Cheung, H. (2012). Tourism in kenya's national parks: a cost-benefit analysis. SURG Journal, 6(1), 31-40. https://doi.org/10.21083/surg.v6i1.2019
[59] CRC. Documento soporte del proyecto regulatorio «Esquemas de remuneración mayorista de redes móviles». Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-9/Propuestas/documento-soporte-esquemas-remuneracion-mayorista-redes-moviles.pdf

La metodología ACB descrita fue utilizada para evaluar las alternativas regulatorias propuestas en la «Subtemática 2: Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude» correspondiente al eje del servicio SMS y la «Subtemática 1: Limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)» del eje del servicio de voz, desarrollada en la sección 9.2 de este documento. En esa sección se presenta en detalle el procedimiento y los resultados obtenidos de la aplicación de esta metodología de análisis.

9.1.3 Metodología de Costos Administrativos

La metodología de Costos Administrativos permite identificar, cuantificar y valorar las cargas administrativas y operativas que una intervención regulatoria impone a los agentes obligados, particularmente aquellas asociadas al cumplimiento de obligaciones de reporte, almacenamiento, validación, monitoreo, adecuaciones tecnológicas, capacitación, gestión documental o intercambio de información. Esta metodología parte de la estimación de los recursos requeridos para cumplir una obligación regulatoria y su valoración monetaria, considerando tanto costos de inversión como costos recurrentes de operación y mantenimiento. En términos generales, el costo administrativo total puede expresarse como la suma de los costos asociados a cada actividad requerida para el cumplimiento regulatorio, de acuerdo con la siguiente expresión:

$$CA = \sum_{i=1}^{n} (Q_i \times P_i)$$

donde CA corresponde al costo administrativo total, Q_i representa la cantidad de recursos, tiempo o actividades requeridas para el cumplimiento de la obligación i, y P_i corresponde al costo unitario asociado a dichos recursos o actividades.

Esta metodología es empleada para evaluar aquel paquete de medidas que resulte de evaluar cada una de las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz, con el fin de contrastar el costo total acumulado frente al costo que implicaría la adopción del método STIR/SHAKEN/RCD. En la sección titulada «Enfoque de evaluación de las alternativas de mejor desempeño frente a STIR/SHAKEN. se presentan los resultados de la aplicación de esta metodología.

9.1.4 Enfoque de simplificación normativa

De acuerdo con la «Política de Mejora Regulatoria» de la CRC y los documentos desarrollados por el DNP al respecto[60], el enfoque de simplificación regulatoria surgió como resultado de la búsqueda de soluciones que tuvieran como propósito disminuir las cargas administrativas experimentadas por los operadores y usuarios del sector de comunicaciones, con el fin de contar con un marco regulatorio eficiente, simple, claro, que reconozca tanto la evolución del mercado y de la tecnología como la existencia de otros regímenes jurídicos transversales sin necesidad de duplicar las normas.

[60] DNP (2016). Guía Metodológica de Análisis de Impacto Normativo. Disponible en: https://bit.ly/2RSQRII y DNP (2014). Consejo
Nacional de Política Económica y Social 3 CONPES. Documento CONPES 3816 Mejora Normativa: Análisis de Impacto. Disponible en: https://bit.ly/3SmXIu9.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Así, la Comisión estableció el enfoque de simplificación como un pilar de la mejora regulatoria de aplicación constante e integral, que tiene como finalidad contar con un marco regulatorio sectorial que, aunque técnico y especializado, sea también, dentro de lo posible, sencillo, de lenguaje claro, flexible y dinámico, considerando que, si bien la regulación genera costos y cargas administrativas, debe buscarse que estos no sean excesivos.

De esta manera, este enfoque de simplificación no se refiere únicamente a la reducción o eliminación de regulación, sino que es un concepto más amplio que incluye mejoras en los procesos de interacción con los sujetos de la regulación y de estos con sus usuarios, así como la optimización, digitalización y automatización de los trámites que se requieran con el fin de reducir los costos que estos puedan generar.

Así las cosas, el pilar de simplificación regulatoria se materializa durante el diseño y desarrollo de la regulación de carácter general, mediante la revisión integral de las temáticas regulatorias que se revisan en los proyectos que se llevan a cabo en la CRC, con el fin de identificar si en al menos una de las medidas sujetas a revisión se cumple alguno de los siguientes criterios:

1. **Evolución de mercado:** Se presenta cuando las condiciones en el mercado que dieron origen a la regulación han dejado de existir, de tal manera que es inviable continuar con la aplicación de la norma existente.
2. **Evolución tecnológica:** Se materializa por la implementación de tecnologías que modifican ciertas características de la prestación de los servicios o transforman los modelos de negocio de los agentes involucrados, por lo que la norma correspondiente ya no es aplicable para los agentes del sector. Lo anterior se debe analizar de conformidad con las circunstancias particulares de cada caso según aplique.
3. **Duplicidad normativa:** Se refiere a la existencia de artículos en dos o más normas que cumplen funciones iguales o similares.
4. **Transitoriedad:** Se presenta en aquellos artículos que eran aplicables durante un periodo de tiempo determinado, que ya finalizó.

Ahora bien, en el Documento de Formulación del proyecto «Simplificación Regulatoria 2024» la CRC desarrolló dos aspectos adicionales a los anteriormente enumerados que entraron a formar parte de los criterios de identificación de las normas susceptibles de simplificación, dentro de los cuales[61] se destaca i) el de *Posibilidad de optimización de la disposición regulatoria* que «[s]e presenta cuando es posible mejorar la formulación, redacción, estructuración y organización interna de la proposición normativa, de manera que se fortalezca el propósito perseguido con la regla subyacente a la norma y, por lo tanto, no se afecte negativamente su finalidad original o se disminuya su eficacia»[62]; y ii) la *Posibilidad de reducción de costos de cumplimiento,* que se presenta cuando es posible modificar la norma de modo que se persigan los mismos objetivos y se logren los mismos resultados, pero con un menor costo de cumplimiento por parte de los agentes regulados.

[61] Ibid. Pág. 34.
[62] «Adicionalmente, esta Comisión agrega las siguientes condiciones para la ejecución de esta metodología de simplificación: En el caso del criterio "posibilidad de optimización de la disposición regulatoria", la CRC verificará que la modificación propuesta no altere la regla subyacente ni el objetivo original, pero que efectivamente sí mejore la formulación de la norma.
Para lo anterior, en los casos que aplique y sea pertinente, la Comisión podría tomar como insumo la información recopilada de los espacios de socialización con los agentes de mercado, agremiaciones y público en general.» CRC. Documento de Formulación y Justificación del proyecto «SIMPLIFICACIÓN REGULATORIA 2024» Pág. 44.

En este sentido, si se materializa al menos uno de los criterios antes descritos en los artículos de la Resolución CRC 5050 de 2016 que son sujetos de revisión en el marco de la presente iniciativa, estos serán candidatos a ser simplificados, siempre y cuando su derogación no colisione con mandatos constitucionales, legales, o lineamientos de política pública que se encuentren vigentes.

En la sección 9.2.4 de este documento se presentan los análisis y resultados obtenidos en la situación problemática analizadas mediante la metodología de simplificación normativa.

9.2. Alternativas de solución a evaluar

De conformidad con los comentarios, observaciones y sugerencias de los agentes interesados, la Comisión estimó necesario modificar, complementar y/o especificar algunas de las alternativas de solución de la temática identificadas. Así, en este capítulo se presentarán las alternativas de solución ajustadas para cada temática.

9.2.1 Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

9.2.1.1 Subtemática 1: Falta de identificación clara del remitente en SMS A2P

Situación identificada:	Actualmente, los SMS A2P se originan principalmente desde códigos cortos numéricos compartidos entre múltiples marcas y campañas, lo que provoca que el usuario no pueda distinguir fácilmente quién envía el mensaje.
Causas relacionadas:	Causa 1: Los desarrollos regulatorios sobre recursos de identificación se han enfocado en su mayoría en la administración y el uso eficiente de dichos recursos escasos. Causa 2: Las medidas de gestión y control frente al contacto fraudulento implementadas por los PRST y asignatarios son insuficientes.
Alternativa 1: Statu quo	Se conserva el esquema regulatorio actual, en el que los remitentes se identifican mediante códigos cortos numéricos compartidos y la regulación exige incluir el nombre del originador dentro del texto del mensaje.
Alternativa 2: Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)	Introduce la obligatoriedad de que todos los remitentes de mensajes de texto A2P utilicen códigos alfanuméricos únicos, en forma de Sender ID similar a un nombre de dominio, el cual sería visible para los usuarios en el encabezado del SMS.
Alternativa 3: Asignación y uso de código alfanumérico solo para tráfico transaccional	Introduce la obligatoriedad de que el Sender ID alfanumérico sea aplicado únicamente a mensajes transaccionales, mientras que el tráfico promocional continúa identificándose mediante códigos cortos o números E.164, manteniendo la obligación actual de incluir el nombre del originador dentro del texto del mensaje.

9.2.1.1.1 Alternativa 1: Statu quo

Bajo esta alternativa, se propone mantener la regulación vigente. Esto implica conservar el esquema actual, en el que los remitentes se identifican mediante códigos cortos numéricos y la regulación exige incluir el nombre del originador dentro del texto del mensaje. Esta alternativa no implica costos

adicionales ni cambios operativos, pero no resuelve la falta de identificación visual inmediata por parte del usuario para facilitar la identificación y veracidad del contenido.

9.2.1.1.2 Alternativa 2: Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)

Esta alternativa introduce la obligatoriedad de que todos los remitentes de mensajes de texto A2P utilicen códigos alfanuméricos únicos, en forma de Sender ID similares a un nombre de dominio, el cual sería visible para los usuarios en el encabezado del SMS. La alternativa implica la creación de un nuevo recurso de identificación en la regulación que será denominado Sender ID, el cual será administrado por la CRC en su asignación, uso y recuperación.

En otras palabras, el SENDER ID sería un recurso de identificación administrado por la CRC, que identifica de manera única e inequívoca al responsable directo por la producción y generación de contenidos o aplicaciones enviados a través de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD). El SENDER ID es visible para el usuario final en el encabezado del mensaje recibido, en sustitución de un código numérico, y permite la identificación clara e inmediata del originador del contenido. Para materializar lo anterior, se incluiría un nuevo capítulo en el TÍTULO VI de la Resolución CRC 5050 de 2016 en el que se regulará la estructura del SENDER ID, los requisitos para su asignación, el trámite para su asignación, el marco regulatorio de su uso y las respectivas causales de recuperación de este nuevo recurso de identificación.

Esta alternativa es útil porque cada marca registrada obtendría un Sender ID único alfanumérico, el cual sería incluido dentro del proceso de validación centralizado o distribuido de originadores de contenido (Alternativas 2, 3 y 4 de la temática 2)

El efecto de esta alternativa es que el usuario pueda identificar de manera clara y legible el remitente de todas las comunicaciones que reciba mediante mensajes cortos de texto tradicionales a través del encabezado del mensaje (ej.: «BancoXYZ» en lugar de «12345»).

Este mecanismo de identificación se complementa con los procesos de validación a fin de aportar herramientas que permitan evitar la suplantación y el fraude, con el propósito de responder a los problemas de atribución de responsabilidades identificados en la generación de contenidos fraudulentos.

El funcionamiento de esta alternativa se entiende como parte de un esquema de trazabilidad extremo a extremo, que incluye:

- verificación del originador
- gestión del recurso de identificación
- atribución de responsabilidades.

Este esquema se comprende bajo un enfoque sistémico en donde se propone la definición de actores, roles o funciones y responsabilidades, es decir, se pasa de una lógica de técnica (identificador) a una lógica institucional (responsabilidad). En este sentido, esta alternativa propone la descripción de los siguientes elementos de un ecosistema de múltiples que conforman el servicio SMS A2P:

- Identificación de actores
- Asignación de responsabilidades según el ejercicio de control del recurso de identificación, del contenido y del tráfico.
- Asociación inequívoca entre identificador (Sender ID) y el titular o asignatario de dicho recurso.
- Adopción de reglas de asignación, modificación y recuperación del recurso, así como para el manejo de homonimias y variaciones engañosas.
- Régimen de prohibiciones.

Así mismo, con el propósito de que el Sender ID no sea únicamente un recurso «visual», se contempla que la identificación esté respaldada por el SIGRI, sistema en donde los usuarios podrán verificar la autenticidad del originador del contenido y el histórico de novedades del recurso. Adicionalmente, se propone una implementación mediante fases.

9.2.1.1.3 Alternativa 3: Asignación y uso de código alfanumérico solo para tráfico transaccional

Esta alternativa contempla que el uso de códigos alfanuméricos (Sender ID) se aplique únicamente a mensajes de carácter transaccional o de autenticación, tales como códigos de verificación (OTP) o alertas bancarias, mientras que el tráfico promocional continuaría identificándose mediante códigos cortos o números E.164, manteniendo la obligación actual de incluir el nombre del remitente dentro del texto del mensaje.

Al igual que en la alternativa anterior, este esquema se enmarca en un modelo de gobernanza del recurso de identificación, en el que los Sender ID asignados para tráfico transaccional deberán cumplir con condiciones de validación, trazabilidad y control, así como con reglas de asignación que eviten el uso indebido de marcas o identificadores engañosos indicados anteriormente.

En este contexto, se mantiene la asignación de responsabilidades sobre los actores que ejercen el control efectivo del recurso y del contenido, quienes deberán garantizar el uso adecuado de los identificadores en los mensajes de mayor criticidad.

Esta alternativa es útil porque introduce un criterio de gestión diferenciada del riesgo, priorizando la protección del usuario en aquellas comunicaciones que tienen un mayor impacto potencial en términos de fraude, como las asociadas a servicios financieros o procesos de autenticación.

Este enfoque permite concentrar los esfuerzos regulatorios y operativos en los segmentos más sensibles del tráfico, lo que puede traducirse en menores costos de implementación y una adopción más rápida de la medida en los casos de mayor relevancia.

El efecto de esta alternativa es que los usuarios cuenten con una identificación clara y validada del remitente en las comunicaciones más críticas, reduciendo el riesgo de suplantación en escenarios de alto impacto, como el acceso a servicios financieros.

En este contexto, por efecto de esta alternativa, el Sender ID alfanumérico se aplicaría únicamente a mensajes transaccionales y de autenticación (p. ej., OTP, alertas bancarias), mientras que el tráfico

promocional continuaría identificándose mediante códigos cortos o números E.164, manteniendo la obligación actual de incluir el nombre del originador dentro del texto del mensaje.

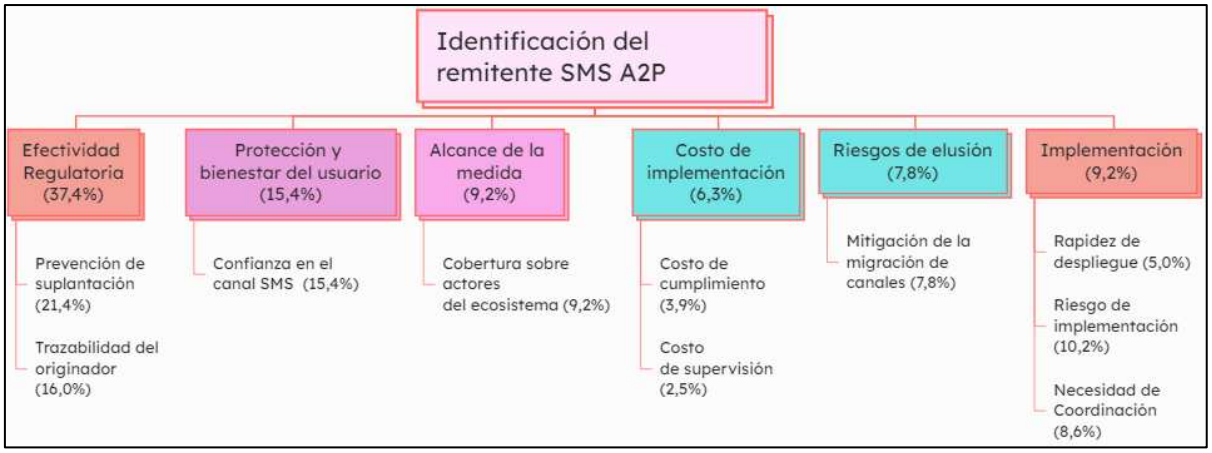
De esta forma, se prioriza la protección del usuario en comunicaciones críticas, como financieras y autenticación, y se reducen tanto los costos como la implementación para contenidos de menor criticidad como son las campañas publicitarias. Esto mejora la seguridad en mensajes sensibles y mantiene un esquema flexible para los demás tipos de tráfico.

9.2.1.1.4 Evaluación de alternativas

La evaluación de alternativas regulatorias para la temática «Falta de identificación clara del remitente en SMS A2P» se desarrolló bajo un enfoque de Análisis de Decisión Multicriterio (ADMC), siguiendo los lineamientos metodológicos descritos en la sección anterior. Este enfoque resulta pertinente dada la necesidad de evaluar simultáneamente múltiples dimensiones asociadas a la implementación de mecanismos de identificación del originador de mensajes SMS A2P, incluyendo aspectos relacionados con la mitigación del fraude, la trazabilidad del remitente, la protección del usuario, los costos de implementación, los riesgos operativos y la viabilidad de despliegue de las medidas propuestas.

En este contexto, la aplicación de esta metodología permitió comparar de manera estructurada el desempeño relativo de cada alternativa regulatoria frente a los criterios definidos, considerando tanto los beneficios esperados en términos de fortalecimiento de la confianza y autenticidad del canal SMS, como los costos, riesgos y necesidades de coordinación asociados a su implementación en el ecosistema conformado por PRST, PCA e IT, en un contexto de tráfico nacional e internacional.

Ilustración 13. Árbol jerárquico de la temática: Falta de identificación clara del remitente en SMS A2P



Fuente: Elaboración CRC

Para el ejercicio de evaluación desarrollado se consideraron seis criterios y diez subcriterios los cuales cumplen con los principios fundamentales para la construcción de estos. El árbol jerárquico de decisión que ilustra el problema sujeto de evaluación se presenta en la Ilustración 13. La matriz de comparación junto con el resultado de la prueba de consistencia, así como la tabulación de los ponderadores de los subcriterios se encuentran en la sección de ANEXOS.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Criterios y Subcriterios

A continuación, se presentan las definiciones de los subcriterios que se establecieron para la evaluación de las diferentes alternativas:

Efectividad regulatoria:

- Prevención de suplantación: Grado en que la alternativa reduce la posibilidad de suplantación de identidad de marcas o entidades legítimas, mediante la implementación de mecanismos de validación del origen del mensaje, uso de identificadores verificables y controles sobre el envío de mensajes.

- Trazabilidad del originador: Grado en que la alternativa permite identificar de manera unívoca, verificable y auditable al originador del mensaje, facilitando la asignación de responsabilidades en caso de fraude.

Protección y bienestar del usuario:

- Confianza en el canal SMS: Grado en que la alternativa contribuye a aumentar la percepción de seguridad y confiabilidad del usuario frente a los mensajes SMS A2P, a partir de información suficiente sobre el remitente.

Alcance de la medida:

- Cobertura sobre actores del ecosistema: Nivel en que la alternativa involucra a agentes relevantes de la cadena valor del servicio SMS A2P (PRST, PCA, IT, tráfico internacional).

Costos de implementación:

- Costos de cumplimiento para los agentes: Costos técnicos, operativos y administrativos que deben asumir PRST, PCA e IT para implementar y mantener la alternativa.

- Costos de supervisión: Nivel de recursos técnicos y administrativos requeridos por la autoridad regulatoria para monitorear, verificar y hacer cumplir la medida.

Riesgos de elusión:

- Mitigación de la migración de canales: Nivel en que la medida reduce el incentivo de migrar el tráfico hacia canales no regulados (OTT, aplicaciones de mensajería).

Implementación:

- Rapidez de despliegue: Tiempo estimado requerido para implementar la alternativa desde su adopción regulatoria hasta su operación efectiva en el mercado.

- Riesgo de implementación: Grado en que la alternativa presenta incertidumbres técnicas, operativas y de coordinación que puedan afectar su adopción efectiva en el ecosistema A2P, considerando la necesidad de ajustes en redes y plataformas (SMS-C, agregadores), la disponibilidad de capacidades para gestionar identificadores alfanuméricos (Sender ID), la

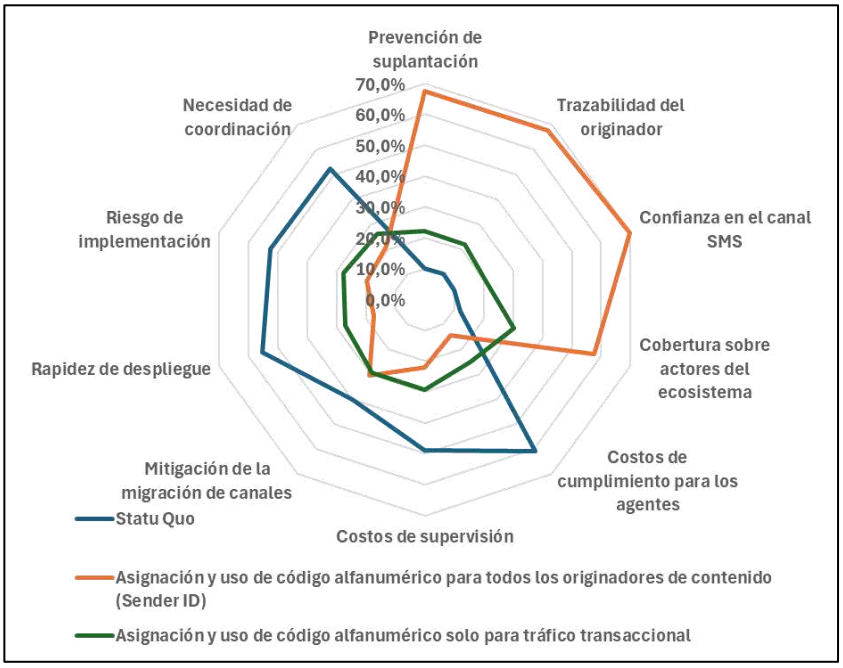
dependencia de actores nacionales e internacionales y la posibilidad de implementación homogénea en el mercado.

- Necesidad de coordinación: Grado en que la alternativa requiere articulación entre múltiples actores de tal manera que presenta, con mecanismos de coordinación simples, una menor dependencia de acuerdos entre actores.

Los resultados que se exponen en la Ilustración 14 corresponden al porcentaje de desempeño relativo alcanzado por cada alternativa en cada subcriterio, multiplicado por su respectivo ponderador, mientras que el puntaje agregado de desempeño global se presenta en la

Ilustración 15. De esta manera, la evaluación permite identificar la alternativa que, en términos integrales, ofrece el mejor balance entre capacidad de respuesta al problema identificado, alineación con los objetivos de política pública y costos de implementación.

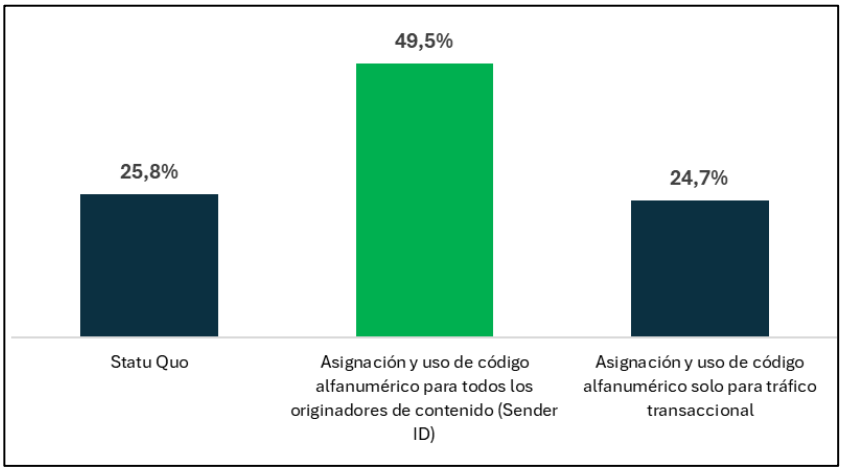
Ilustración 14. Desempeño relativo de las alternativas de la temática: Falta de identificación clara del remitente en SMS A2P



Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 15. Puntaje agregado de cada alternativa de la temática: Falta de identificación clara del remitente en SMS A2P



Fuente: Elaboración CRC.

A continuación, se presenta la descripción del desempeño de las alternativas regulatorias evaluadas para la temática «Falta de identificación clara del remitente en SMS A2P», frente a cada uno de los criterios considerados en el análisis multicriterio.

a. En cuanto al criterio de prevención de suplantación, este evalúa el grado en que cada alternativa reduce la posibilidad de suplantación de identidad de marcas o entidades legítimas mediante mecanismos de validación del origen del mensaje y uso de identificadores verificables. La alternativa de «Statu Quo» presenta el menor desempeño relativo (10,2%), dado que mantiene el esquema actual basado en códigos cortos numéricos compartidos y en la obligación de incluir el nombre del originador dentro del texto del mensaje, lo cual limita la capacidad de validar de manera visual e inmediata la autenticidad del remitente.

   Por su parte, la alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» obtiene un desempeño intermedio (22,3%), debido a que introduce mecanismos de identificación reforzada únicamente para mensajes críticos o de autenticación, reduciendo parcialmente los riesgos de suplantación en comunicaciones de mayor sensibilidad.

   La alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» presenta el mejor desempeño en este criterio (67,6%), en la medida en que establece un esquema generalizado de identificadores alfanuméricos únicos y verificables para todos los remitentes A2P, fortaleciendo significativamente la autenticidad del originador y reduciendo la posibilidad de uso indebido de marcas o identidades legítimas de forma generalizada.

b. Respecto del criterio de trazabilidad del originador, este evalúa la capacidad de las alternativas para identificar de manera unívoca, verificable y auditable al originador del mensaje, facilitando la asignación de responsabilidades en caso de fraude. La alternativa de «Statu Quo» presenta

nuevamente el menor desempeño (10,2%), dado que el uso de códigos numéricos compartidos dificulta la atribución clara de responsabilidades y limita la capacidad de auditoría sobre el origen efectivo del tráfico.

La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» alcanza un desempeño intermedio (22,0%), ya que fortalece la trazabilidad únicamente sobre el subconjunto de tráfico asociado a procesos de autenticación o mensajes transaccionales.

Por su parte, la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» obtiene el mejor desempeño relativo (67,8%), debido a que incorpora un esquema integral de gestión y validación de identificadores asociados de manera inequívoca al originador del contenido, permitiendo mejorar significativamente la atribución de responsabilidades y los mecanismos de control sobre el ecosistema A2P.

c. En relación con el criterio de confianza en el canal SMS, este evalúa el grado en que las alternativas contribuyen a aumentar la percepción de seguridad y confiabilidad de los usuarios frente a los mensajes A2P. La alternativa de «Statu Quo» presenta el menor desempeño (9,8%), dado que mantiene las condiciones actuales en las cuales el usuario no puede identificar de manera clara e inmediata el remitente legítimo del mensaje.

   La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño intermedio (20,5%), debido a que mejora la identificación del remitente únicamente en comunicaciones críticas.

   Por su parte, la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» obtiene el mayor desempeño (69,6%), en la medida en que permite que los usuarios visualicen directamente el nombre verificable de la entidad emisora en el encabezado del mensaje, fortaleciendo la percepción de autenticidad y reduciendo la incertidumbre frente al origen de las comunicaciones recibidas.

d. En cuanto al criterio de cobertura sobre actores del ecosistema, este evalúa el nivel en que cada alternativa involucra a los distintos agentes relevantes de la cadena de valor del servicio SMS A2P. La alternativa de «Statu Quo» presenta un desempeño reducido (12,0%), dado que no incorpora nuevas obligaciones o mecanismos de validación aplicables de manera transversal a los actores del ecosistema.

   La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño intermedio (30,4%), debido a que el alcance de la medida se limita únicamente al tráfico transaccional y de autenticación.

   La alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» presenta el mejor desempeño relativo (57,6%), dado que incorpora un esquema integral aplicable a PRST, PCA, IT y tráfico internacional, promoviendo un modelo homogéneo de identificación y gobernanza del recurso de identificación dentro del ecosistema A2P.

e. Respecto del criterio de costos de cumplimiento para los agentes, este evalúa los costos técnicos, operativos y administrativos que deben asumir PRST, PCA e IT para implementar y mantener la

alternativa. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (60,7%), debido a que no requiere modificaciones regulatorias, adecuaciones tecnológicas ni nuevos procesos de validación o administración de recursos de identificación.

La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño intermedio (25,1%), dado que restringe las exigencias técnicas y operativas únicamente al tráfico transaccional.

Por el contrario, la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» presenta el menor desempeño (14,3%), debido a los costos asociados a la implementación integral del esquema de Sender ID, incluyendo adecuaciones en plataformas SMS-C, procesos de asignación y validación, gestión de gobernanza y mecanismos de trazabilidad.

f. En el subcriterio de costos de supervisión se observa una situación similar al anterior. Este criterio evalúa el nivel de recursos técnicos y administrativos requeridos por la autoridad regulatoria para monitorear, verificar y hacer cumplir las medidas. La alternativa de «Statu Quo» presenta el mayor desempeño (48,9%), dado que mantiene los mecanismos actuales de supervisión sin introducir nuevas cargas regulatorias.

   La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño intermedio (29,2%), mientras que la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» obtiene el menor desempeño relativo (21,9%), debido a la necesidad de supervisar la asignación, uso, recuperación y validación permanente del nuevo recurso de identificación, así como el cumplimiento de obligaciones por parte de múltiples actores del ecosistema.

g. En cuanto al criterio de mitigación de la migración de canales, este evalúa el grado en que las alternativas reducen el incentivo de migrar tráfico hacia canales no regulados como OTT o aplicaciones de mensajería. La alternativa de «Statu Quo» presenta el mayor desempeño relativo (40,2%), debido a que no introduce cargas regulatorias adicionales que puedan incentivar el desplazamiento del tráfico hacia canales alternativos.

   Las alternativas basadas en Sender ID presentan desempeños inferiores. La alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» obtiene una valoración de 30,5%, mientras que la alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño ligeramente menor (29,3%).

   Estos resultados reflejan que la incorporación de nuevas obligaciones regulatorias y mecanismos de validación podría generar incentivos parciales para la migración de tráfico promocional hacia canales OTT u otras plataformas de mensajería.

h. Respecto del criterio de rapidez de despliegue, este evalúa el tiempo requerido para implementar cada alternativa desde su adopción regulatoria hasta su operación efectiva en el mercado. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (55,4%), dado que no requiere implementación de nuevas capacidades técnicas ni procesos regulatorios adicionales.

La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño intermedio (27,1%), debido a que limita el alcance de las adecuaciones técnicas únicamente al tráfico crítico.

Por su parte, la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» presenta el menor desempeño (17,5%), considerando que requiere el desarrollo gradual de adecuaciones técnicas, pilotos, mecanismos de asignación y despliegues progresivos en distintos segmentos del ecosistema.

i. En relación con el criterio de riesgo de implementación, este evalúa el grado de incertidumbre técnica, operativa y de coordinación asociado a la adopción efectiva de las alternativas. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (52,7%), dado que no introduce cambios regulatorios ni dependencias adicionales entre actores del ecosistema.

   La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño intermedio (27,6%), ya que reduce parcialmente las complejidades operativas derivadas del despliegue generalizado de Sender ID.

   Por su parte, la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» presenta el menor desempeño (19,7%), debido a la necesidad de implementar ajustes técnicos homogéneos en redes y plataformas, coordinar múltiples actores nacionales e internacionales y establecer capacidades robustas para la administración del nuevo recurso de identificación.

j. Finalmente, el criterio de necesidad de coordinación evalúa el grado de articulación requerido entre múltiples actores para implementar cada alternativa. La alternativa de «Statu Quo» presenta el mejor desempeño (52,5%), dado que conserva los esquemas actuales sin requerir nuevos mecanismos de coordinación sectorial.

   La alternativa de «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta un desempeño intermedio (26,2%), mientras que la alternativa de «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» obtiene el menor desempeño relativo (21,4%), considerando la necesidad de articular procesos de asignación, validación, administración y supervisión del Sender ID entre PRST, PCA, IT y la CRC.

En síntesis, el análisis multicriterio evidencia que la alternativa «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» presenta el mejor desempeño global entre las alternativas evaluadas, alcanzando un puntaje agregado de 49,5%. Esta alternativa sobresale especialmente en los criterios asociados a efectividad regulatoria, trazabilidad del originador, confianza del usuario y cobertura sobre el ecosistema, debido a que introduce un esquema integral de identificación verificable para todos los remitentes A2P.

No obstante, esta alternativa también implica mayores costos de implementación, mayores requerimientos de supervisión y mayores necesidades de coordinación sectorial frente a las demás alternativas. Por su parte, la alternativa «Statu Quo» presenta ventajas importantes en términos de costos, rapidez y simplicidad de implementación, aunque mantiene las limitaciones actualmente identificadas en materia de autenticidad y trazabilidad del remitente. Finalmente, la alternativa «Asignación y uso de código alfanumérico solo para tráfico transaccional» presenta desempeños

intermedios en la mayoría de los criterios, reflejando un enfoque focalizado que prioriza la protección sobre comunicaciones críticas, aunque con un alcance más limitado frente a un esquema integral de Sender ID.

Conclusión

En consideración de los resultados obtenidos en el análisis multicriterio, la alternativa «Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)» presenta el mejor desempeño global frente a los objetivos perseguidos en la temática de identificación clara del remitente en SMS A2P. Lo anterior, debido a que fortalece de manera significativa la autenticidad y trazabilidad de las comunicaciones, mejora la capacidad de prevención de escenarios de suplantación y contribuye a incrementar la confianza de los usuarios en el canal SMS.

Si bien esta alternativa implica mayores requerimientos de implementación, supervisión y coordinación frente a las demás opciones evaluadas, dichos esfuerzos se encuentran asociados a la adopción de un esquema integral de identificación verificable aplicable de manera transversal al ecosistema A2P. En este sentido, la alternativa permite avanzar hacia condiciones más robustas de transparencia y validación del originador de los mensajes, alineando el funcionamiento del canal SMS con objetivos de mitigación del fraude y fortalecimiento de la protección de los usuarios.

9.2.1.1.5 Propuesta regulatoria «Falta de identificación clara del remitente en SMS A2P»

La materialización de esta propuesta regulatoria implica la creación de un nuevo recurso de identificación que se denominará SENDER ID, que contará con reglas específicas de asignación y operación. Este recurso de identificación será administrado por la CRC e identificará de manera única e inequívoca a la persona natural o jurídica responsable directa por la producción y generación de contenidos o aplicaciones enviados a través de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD).

El SENDER ID es visible para el usuario final en el encabezado del mensaje recibido y permite la identificación clara e inmediata del originador del contenido. A cada persona natural o jurídica que lo solicite y que tenga la intención de usar el canal de SMS para contactar con los usuarios, la CRC le asignará un único SENDER ID para su identificación dentro del sistema luego de cumplir con los requisitos y el procedimiento de asignación.

De manera concreta, se adicionará el Capítulo 12 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, en el cual se especificará el régimen de administración de este nuevo recurso, estableciendo, entre otros aspectos, los requisitos de asignación, las modalidades de contenido en las que se podrá utilizar, las causales específicas de recuperación y, en general, todas las particularidades para su funcionamiento.

Seguidamente se incorpora la propuesta regulatoria:

Adiciónese el Capítulo 12 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, el cual quedará así: **«CAPÍTULO 12**

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

SENDER ID

SECCIÓN 1.
PLANIFICACIÓN Y FUNCIONAMIENTO DEL SENDER ID

ARTÍCULO 6.12.1.1. ESTRUCTURA DEL SENDER ID. El SENDER ID para Colombia es un identificador alfanumérico visible para el usuario final en el encabezado del mensaje recibido. Tendrá una extensión mínima de tres (3) caracteres y máxima de once (11) caracteres alfanuméricos. El Administrador de los Recursos de Identificación mantendrá y publicará en el SIGRI una lista dinámica de los SENDER ID asignados, actualizada en tiempo real a medida que se produzcan nuevas asignaciones. Las denominaciones de SENDER ID sugeridas por los solicitantes podrán ser objeto de evaluación y eventual asignación, siempre que acrediten el cumplimiento de los requisitos técnicos, operativos y regulatorios aplicables que están contenidos en esta resolución.

PARÁGRAFO. El SENDER ID deberá tener relación de manera inequívoca con: (i) la razón social de la persona jurídica; o (ii) el nombre de la persona natural; o (iii) el nombre comercial; o (iv) la marca registrada del asignatario. No se admitirán identificadores que puedan inducir al usuario en error o confusión, que imiten nombres de entidades públicas, financieras u operadores de telecomunicaciones, ni que contengan palabras reservadas por el Administrador de Recursos de Identificación, las cuales serán publicadas y actualizada en el SIGRI de manera dinámica cuando la CRC lo estime necesario por vía de circular.

ARTÍCULO 6.12.1.2. ASIGNATARIOS DEL SENDER ID. Podrán solicitar y ser asignatarios de SENDER ID los agentes responsables directos por la producción y generación de contenidos o aplicaciones enviados a través de SMS y USSD. El asignatario del SENDER ID no será asignatario de código corto A2P, salvo la situación descrita en el Parágrafo 1 del artículo 6.4.1.3. También podrán ser asignatarios:

6.12.1.2.1. Los PCA e IT inscritos en el RPCAI, responsables directos por la producción de contenidos y/o aplicaciones propias.

6.12.1.2.2. Las entidades de la fuerza pública y organismos del Estado cuya función esté orientada a preservar el orden público, el orden constitucional y/o la administración de justicia.

6.12.1.2.3. Los PRST en su condición de PCA, cuando sean responsables directos por la producción de contenidos propios para sus usuarios.

PARÁGRAFO 1. Los agentes que únicamente provean infraestructura de conexión para cursar tráfico de mensajes de texto (SMS) de terceros no podrán ser asignatarios de SENDER ID.

PARÁGRAFO 2. A cada persona natural o jurídica le será asignado un único SENDER ID. La CRC solo asignará un SENDER ID por número de identificación tributaria (NIT) o por cédula de ciudadanía. No podrán existir dos asignatarios distintos con el mismo número de identificación, ni un mismo asignatario con más de un SENDER ID asignado simultáneamente. Los solicitantes extranjeros podrán ser asignatarios siempre que hayan establecido una sucursal en Colombia, en los términos de las disposiciones legales y reglamentarias previstas para el efecto.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ARTÍCULO 6.12.1.3. MODALIDADES DE CONTENIDO QUE SE ASOCIAN AL SENDER ID. Los SENDER ID podrán utilizarse para una o varias de las siguientes modalidades de contenido, conforme a las que el asignatario justifique al momento de la solicitud:

6.12.1.3.1. MENSAJES DE AUTENTICACIÓN Y SEGURIDAD. Son aquellos mensajes cortos de texto A2P destinados exclusivamente a verificar la identidad del usuario o proteger la seguridad de accesos y operaciones. Incluyen, entre otros, los códigos de verificación de un solo uso (OTP) enviados como parte de sistemas de autenticación multifactor, las alertas inmediatas de seguridad sobre inicios de sesión o actividades inusuales en una cuenta, y las confirmaciones de activación o desbloqueo de servicios por parte del usuario.

En virtud de su naturaleza, estos mensajes se generan normalmente a solicitud explícita del usuario o como parte intrínseca de un servicio contratado (por ejemplo, al iniciar sesión en una plataforma o autorizar una transacción sensible), por lo que su envío no requiere un consentimiento adicional expreso del usuario, entendiéndose amparado por la acción u operación que los origina y el vínculo servicio-usuario existente.

6.12.1.3.2. MENSAJES TRANSACCIONALES E INFORMATIVOS. Son los mensajes cortos de texto A2P vinculados a la prestación de un servicio, transacción o relación contractual en curso, cuyo contenido tiene carácter operativo o explicativo y está directamente asociado a acciones o eventos que el usuario espera.

Comprenden, por ejemplo, notificaciones de transacciones bancarias realizadas (avisos de débito o crédito en cuenta), confirmaciones de operaciones o solicitudes (como confirmación de una compra, de una reserva o de una cita), avisos de logística (seguimiento de envíos, entrega de paquetes), recordatorios de pago oportuno o vencimientos, así como otras comunicaciones de servicio al cliente (actualización de saldos, cambios de condiciones, mensajes de cobranza bajo un contrato vigente).

En estos casos, el consentimiento del usuario se entiende implícito o derivado de la relación contractual o la solicitud previa que soporta la comunicación, es decir, el usuario ha proporcionado su número dentro del contexto del servicio o transacción, autorizando estas notificaciones necesarias para la correcta ejecución del servicio.

6.12.1.3.3. MENSAJES COMERCIALES O PUBLICITARIOS. Son los mensajes cortos de texto A2P con fines de promoción, mercadeo o publicidad, dirigidos a ofrecer, difundir o incentivar la contratación de bienes, servicios, eventos o programas de fidelización a los usuarios finales.

Esta categoría incluye, por ejemplo, las campañas de publicidad o promociones enviadas por empresas (descuentos, anuncios de nuevos productos, invitaciones a eventos comerciales), los mensajes de mercadeo directo para la captación de clientes o ventas, las encuestas de satisfacción con carácter comercial, así como cualquier otra comunicación cuyo objetivo principal sea publicitario o de telemercadeo (fidelización, branding, posicionamiento de marca, etc.).

Dado su carácter no solicitado dentro de una transacción específica, estos mensajes requieren el consentimiento expreso previo del usuario (opt-in), otorgado de forma libre, específica e informada, para ser enviados de conformidad con la normativa de protección de datos y

protección al usuario vigente. En particular, el remitente debe contar con una autorización clara del destinatario para recibir comunicaciones comerciales por este medio, y es responsable de respetar las preferencias del usuario sobre no recepción de publicidad en línea con las reglas de la inscripción del número que el usuario haya realizado en el Registro de Números Excluidos – RNE.

6.12.1.3.4. MENSAJES REGULATORIOS Y DE INTERÉS PÚBLICO. Son aquellos mensajes cortos de texto A2P cuyo envío responde a obligaciones legales, regulatorias o a finalidades de interés general, y no tienen un propósito comercial ni obedecen a una solicitud individual del usuario sino al cumplimiento de un deber normativo o la protección del bienestar público.

Esta categoría abarca, entre otros, los mensajes exigidos por la regulación sectorial a los proveedores de servicios (por ejemplo, notificaciones que un operador móvil debe enviar obligatoriamente sobre activación de servicios, confirmación de recargas, consumos de datos o condiciones tarifarias, de acuerdo con la normativa vigente), las alertas oficiales de emergencia o gestión del riesgo emitidas por organismos gubernamentales (tales como avisos de desastres naturales, seguridad ciudadana o salud pública), las comunicaciones masivas de carácter institucional (por ejemplo, campañas de servicio público, información de beneficios sociales a poblaciones vulnerables) y, en general, las notificaciones institucionales o administrativas que las entidades públicas o privadas deban remitir a los usuarios en virtud de normas específicas.

Estos mensajes se emiten sin requerir consentimiento previo del usuario, ya que su envío está justificado en un mandato normativo expreso o en razones de interés público esencial. Por tanto, pueden enviarse incluso a usuarios que hayan manifestado su preferencia de no recibir comunicaciones comerciales, dado que no persiguen fines publicitarios sino el cumplimiento de un deber legal o la difusión de información relevante para la colectividad.

PARÁGRAFO. Un mismo SENDER ID podrá utilizarse para más de una modalidad siempre que exista una plantilla de contenido independiente aprobada por el validador centralizado para cada modalidad, y que el asignatario haya acreditado ante el validador el cumplimiento de las condiciones aplicables a cada una. El asignatario de SENDER ID podrá solicitar ante el Administrador de Recursos de Identificación la modificación de la asignación del respectivo recurso de identificación, con la finalidad de adicionar o eliminar modalidades de contenido asociadas al respectivo SENDER ID.

SECCIÓN 2.
ASIGNACIÓN DEL SENDER ID

ARTÍCULO 6.12.2.1. REQUISITOS PARA LA ASIGNACIÓN DEL SENDER ID. El asignatario del código corto A2P, vinculado al solicitante del SENDER ID, remitirá al Administrador de Recursos de Identificación, en nombre y representación del solicitante del SENDER ID, a través del trámite unificado de recursos de identificación, la siguiente información:

6.12.2.1.1. Constancia de inscripción previa del futuro asignatario del SENDER ID en el RPCAI como PCA. Los solicitantes extranjeros podrán ser asignatarios siempre que hayan establecido una sucursal en Colombia, en los términos de las disposiciones legales y reglamentarias previstas para el efecto.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.12.2.1.2. Sugerencia del SENDER ID solicitado y que requiere ser asignado, con indicación detallada de la modalidad o modalidades de contenido para las cuales se solicita su uso, con la justificación de cada una de ellas.

6.12.2.1.3. Soporte del derecho al uso del identificador alfanumérico mediante alguno de los siguientes documentos: certificado de registro de marca ante la SIC; certificado de existencia y representación legal que acredite que la razón social o nombre comercial corresponde al identificador solicitado; matrícula mercantil y, para el caso de personas naturales, cédula de ciudadanía. Para entidades del numeral 6.12.1.2.2. de esta resolución, el acto de creación o acto que acredite su denominación oficial.

6.12.2.1.4. Descripción del servicio o servicios a prestar por cada modalidad solicitada, incluyendo: indicación de si es contenido, aplicación o ambos; descripción del contenido y propósito de cada tipo de comunicación; procedimiento de interacción con el usuario y mecanismo de obtención del consentimiento por modalidad; forma de pago si no es gratuito; y medidas de control para prevenir fraudes.

6.12.2.1.5. Identificación del código corto A2P del agente solicitante, con acreditación de que está asignado e implementado en el SIGRI y que existe contrato vigente entre el asignatario del código corto A2P y el potencial asignatario del SENDER ID.

6.12.2.1.6. Certificado de existencia y representación legal vigente del asignatario del código corto A2P, expedido con no más de noventa (90) días.

6.12.2.1.7. Certificado de existencia y representación legal vigente del potencial asignatario del SENDER ID, expedido con no más de noventa (90) días, en caso de que se trate de una persona jurídica.

6.12.2.1.8. Certificación del validador centralizado conforme al Capítulo 13 del Título VI de esta resolución, en la que conste el cumplimiento del KYC por parte del asignatario del código corto A2P respecto del potencial asignatario del SENDER ID, la acreditación del contrato vigente y la validación de la información comercial y técnica del servicio por cada modalidad solicitada.

6.12.2.1.9. Cualquier otra información que el solicitante considere pertinente.

PARÁGRAFO 1. Cuando el asignatario del SENDER ID sea a su vez asignatario de código corto A2P conforme al Parágrafo 1 del artículo 6.4.1.3, podrá presentar directamente la solicitud adaptando los requisitos.

PARÁGRAFO 2. Para las entidades del numeral 6.12.1.2.2. de esta resolución, el requisito de inscripción en el RPCAI no es exigible y podrán presentar directamente la solicitud ante el Administrador de Recursos de Identificación.

ARTÍCULO 6.12.2.2. PROCEDIMIENTO DE ASIGNACIÓN DEL SENDER ID. Una vez presentada la solicitud conforme al artículo 6.12.2.1, el Administrador de Recursos de Identificación resolverá en quince (15) días hábiles conforme al siguiente procedimiento:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.12.2.2.1. Se verificará que la solicitud cumpla con todos los requisitos del artículo 6.12.2.1. Si no los cumple, se negará la asignación.

6.12.2.2.2. Se verificará que el código corto A2P está asignado e implementado, y que el contrato entre el asignatario del código corto A2P y el potencial asignatario del SENDER ID está vigente.

6.12.2.2.3. Se verificará que en el año anterior no se recuperó al potencial asignatario un SENDER ID por los numerales 6.12.3.2.5., 6.12.3.2.6., 6.12.3.2.7. o 6.12.3.2.12. del artículo 6.12.3.2. Si hubo recuperación por esas causales, se negará la asignación.

6.12.2.2.4. Se verificará que el identificador alfanumérico no corresponde a uno ya asignado en el SIGRI, ni a una denominación engañosa conforme al Parágrafo del artículo 6.12.1.1. En caso de homonimia total se negará. En caso de similitud, que a juicio de la CRC pueda ser considerada engañosa o confusa, se requerirá un identificador alternativo.

6.12.2.2.5. Se verificará que el solicitante no cuenta con un SENDER ID asignado en el SIGRI bajo el mismo número de identificación tributaria (NIT) o cédula de ciudadanía. Si existe un SENDER ID asignado para ese número de identificación, se negará la asignación.

6.12.2.2.6. Se verificará que la descripción del servicio es consistente con la modalidad o modalidades de contenido solicitadas y con la justificación presentada conforme al numeral 6.12.2.1.2. de esta resolución.

6.12.2.2.7. Se llevará a cabo el análisis de las solicitudes según orden de llegada y justificación presentada.

6.12.2.2.8. Se verificará la disponibilidad en el SIGRI del SENDER ID solicitado. Si se cumplen todos los requisitos, el estado del SENDER ID solicitado pasará a «Preasignado».

6.12.2.2.9. Cumplidos los pasos anteriores, se procederá con la expedición del acto administrativo de asignación y se cambiará el estado del SENDER ID a «Asignado» en el SIGRI, una vez quede en firme dicho acto administrativo.

PARÁGRAFO. El término de quince (15) días hábiles se suspende cuando se requiera información adicional o cuando se requiera al solicitante proponer un identificador alternativo.

SECCIÓN 3.
USO DEL SENDER ID

ARTÍCULO 6.12.3.1. CRITERIOS DE USO EFICIENTE. El Administrador de Recursos de Identificación verificará el uso eficiente del SENDER ID en observancia de los siguientes criterios:

6.12.3.1.1. Cumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6. de esta resolución.

6.12.3.1.2. Cumplimiento de las obligaciones especiales del asignatario del SENDER ID establecidas en el Capítulo 13 del TÍTULO VI de esta resolución.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.12.3.1.3. El SENDER ID debe ser implementado en un término máximo de seis (6) meses desde la firmeza del acto de asignación.

6.12.3.1.4. El SENDER ID implementado no deberá reportar ausencia de tráfico en períodos consecutivos iguales o superiores a seis (6) meses.

6.12.3.1.5. El asignatario deberá mantener vigente en todo momento al menos una relación contractual con un asignatario de código corto A2P con conexión directa operativa a un PRST, salvo que él mismo sea el asignatario de código corto A2P.

6.12.3.1.6. A través del SENDER ID únicamente podrán enviarse mensajes correspondientes a las modalidades para las que fue asignado conforme a la solicitud del artículo 6.12.2.1.2. de esta resolución, respaldados por una plantilla previamente aprobada y vigente en el sistema del validador centralizado.

6.12.3.1.7. A través del SENDER ID no podrán enviarse mensajes en nombre de terceros distintos al asignatario.

6.12.3.1.8. El asignatario deberá mantener actualizada su información en el RPCAI y en la respectiva matrícula mercantil que proporciona información al RUES.

6.12.3.1.9. El asignatario deberá completar la validación anual ante el validador centralizado conforme al artículo 6.12.3.3 de la presente resolución. El incumplimiento de esta obligación dentro del plazo establecido constituirá un uso ineficiente y dará lugar al inicio del procedimiento de recuperación conforme al artículo 6.1.1.8. de esta resolución.

ARTÍCULO 6.12.3.2. CAUSALES DE RECUPERACIÓN DEL SENDER ID. El Administrador de Recursos de Identificación podrá recuperar el SENDER ID conforme al artículo 6.1.1.8 cuando el asignatario incumpla los criterios del artículo 6.12.3.1 o incurra en las siguientes causales:

6.12.3.2.1. Incumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6.

6.12.3.2.2. Incumplimiento de las obligaciones especiales del asignatario del SENDER ID establecidas en el Capítulo 13 del TÍTULO VI de esta resolución.

6.12.3.2.3. No implementación dentro de los seis (6) meses siguientes a la firmeza del acto de asignación.

6.12.3.2.4. Ausencia de tráfico durante seis (6) meses consecutivos.

6.12.3.2.5. Uso diferente al declarado al momento de la solicitud, incluyendo mensajes cuyo contenido no corresponda a ninguna modalidad para la que fue solicitado el SENDER ID conforme al numeral 6.12.2.1.2, o sin respaldo de plantilla aprobada y vigente.

6.12.3.2.6. Envío de mensajes en nombre de terceros distintos al asignatario.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.12.3.2.7. Envío de mensajes a usuarios inscritos en el RNE cuyo envío no haya sido autorizado conforme a la modalidad de contenido de la plantilla previamente aprobada.

6.12.3.2.8. Establecimiento, mediante decisión ejecutoriada, de incumplimiento de disposiciones en materia de protección de datos personales o propiedad intelectual.

6.12.3.2.9. Imposibilidad de continuar ejerciendo su objeto social, incluyendo liquidación judicial o voluntaria, o cancelación de matrícula mercantil.

6.12.3.2.10. Razones de interés general o seguridad nacional.

6.12.3.2.11. Modificación, por parte del Administrador de Recursos de Identificación, de una modalidad de contenido que haga incompatible el uso del SENDER ID para dicha modalidad.

6.12.3.2.12. Envío de mensajes de texto (SMS) que potencialmente pueden ser atribuibles al mal uso de las plantillas y que sea imputable al asignatario del SENDER ID conforme al artículo 6.13.4.4 de la presente resolución.

6.12.3.2.13. Incumplimiento injustificado de la validación anual establecida en el artículo 6.12.3.3. de esta resolución dentro del plazo establecido para su realización.

PARÁGRAFO 1. La recuperación del SENDER ID genera efectos sobre todas las plantillas activas vinculadas al mismo. Simultáneamente con el inicio del procedimiento, cuando la causal de recuperación sea la de los numerales 6.12.3.2.5., 6.12.3.2.6., 6.12.3.2.7. o 6.12.3.2.12. del artículo 6.12.3.2, la CRC podrá ordenar al validador centralizado la suspensión inmediata de todas las plantillas activas vinculadas al SENDER ID. Una vez en firme el acto de recuperación, todas las plantillas asociadas deberán quedar desactivadas y no se podrán enviar mensajes mediante dicho SENDER ID.

PARÁGRAFO 2. La recuperación del SENDER ID no implica automáticamente la recuperación del código corto A2P, salvo que el motivo configure también una causal de recuperación del código corto A2P.

ARTÍCULO 6.12.3.3. VALIDACIÓN ANUAL DEL SENDER ID. El asignatario del SENDER ID deberá completar una validación anual ante el validador centralizado para mantener vigente el derecho al uso del recurso. Esta validación se realizará dentro de los treinta (30) días hábiles anteriores al vencimiento de cada año contado desde la firmeza del acto de asignación o desde la última validación exitosa. La validación anual comprende como mínimo:

6.12.3.3.1. Confirmación de la vigencia de la relación contractual con el asignatario del código corto A2P.

6.12.3.3.2. Actualización de la información del KYC conforme al artículo 6.13.3.2 de la presente resolución.

6.12.3.3.3. Revisión y confirmación o actualización de las modalidades de contenido para las cuales se utiliza el SENDER ID, con acreditación del cumplimiento de las condiciones aplicables a cada una.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.12.3.3.4. Confirmación de que las plantillas activas vinculadas al SENDER ID corresponden a las comunicaciones efectivamente enviadas, con actualización o desactivación de aquellas que ya no se utilicen.

PARÁGRAFO. Si el asignatario no completa la validación dentro del plazo establecido, el validador centralizado notificará al Administrador de los Recursos de Identificación, quien iniciará el procedimiento de recuperación conforme al artículo 6.1.1.8. de esta resolución»

9.2.1.2 Subtemática 2: Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude

Situación identificada:	El ecosistema de comunicaciones Application to Person (A2P) presenta debilidades estructurales que obstaculizan la trazabilidad y la asignación de responsabilidades en caso de fraude. Por una parte, opera un mercado informal con originadores de contenido sin controles homogéneos ni verificaciones previas, lo que facilita la suplantación de identidad y el envío de mensajes no autorizados en nombre de terceros. Por otra, la cadena de valor carece de puntos de control claros para imputar responsabilidades cuando se perjudica al usuario, pues no existen identificadores estandarizados y verificables que vinculen, de punta a punta, al agregador, la marca y la campaña con el contenido efectivamente cursado.
Causas relacionadas:	Causa 1: Los desarrollos regulatorios sobre recursos de identificación se han enfocado en su mayoría en la administración y el uso eficiente de dichos recursos escasos. Causa 2: Las medidas de gestión y control frente al contacto fraudulento implementadas por los PRST y asignatarios son insuficientes.
Alternativa 1: Statu quo	No se introducen cambios regulatorios. Se mantiene el esquema actual, en el que los operadores y agregadores gestionan el tráfico A2P sin un proceso formal, uniforme y obligatorio de validación de remitentes, marcas y campañas, con obligaciones generales orientadas a implementar herramientas tecnológicas adecuadas que permitan prevenir la comisión de fraudes al interior de sus redes.
Alternativa 2: Proceso de validación centralizado de originadores de contenido	Establece un proceso centralizado administrado por un tercero para validar agregadores, marcas y campañas antes de cursar tráfico A2P. Incluye: • Medida 1: Obligación de KYC para agregadores (verificación de legitimidad y contratos formales). • Medida 2: Validación centralizada con asignación de Código Corto A2P, Sender_ID y Template_ID para plantillas aprobadas. • Medida 3: Bloqueo obligatorio de mensajes sin identificadores válidos o marcado opcional como «sin verificar» o «probable estafa». • Medida 4: Categorización del contenido (transaccional, promocional, implícito, explícito, gobierno) y articulación con el RNE para consentimiento. • Medida 5: Parámetros para monitoreo de tráfico por agregadores, detectando mensajes sospechosos en tránsito.

Alternativa 3: Proceso de validación distribuido (DLT) de originadores de contenido	Establece un proceso de validación distribuido soportado en tecnología blockchain (DLT), para garantizar inmutabilidad y auditoría descentralizada, a fin de verificar agregadores, marcas y campañas antes de cursar tráfico A2P. Incluye: • Medida 1: KYC obligatorio para agregadores (verificación de legitimidad y contratos formales). • Medida 2: Validación distribuida en DLT con registro de Código Corto A2P, Sender_ID y Template_ID. • Medida 3: Obligación de bloqueo o marcado de tráfico no autorizado. • Medida 4: Categorización del contenido y consentimiento articulado con el RNE. • Medida 5: Monitoreo de tráfico por agregadores con telemetría distribuida para correlación de riesgos.
Alternativa 4: Identificación exclusiva mediante códigos cortos y numeración E.164	Asigna a cada marca un código corto o número E.164 exclusivo (NDC 940) para mejorar la identificación, pero sin validación preventiva. Incluye: • Medida 1: Asignación de recursos exclusivos para las marcas (códigos cortos o E.164). • Medida 2: Categorización del contenido y consentimiento articulado con el RNE. • Medida 3: KYC obligatorio para agregadores (verificación de legitimidad y contratos formales). • Medida 4: Parámetros para monitoreo de tráfico por agregadores. • Medida 5: Obligación de bloqueo o marcado de mensajes sospechosos.

9.2.1.2.1 Alternativa 1: Statu quo

Bajo esta alternativa no se introducen cambios regulatorios. Se mantiene el esquema actual, en el que los operadores y agregadores gestionan el tráfico A2P sin un proceso formal, uniforme y obligatorio de validación de remitentes, marcas y campañas. Aunque evita costos inmediatos de adopción y fricciones operativas, perpetúa los incentivos al mercado informal, preserva asimetrías de información y mantiene las dificultades para obtener la trazabilidad completa de la comunicación, lo que dificulta la prevención, la respuesta oportuna ante incidentes y la judicialización de responsables.

9.2.1.2.2 Medidas transversales presentes en las alternativas 2, 3 y 4

9.2.1.2.2.1 Conocimiento del cliente (KYC) obligatorio para IT

Los IT deben asegurarse de que sus clientes sean empresas reales y legítimas. Esto se hace mediante un proceso llamado «Conozca a su Cliente» (KYC), donde el IT revisa la documentación de constitución de la empresa y certifica que se trata de una empresa válida y legalmente constituida, para luego formalizar un contrato por escrito.

Para efectos de cumplir con lo anterior, se deberán revisar el certificado de existencia y representación legal de las empresas con las cuales tendrán una relación contractual para verificar que la matricula mercantil esté vigente.

Además, se deberán adoptar medidas de debida diligencia que permitan, entre otras finalidades, identificar los beneficiarios finales, teniendo en cuenta como mínimo los siguientes criterios:

1. Identificar la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico.

2. Identificar los beneficiarios finales y la estructura de titularidad y control de la persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico. Para el anterior efecto, los IT deberán solicitar el diligenciamiento del formato que se creará para efectos de identificar al beneficiario final.

3. Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico.

4. Realizar una debida diligencia de manera continua del negocio jurídico celebrado, examinando las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones sean consistentes con el conocimiento de la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se realiza el negocio jurídico, su actividad comercial, perfil de riesgo y fuente de los fondos.

Los agregadores deben conservar la información obtenida en aplicación del principio de debida diligencia durante el tiempo que dure el negocio jurídico, y al menos durante los cinco años siguientes contados a partir de la terminación del respectivo contrato. Esta información deberá ser proporcionada a la CRC en caso de ser solicitada.

Esta medida es útil porque de esta forma se evita que empresas fantasma o delincuentes usen el canal de SMS para enviar mensajes fraudulentos, y el efecto de su aplicación se vería reflejado en que solo empresas verificadas pueden enviar campañas de SMS, cerrando la puerta al fraude desde el inicio, es decir, de manera preventiva.

En este contexto, por efecto de esta medida los IT deberán verificar la legitimidad de sus clientes (marcas) y formalizar contratos por escrito que definan de forma expresa responsabilidades, alcances, uso permitido de recursos de identificación y obligaciones de cumplimiento. Este conocimiento del cliente (KYC) se integra como requisito previo para acceder al sistema de validación y constituye la primera barrera contra el uso indebido del canal de mensajes cortos de texto tradicionales y de los recursos de identificación asociados.

9.2.1.2.2.2 Bloqueo o marcado por parte del PRSTM de tráfico no autorizado

Para que la medida de un validador pueda ser efectiva, los PRSTM deben revisar que cada mensaje contenga el paquete de identificadores válidos. Si no los tiene, o si encuentra alguna inconsistencia en ellos, podría proceder con su bloqueo o con el marcado del mensaje como «sin verificar» enviándolo de esta manera con una alerta expresa para el usuario.

Esto resulta útil porque se ejercerán controles estrictos a través de las redes de los PRSTM que permitirán que los usuarios reciban solo mensajes confiables, y en caso de llegar alguna comunicación sospechosa, puedan identificarla fácilmente y evitar caer en el fraude.

El efecto esperado de esta medida es que se reduzca drásticamente la llegada de mensajes con fines fraudulentos, y que se alerte al usuario sobre posibles riesgos.

En este sentido, de manera específica los PRSTM deberán verificar, previo al enrutamiento, que cada mensaje cuente con el respectivo Código Corto A2P, Sender_ID y Template_ID válidos y habilitados. En ausencia de alguno de estos identificadores, o de su habilitación por parte del validador, el mensaje debe bloquearse.

Alternativamente, para no restringir el tráfico, se podrá permitir el paso del SMS no conforme, marcándolo obligatoriamente con una etiqueta alfanumérica informativa (p. ej., «sin verificar») o de riesgo (p. ej., «probable estafa»), para que todos los mensajes no verificados se encaminen a un buzón único en el teléfono del usuario similar al spam, alertándolo de este modo con el contenido de ese mensaje.

9.2.1.2.2.3 Categorización del contenido y consentimiento del usuario (articulación con RNE)

Con el fin de generar una clasificación de los mensajes acorde con el contenido remitido, y con ello aportar más información y control sobre las comunicaciones recibidas por los usuarios mediante SMS, esta medida propone que los mensajes se clasifiquen según su propósito. Además, con esta medida se busca que se respete de manera más efectiva el consentimiento del usuario para recibir comunicaciones comerciales. Por ejemplo, los mensajes promocionales y publicitarios solo se enviarían si el usuario no está inscrito en el Registro de Números Excluidos (RNE) de la CRC.

Esta medida es útil porque genera un mecanismo más expedito para que los usuarios no reciban publicidad no deseada mediante SMS, y que los mensajes importantes (como alertas de seguridad, mensajes OTP o notificaciones de entidades financieras) lleguen sin restricciones.

El efecto de esta medida es que se tendría un mayor control sobre qué tipo de mensajes recibe el usuario, y de esa forma se protege su privacidad y sus derechos de una manera más efectiva.

Esta medida adopta una clasificación estándar del contenido y su relación con el consentimiento del usuario, así:

- **MENSAJES DE AUTENTICACIÓN Y SEGURIDAD.** Son aquellos mensajes cortos de texto A2P destinados exclusivamente a verificar la identidad del usuario o proteger la seguridad de accesos y operaciones. Incluyen, entre otros, los códigos de verificación de un solo uso (OTP) enviados como parte de sistemas de autenticación multifactor, las alertas inmediatas de seguridad sobre inicios de sesión o actividades inusuales en una cuenta, y las confirmaciones de activación o desbloqueo de servicios por parte del usuario.

En virtud de su naturaleza, estos mensajes se generan normalmente a solicitud explícita del usuario o como parte intrínseca de un servicio contratado (por ejemplo, al iniciar sesión en una plataforma o autorizar una transacción sensible), por lo que su envío no requiere un consentimiento adicional expreso del usuario, entendiéndose amparado por la acción u operación que los origina y el vínculo servicio-usuario existente.

- **MENSAJES TRANSACCIONALES E INFORMATIVOS.** Son los mensajes cortos de texto A2P vinculados a la prestación de un servicio, transacción o relación contractual en curso, cuyo contenido tiene carácter operativo o explicativo y está directamente asociado a acciones o eventos que el usuario espera.

  Comprenden, por ejemplo, notificaciones de transacciones bancarias realizadas (avisos de débito o crédito en cuenta), confirmaciones de operaciones o solicitudes (como confirmación de una compra, de una reserva o de una cita), avisos de logística (seguimiento de envíos, entrega de paquetes), recordatorios de pago oportuno o vencimientos, así como otras comunicaciones de servicio al cliente (actualización de saldos, cambios de condiciones, mensajes de cobranza bajo un contrato vigente).

  En estos casos, el consentimiento del usuario se entiende implícito o derivado de la relación contractual o la solicitud previa que soporta la comunicación, es decir, el usuario ha proporcionado su número dentro del contexto del servicio o transacción, autorizando tácitamente estas notificaciones necesarias para la correcta ejecución del servicio.

- **MENSAJES COMERCIALES O PUBLICITARIOS.** Son los mensajes cortos de texto A2P con fines de promoción, mercadeo o publicidad, dirigidos a ofrecer, difundir o incentivar la contratación de bienes, servicios, eventos o programas de fidelización a los usuarios finales.

  Esta categoría incluye, por ejemplo, las campañas de publicidad o promociones enviadas por empresas (descuentos, anuncios de nuevos productos, invitaciones a eventos comerciales), los mensajes de mercadeo directo para la captación de clientes o ventas, las encuestas de satisfacción con carácter comercial, así como cualquier otra comunicación cuyo objetivo principal sea publicitario o de telemercadeo (fidelización, branding, posicionamiento de marca, etc.).

  Dado su carácter no solicitado dentro de una transacción específica, estos mensajes requieren el consentimiento expreso previo del usuario (opt-in), otorgado de forma libre, específica e informada, para ser enviados de conformidad con la normativa de protección de datos y protección al usuario vigente. En particular, el remitente debe contar con una autorización clara del destinatario para recibir comunicaciones comerciales por este medio, y es responsable de respetar las preferencias del usuario sobre no recepción de publicidad (por ejemplo, la inscripción del número que el usuario haya realizado en el Registro de Números Excluidos –RNE).

- **MENSAJES REGULATORIOS Y DE INTERÉS PÚBLICO.** Son aquellos mensajes cortos de texto A2P cuyo envío responde a obligaciones legales, regulatorias o a finalidades de interés general, y no tienen un propósito comercial ni obedecen a una solicitud individual del usuario sino al cumplimiento de un deber normativo o la protección del bienestar público.

Esta categoría abarca, entre otros, los mensajes exigidos por la regulación sectorial a los proveedores de servicios (por ejemplo, notificaciones que un operador móvil debe enviar obligatoriamente sobre activación de servicios, confirmación de recargas, consumos de datos o condiciones tarifarias, de acuerdo con la normativa vigente), las alertas oficiales de emergencia o gestión del riesgo emitidas por organismos gubernamentales (tales como avisos de desastres naturales, seguridad ciudadana o salud pública), las comunicaciones masivas de carácter institucional (por ejemplo, campañas de servicio público, información de beneficios sociales a poblaciones vulnerables) y, en general, las notificaciones institucionales o administrativas que las entidades públicas o privadas deban remitir a los usuarios en virtud de normas específicas.

Estos mensajes se emiten sin requerir consentimiento previo del usuario, ya que su envío está justificado en un mandato normativo expreso o en razones de interés público esencial. Por tanto, pueden enviarse incluso a usuarios que hayan manifestado su preferencia de no recibir comunicaciones comerciales, dado que no persiguen fines publicitarios sino el cumplimiento de un deber legal o la difusión de información relevante para la colectividad.

9.2.1.2.2.4 Definición de reglas de monitoreo de tráfico por IT

Esta medida pretende que los IT usen herramientas de monitoreo que analicen en tiempo real el comportamiento del tráfico enviado por las marcas que han contratado sus servicios, incluyendo los enlaces incluidos y los patrones de envío. Si detectan algo sospechoso (por ejemplo, un enlace malicioso, un patrón atípico o un volumen inusual de mensajes), pueden bloquear el mensaje o marcarlo como riesgoso. Es importante aclarar que este monitoreo de ninguna manera implica la violación a la privacidad de la información de los usuarios o a la obtención de sus datos personales.

Esta medida es útil y necesaria ya que permite detectar y detener campañas fraudulentas antes de que puedan llegar a los usuarios, y el efecto que produciría es crear una red de vigilancia por parte de los IT, que protege a los usuarios y facilita la investigación de fraudes por parte de las autoridades competentes.

Con el anterior contexto, esta medida de manera específica establece la obligación para los IT de implementar herramientas de monitoreo proactivo del tráfico A2P, alineadas con parámetros internacionales y adaptadas a la regulación nacional. Estas herramientas deberán permitir la detección temprana de patrones anómalos y la intervención preventiva antes de que los mensajes lleguen al usuario.

Las características y parámetros mínimos que debería tener en cuenta el monitoreo por parte de los IT son:

- **Filtrado de enlaces:** Análisis en tiempo real de las URL declaradas en las plantillas e incluidas en los mensajes, comparándolas con listas negras dinámicas para bloquear enlaces maliciosos o sospechosos.
- **Etiquetado y marcado de riesgo:** Mensajes que no cumplan con los requisitos de validación (Código Corto A2P, Sender_ID, Template_ID), o que presenten indicadores de fraude, deberán ser marcados con etiquetas visibles para el usuario, tales como «sin verificar» o «probable estafa».

- **Listas blancas dinámicas:** Sincronización periódica con el registro central para garantizar que solo se cursen mensajes provenientes de remitentes y plantillas autorizadas.
- **Análisis de comportamiento:** Monitoreo de volumen, frecuencia de envío, velocidad de entrega y correlación con reportes de fraude para identificar patrones inusuales.
- **Auditoría y trazabilidad:** Registro detallado de eventos de validación, bloqueos y alertas, disponible para las autoridades competentes en caso de investigación.
- **Interoperabilidad con operadores y otros IT:** Los IT deberán exponer APIs seguras para compartir señales de riesgo con los PRSTM, permitiendo así la activación de bloqueos coordinados en red.

9.2.1.2.3 Alternativa 2: Proceso de validación centralizado de originadores de contenido

Actualmente, los PCA e IT pueden enviar mensajes masivos sin un mecanismo unificado que verifique la legitimidad del remitente ni controle de forma homogénea las campañas, lo cual facilita el *smishing* y la suplantación dado que los usuarios no pueden distinguir mensajes legítimos de fraudulentos.

En ese contexto, esta alternativa contempla la aplicación del conjunto de medidas transversales para esta temática (descrito en la sección 9.2.1.2.2), articuladas con un proceso centralizado de validación de los originadores de contenidos administrado por un tercero (validador) donde todo originador de mensajería A2P debe registrarse y validar previamente sus datos (identidad de la empresa, tipo de campaña, contenido básico y, si incluye URLs, dominio de destino, etc). Una vez validado, al originador de contenido le es asignado un identificador único (alfanumérico o numérico) para sus envíos, es decir, cada campaña de mensajería masiva y remitente autorizado obtienen un identificador (ID) registrado.

El proceso se basa en la asignación de identificadores únicos para cada nivel, así:

- Un **Código Corto A2P** para los PCA o IT validados. Para estos efectos, se cambiará la forma en la que actualmente funcionan los códigos cortos para que, en su lugar, luego de un periodo de transición definido, este recurso de identificación comience a identificar de manera única a personas naturales y jurídicas en el ecosistema A2P.

- Un **Sender_ID** para las marcas validadas. El SENDER ID correspondería a un recurso de identificación administrado por la CRC, que identifica de manera única e inequívoca al responsable directo por la producción y generación de contenidos o aplicaciones enviados a través de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD).

  El SENDER ID es visible para el usuario final en el encabezado del mensaje recibido, en sustitución de un código numérico, y permite la identificación clara e inmediata del originador del contenido. Para materializar lo anterior, se incluiría un nuevo capítulo en el TÍTULO VI de la Resolución CRC 5050 de 2016 en el que se regula la estructura del SENDER ID, los requisitos para su asignación, el trámite para su asignación, el marco regulatorio de su uso y las respectivas causales de recuperación de este nuevo recurso de identificación. El SENDER ID podrá cubrir una o más modalidades de contenido, siempre que para cada una de ellas exista un TEMPLATE ID independiente debidamente validado.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Un **Template_ID** para las plantillas de contenido de campañas validadas y aprobadas. El Template ID no correspondería a un recurso de identificación administrado por la CRC, sino que sería un formato que se presenta ante el validador para que identifique de manera única e inequívoca una plantilla de contenido para ser cursada a través de un SENDER ID determinado.

  El TEMPLATE ID vincula de manera trazable e inmodificable el contenido base del mensaje, la modalidad de contenido aplicable, el SENDER ID del originador y, cuando corresponda, las URLs o dominios de destino autorizados para su inclusión en el mensaje. Ningún mensaje A2P podrá ser cursado a través de las redes de los PRST si no está respaldado por un TEMPLATE ID validado por el tercero.

Los roles que intervendrían en el proceso son los siguientes:

- **El validador central**: administra el registro, revisa documentación (KYC) y aprueba solicitudes para que los PCA e IT envíen la solicitud de asignación de identificadores a la CRC. Este tercero será seleccionado y financiado por los asignatarios del nuevo código corto A2P y tendrá a su cargo la administración, gestión e integridad del proceso de validación de los agentes, marcas y plantillas de contenido que participan en el ecosistema de tráfico A2P, incluyendo la verificación del proceso de conocimiento del cliente (KYC) adelantado por los asignatarios del Código Corto A2P respecto de los potenciales asignatarios del SENDER ID, la aprobación de las plantillas de contenido que darán lugar a la asignación de TEMPLATE ID, y la emisión de las certificaciones requeridas en el proceso de asignación de los recursos de identificación Código Corto A2P y SENDER ID. La actuación del validador centralizado se enmarca en los lineamientos regulatorios que para el efecto expida la CRC y bajo la supervisión permanente del Administrador de los Recursos de Identificación.
- **Los IT**: Se registran en el validador central e inscriben los PCA y sus campañas, garantizando la veracidad de la información y cumpliendo con el conocimiento de su cliente (KYC). Una vez obtienen autorización del validador, remiten solicitud de recursos de identificación a la CRC.
- **Los PCA**: Se registran a través de los IT ante el validador, definen las plantillas con el contenido base y la clasificación de sus campañas.
- **CRC**: Asigna los recursos de identificación.
- **PRSTM**: verifican en tiempo real que cada mensaje tenga identificadores válidos antes de cursarlo, y realizar el bloqueo o marcado del mensaje cuando esta condición no se cumpla.

El proceso de validación consistiría en la aplicación de los siguientes pasos:

Validación de IT. Cada IT se inscribe ante el validador y remite la documentación requerida. El validador verifica la información oficial y, de ser conforme, emite una certificación. En caso de no ser conforme, solicitará las aclaraciones que considere pertinentes hasta tener la verificación de la información oficial requerida, antes de que la CRC asigne el código corto A2P.

Validación de PCA. Una vez inscritos y validados, los IT proceden con la inscripción de los PCA registrados que originarán contenido. El validador revisa la documentación del PCA y el contrato suscrito con el IT. Si todo es conforme, otorga una certificación para que se pueda asignar una identificación del PCA (Sender_ID) que se utilizará como remitente alfanumérico visible para el usuario a la hora de recibir el mensaje de texto. La vigencia del Sender ID será limitada y requerirá de una

renovación periódica, para la cual se definirá la frecuencia específica, a fin de validar la información registrada y la operatividad de la marca.

Validación de campañas. Cuando el PCA tiene su correspondiente validación en el sistema, define el contenido base de cada campaña, con posibilidad de añadir etiquetas variables, y asigna una clasificación conforme al catálogo regulatorio. El PCA registra la plantilla ante el validador, quien corrobora la clasificación, y la aprueba o rechaza. Si aprueba, emite un certificado que le permitirá al PCA obtener un identificador de plantilla (Template_ID) que vincula campaña, remitente y la estructura del contenido autorizado. La plantilla deberá especificar si el mensaje contiene enlaces a sitios web (URL), y en el caso de contenerlos, deberá especificarlos, incluyendo aquellos casos en los que se pretendan enviar enlaces acortados.

Una vez operativo este proceso de validación, los PRSTM y los PCA/IT contarían con la obligación de consultar el registro de identificadores autorizado para permitir o bloquear el tráfico A2P. En ese sentido, solo se permitiría el curso de mensajes a los usuarios cuyos identificadores sean válidos al momento del envío. El sistema funcionaría en tiempo real, permitiendo consultar la validez del PCA/IT, marca y campaña antes del envío de los SMS.

En cuanto a los requerimientos técnicos mínimos de esta solución, sería necesaria una plataforma de base de datos centralizada, accesible vía API para los PRST, PCA e IT en el momento de pretender enviar mensajes a los usuarios. Deberá contar también con una interfaz de administración que le permita al validador central registrar y verificar nuevos IT, sus PCA y las respectivas campañas.

En cuanto a la Integración con las redes de SMS, se requeriría que los *SMSC/Hubs* de los PRSTM, IT y PCA se conecten al sistema para consultar y validar los identificadores de cada mensaje (p. ej., mediante protocolos API/REST que consulten el Código Corto A2P, Sender_ID y Template_ID y reciban respuesta sobre su autenticidad).

El sistema de validación centralizado deberá contar con la disponibilidad y capacidad suficientes para procesar los volúmenes de consultas concurrentes (*throughput)* acorde al tráfico de mensajería A2P nacional, así como con módulos de seguridad robustos (p. ej., autenticación robusta, cifrado de las consultas) que permitan garantizar la integridad y confiabilidad del sistema, teniendo en cuenta la sensibilidad de la información manejada.

En cuanto a los requerimientos operativos, se requeriría definir un administrador del validador central con la función de recibir solicitudes de registro de remitentes, validar la documentación (NIT, certificaciones empresariales), aprobar o denegar registros y asignar identificadores.

Los IT tendrían la obligación de: i) registrar la información de sus PCA y campañas en el validador (antes de enviar tráfico); ii) mantener actualizada la información de sus PCA y campañas (p. ej., baja de campañas finalizadas, cambios de razón social); iii) atender eventuales requerimientos de verificación adicional (p. ej., documentación legal del cliente).

Los PRSTM deberán: i) consultar en el registro central en línea para confirmar que los identificadores están autorizados antes de cursar tráfico, ii) bloquear o marcar mensajes cuyos remitentes no estén en el registro o figuren revocados, y iii) reportar al validador central cualquier uso indebido o sospechoso de un ID por parte de un remitente.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9.2.1.2.4 Alternativa 3: Proceso de validación distribuido (DLT) de originadores de contenido

Esta alternativa contempla la aplicación del conjunto de medidas transversales para esta temática (descrito en el numeral 9.2.1.2.2), articuladas con un sistema de validación distribuido basado en tecnología DLT (Distributed Ledger Technology), similar a blockchain, para atacar el fraude por SMS (smishing). En lugar de tener un único validador central, varios actores participan en una red compartida y segura donde se registran y validan los remitentes y sus mensajes. Esto permite mayor transparencia, trazabilidad y resistencia al fraude, y responde a la preocupación por posibles fallos de un sistema centralizado único y la necesidad de transparencia auditada en la trazabilidad.

Bajo la implementación de una plataforma de registro de remitentes sobre tecnología DLT, cada PCA se registra en la red distribuida con sus datos y previamente obtiene un identificador que será su Sender ID autorizado por parte de la CRC. Los nodos de la red deberían estar operados por los PRSTM y una entidad coordinadora, de modo que la verificación de un remitente y su campaña se realice de forma descentralizada y consensuada entre varios participantes (evitando punto único de falla).

El proceso se basa en la asignación de identificadores únicos para cada nivel:

- Un **Código Corto A2P** para los IT validados, el cual se asigna por la CRC previo al momento del registro en la red distribuida por parte del nodo, el cual tendría la coonotación de un recurso de identificación.
- Un **Sender_ID** para los PCA validados, el cual es asignado por la CRC.
- Un **Template_ID** para las plantillas de contenido de campañas validadas y aprobadas, el cual se asigna de manera consecutiva al momento del registro en la red distribuida por parte del nodo, el cual no tendría la naturaleza de un recurso de identificación.

Los roles que intervendrían en el proceso son los siguientes:

- **Validador o nodo**: administra un nodo del registro distribuido, revisa documentación, aprueba solicitudes y asigna identificadores que no sean recursos de identificación.
- **IT**: inscriben PCA y campañas, garantizando la veracidad de la información y cumpliendo con KYC.
- **PCA**: definen el contenido base de la plantilla y la clasificación de sus campañas.
- **CRC**: Asigna SENDER ID y Código Corto A2P.
- **PRSTM**: verifican en tiempo real que cada mensaje tenga identificadores válidos antes de cursarlo.

En este contexto, el proceso de validación consistiría en la aplicación de los siguientes pasos:

Validación del IT. Cada IT se inscribe ante cualquier nodo validador y remite la documentación requerida. El nodo validador verifica la información oficial y, de ser conforme, lo habilita dentro del sistema DLT para la posterior asignación del código corto A2P ante la CRC.

Validación de PCA. Los IT inscriben los PCA registrados que originarán contenido. El nodo validador revisa la documentación del PCA y el contrato suscrito con el IT, y si todo es conforme, solicita a la CRC la asignación de una identificación de la marca (Sender_ID) y la incluye dentro del sistema DLT

una vez haya sido autorizada. La vigencia del Sender ID será limitada y requerirá de una renovación periódica, para la cual se definirá la frecuencia específica, a fin de validar la información registrada y la operatividad de la marca.

Validación de campañas. El PCA define el contenido base de cada campaña, con posibilidad de incluir etiquetas variables, y asigna una clasificación conforme al catálogo que se defina. El PCA registra la plantilla ante el nodo validador, quien corrobora la clasificación, y la aprueba o rechaza. Si aprueba, emite un identificador de plantilla (Template_ID) que vincula campaña, remitente y contenido autorizado en el sistema distribuido DLT. La plantilla deberá especificar si el mensaje contiene enlaces a sitios web (URL), y en el caso de contenerlos, deberá especificarlos, incluyendo aquellos casos en los que se pretendan enviar enlaces acortados.

Cada mensaje A2P enviado se compara contra la base distribuida, y si el remitente o sus campañas no están registrados, o su firma digital no coincide, el mensaje es rechazado por los nodos de la red y en consecuencia los PRSTM no lo podrán cursar. Este sistema garantiza integridad (las inscripciones quedan inmutables en el ledger) y trazabilidad transparente (cualquier nodo puede auditar las transacciones de registro de remitentes).

En cuanto a los requerimientos técnicos mínimos necesarios para el despliegue de una red DLT por parte de los PRSTM, cada proveedor operaría un nodo validando transacciones (altas, bajas y actualizaciones de marcas y campañas) y asegurando redundancia. Se debe definir la plataforma DLT (p. ej., Hyperledger Fabric, Corda u otra) con tiempos de confirmación adecuados para no aumentar el tiempo de entrega de los SMS.

Para que los IT y sus PCA, así como los sistemas de mensajería se comuniquen con la red DLT al enviar un SMS, se deberán implementar interfaces (APIs) para consultar o actualizar el estado de los identificadores de la marca o sus campañas. La red DLT deberá garantizar inmutabilidad y seguridad criptográfica en los registros mediante el uso de certificados digitales, para que cada registro de un PCA o de una campaña quede firmada y sea verificable por todos los nodos, previniendo así manipulaciones.

En relación con los requerimientos operativos de esta alternativa, sería necesario conformar un gobierno colaborativo de la red DLT, a través de un comité operativo entre PRSTM y el acompañamiento de la CRC en caso de ser necesario, para operar y mantener la blockchain. Esto requiere definir acuerdos de nivel de servicio, reglas de consenso (p. ej., mayoría simple de nodos para aprobar un registro de remitente) y resolución de conflictos (si un operador detecta un abuso, cómo marcar a un remitente en la red), y dado el caso que no se logre acuerdo en alguno de los parámetros operativos necesarios, la CRC tendrá la facultad de fijarlo.

Los IT y sus PCA deberán interactuar con la red a través de los PRSTM, enviando sus solicitudes de registro o verificación para que se propaguen a todos los nodos para su validación. También es necesario que se establezca un plan de contingencia por si la red DLT presenta fallas, caso en el cual los PRSTM deben tener mecanismos alternos de validación temporal (como listas blancas de emergencia, etc.).

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9.2.1.2.5 Alternativa 4: Identificación exclusiva mediante códigos cortos, numeración E.164, o códigos alfanuméricos (remitente único)

Teniendo en cuenta que el uso compartido de códigos cortos dificulta la identificación del originador del contenido y permite a defraudadores ocultarse tras identificadores comunes, esta alternativa ataca esa confusión de identidad en los SMS A2P ya que busca que cada remitente legítimo use un identificador único e intransferible, de modo que los usuarios puedan reconocer la marca o servicio real y no sean engañados a través de números genéricos.

En ese sentido, esta alternativa consiste en asignar identificadores exclusivos a cada PCA autorizado para generar campañas A2P, acompañado de la aplicación del conjunto de medidas transversales para esta temática (descrito en el numeral 9.2.1.2.2). De este modo, cada mensaje aparecerá en el teléfono del usuario con identificador exclusivo de la marca evitando de esta manera la confusión. Esta medida cierra la puerta a la usurpación de identificadores comunes que usan los estafadores para hacerse pasar por múltiples entidades.

En cuanto a los requerimientos técnicos para desarrollar esta alternativa, los PRSTM e IT deben adaptar sus plataformas de SMS para soportar identificadores alfanuméricos en el campo *Sender ID* de los mensajes. Si bien es sabido por la CRC que la mayoría de los equipos SMS (SMSC) modernos ya soportan códigos alfanuméricos, resultaría necesario configurar y probar que todos los nodos en la ruta de un mensaje (SMSC del originador, hubs internacionales si aplican, SMSC de terminación) no alteren ni bloqueen el identificador alfanumérico.

Desde el punto de vista operativo, la CRC definiría el régimen de administración de los identificadores alfanuméricos (requisitos y procedimiento de asignación, criterios de uso eficiente y causales de recuperación) y elementos técnicos como la longitud permitida, los caracteres válidos, si pueden parecerse a nombres de entidades públicas o estratégicas, etc, y revisar los ya definidos para los códigos cortos y la numeración E.164 en el NDC 940 para adaptarlos al nuevo contexto regulatorio.

Por su parte, los PCA que soliciten recursos de identificación únicos deberán proveer la documentación que acredite su nombre comercial y una lista de palabras reservadas. Operativamente, los PRST, IT y PCA tendrán que actualizar sus procesos internos de provisión de servicio. Antes de habilitar una campaña A2P para un PCA, los IT deberán radicar ante la CRC la solicitud del identificador de su cliente. Adicionalmente, los PCA deberán incluir en sus contratos con los IT la obligación de usar solo su identificador autorizado.

Finalmente, sería indispensable diseñar amplias campañas de comunicación y educación al usuario, informando que a futuro los SMS legítimos de empresas llegarán identificados con un nombre específico, advirtiendo desconfiar de mensajes desde números o nombres genéricos. Esto se alinea con medidas de educación al usuario contempladas en el presente documento.

9.2.1.2.6 Evaluación de alternativas

La evaluación para seleccionar la alternativa regulatoria más adecuada para abordar la dificultad de trazabilidad en las comunicaciones A2P y la ausencia de controles efectivos para prevenir el fraude mediante SMS se desarrolló bajo un enfoque de análisis costo-beneficio, siguiendo los lineamientos metodológicos descritos en la sección 9.1 del presente documento. Este enfoque resulta pertinente

considerando que las distintas alternativas regulatorias evaluadas generan impactos diferenciados tanto en términos de efectividad para mitigar el fraude y fortalecer la trazabilidad de las comunicaciones, como en los costos de implementación, operación y supervisión que deben asumir los diferentes actores del ecosistema.

En este contexto, la aplicación de esta metodología requirió evaluar simultáneamente:

(i) la capacidad de cada alternativa para reducir los riesgos asociados al uso fraudulento de comunicaciones A2P;
(ii) su capacidad para mejorar la autenticidad, validación y trazabilidad de remitentes y campañas, y;
(iii) los costos asociados a la implementación de infraestructura tecnológica, integración operativa, administración y supervisión regulatoria.

Así las cosas, para estimar los beneficios derivado de las medidas para combatir el smishing en Colombia, se supuso que todas las reclamaciones reportadas a la Superintendencia Financiera correspondían a la modalidad de fraude A2P, teniendo en cuenta que no existen estadísticas desagregadas que permitan identificar la proporción de reclamos A2P y de P2P (Persona a Persona). En todo caso es importante señalar que, el tráfico SMS A2P concentra el 98,6% del total de mensajes realizados en este canal de comunicación.

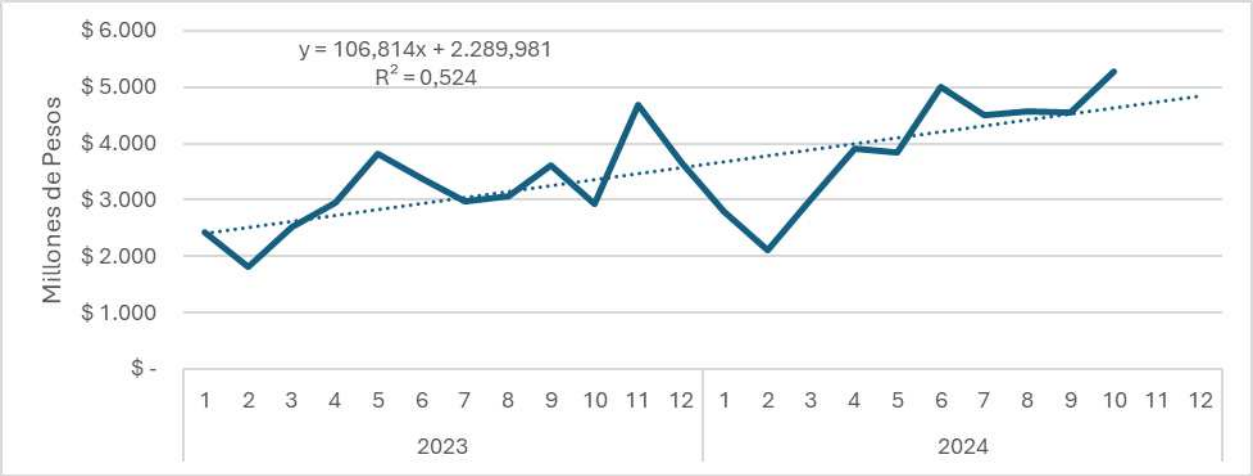
Ahora bien, para efectos de la presente evaluación, el beneficio asociado a las medidas regulatorias se define como el valor de las pérdidas económicas que potencialmente podrían evitarse mediante la reducción de las acciones fraudulentas desarrolladas a través de comunicaciones SMS. En este sentido, el beneficio económico de cada alternativa regulatoria corresponde a los recursos financieros que dejarían de ser afectados por actividades de smishing como resultado de la implementación de mecanismos orientados a fortalecer la trazabilidad, autenticidad y control de las comunicaciones A2P. Bajo esta lógica, la efectividad de las medidas regulatorias se refleja en su capacidad para disminuir el valor esperado de las reclamaciones asociadas a fraude mediante SMS reportadas al sistema financiero.

En primera medida, es importante establecer cuáles podrían ser las pérdidas potenciales derivadas de este tipo de acciones fraudulentas. Para ello, se toma como línea base el valor de las reclamaciones realizadas por usuarios del sistema financiero como consecuencia de pérdidas ocasionadas mediante esquemas de ingeniería social asociados a la modalidad de smishing. De acuerdo con la información reportada por la Superintendencia Financiera de Colombia, analizada en la sección 6.2 del presente documento, las reclamaciones relacionadas con este tipo de fraude han presentado una tendencia creciente y sostenida durante los últimos años, tanto en frecuencia como en valor económico reclamado.

Esta información permite aproximar el nivel de afectación económica atribuible al uso fraudulento de comunicaciones SMS y constituye un referente observable para estimar el beneficio potencial derivado de las medidas regulatorias propuestas. En consistencia, con el propósito de proyectar los perjuicios causados por la modalidad de fraude de smishing, se tomó como horizonte temporal el período comprendido entre 2025 y 2031. Para ello, se consideró que, como se evidencia en la Ilustración 16 y en la Ilustración 17, durante el año 2022 y los primeros meses de 2023 las pérdidas económicas asociadas a esta modalidad se mantuvieron relativamente estables y en niveles bajos frente a los años posteriores. No obstante, entre febrero y marzo de 2023 se observa un incremento significativo en el

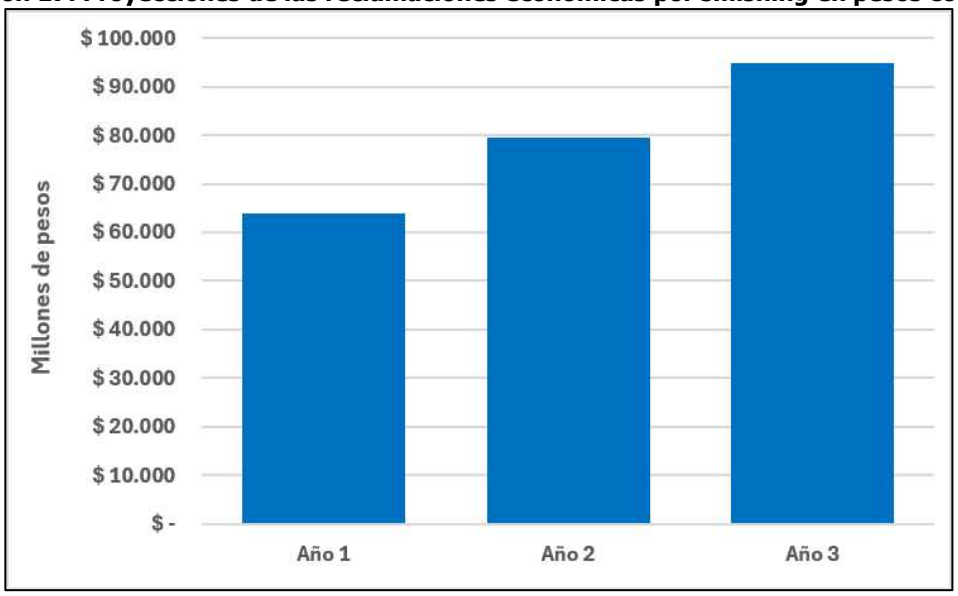
valor de las reclamaciones, seguido de una tendencia creciente y sostenida entre marzo de 2023 y diciembre de 2024, con algunas variaciones puntuales.

Ilustración 16. Tendencia y proyección de los valores reclamados por smishing a partir de enero de 2023 en millones de pesos corrientes



Fuente: Elaboración propia a partir de la Superintendencia Financiera de Colombia[63]

Ilustración 17. Proyecciones de las reclamaciones económicas por smishing en pesos corrientes.



Fuente: Elaboración propia a partir de la Superintendencia Financiera de Colombia[64]

Teniendo en cuenta que los valores observados antes de marzo de 2023 podrían reflejar una etapa inicial de subregistro o menor materialización del fenómeno, se estimó una regresión lineal utilizando

[63] Ídem
[64] Ídem

exclusivamente la información comprendida entre marzo de 2023 y diciembre de 2024. A partir de los resultados obtenidos se proyectó la evolución esperada de las pérdidas económicas asociadas al smishing desde enero de 2025, cuyo resultado se presenta en la Ilustración 16.

Los resultados obtenidos se presentan en la Ilustración 17. Estos evidencian que, de mantenerse las tendencias actuales y en ausencia de medidas regulatorias o mecanismos efectivos de mitigación, las pérdidas económicas asociadas a estas modalidades de fraude continuarían incrementándose de manera significativa durante los próximos años. En particular, las proyecciones sugieren que hacia el año 2031 las reclamaciones podrían superar los $156 mil millones anuales para smishing, consolidando esta práctica como una fuente creciente de afectación económica para los usuarios y para el ecosistema digital en general.

Ahora bien, una vez estimado el escenario base de pérdidas económicas asociadas a la modalidad de smishing en ausencia de intervención regulatoria, resulta necesario determinar el nivel de efectividad que podrían alcanzar las distintas alternativas propuestas para reducir dichas afectaciones.

En este sentido, debido a que no existe información estadística nacional que permita medir ex ante el impacto específico de cada medida sobre la reducción del fraude mediante comunicaciones A2P, la CRC recurrió al análisis de experiencias internacionales, estudios sectoriales y reportes técnicos elaborados por autoridades regulatorias, entidades multilaterales y organismos especializados en fraude y ciberseguridad. A partir de esta evidencia, se construyeron escenarios prospectivos de efectividad que permiten aproximar el potencial de reducción de pérdidas económicas derivado de la implementación de las medidas regulatorias evaluadas.

Es importante señalar que la extrapolación de resultados internacionales al contexto colombiano presenta limitaciones metodológicas asociadas a diferencias en las condiciones de mercado, niveles de madurez tecnológica, arquitectura institucional, capacidades de supervisión, comportamiento de los usuarios y tipologías predominantes de fraude. Por esta razón, la CRC adoptó un enfoque basado en escenarios de sensibilidad, con el propósito de capturar distintos niveles posibles de desempeño de las medidas regulatorias y reducir la incertidumbre inherente al ejercicio de estimación.

Bajo esta aproximación, para cada alternativa regulatoria se definieron tres escenarios de efectividad:

- un escenario pesimista, que representa condiciones de implementación con menores niveles de adopción, efectividad parcial de los controles o adaptación rápida de los esquemas de fraude;
- un escenario moderado o base, que representa un nivel de efectividad esperado bajo condiciones normales de implementación y operación;
- un escenario optimista, que representa condiciones de implementación robusta, alta coordinación sectorial y mayor efectividad de los mecanismos de prevención y validación.

En términos generales, la literatura y la experiencia internacional analizada evidencian los siguientes resultados:

Alternativa 2: Proceso de validación centralizado de originadores de contenido.

La referencia internacional más cercana a esta alternativa corresponde a los modelos implementados en Singapur y Irlanda, los cuales establecieron esquemas centralizados de validación y registro previo de remitentes, marcas y campañas para comunicaciones A2P.

País	Intervención	Supuesto	Efectividad	
			Inicial	Declive
Singapur[65]	SMS Sender ID Registry (SSIR)	La medida regulatoria aplica para todos los mensajes de texto. La efectividad podría decaer en la medida en que los estafadores pudieran llegar a identificar los puntos vulnerables del proceso de registro.	**-65%**	**-60%**
Irlanda[66]	SMS Registry			

En consecuencia, tomando como referencia estas experiencias internacionales y considerando diferencias estructurales frente al contexto colombiano, se definieron los siguientes escenarios de efectividad para esta alternativa:

- Escenario pesimista: 50%
- Escenario moderado: 65%
- Escenario optimista: 80%

Se considera que esta alternativa presenta altos niveles potenciales de efectividad debido a que:

- impide preventivamente el uso de remitentes no autorizados;
- fortalece la trazabilidad de campañas;
- permite verificar identidad de agregadores y marcas;
- facilita acciones de supervisión y auditoría;
- reduce la capacidad de spoofing y suplantación de identidad.

Alternativa 3: Proceso de validación distribuido (DLT) de originadores de contenido.

La principal referencia internacional para esta alternativa corresponde a la experiencia de India, país que implementó un ecosistema nacional de trazabilidad y validación distribuida para SMS A2P basado en tecnología Distributed Ledger Technology (DLT), bajo lineamientos de la Telecom Regulatory Authority of India (TRAI)[67].

Si bien no existe un porcentaje oficial único y consolidado de reducción de pérdidas económicas atribuibles exclusivamente al modelo DLT, diferentes análisis sectoriales indican reducciones

[65] Infocomm Media Development Authority (IMDA). Enhanced measures against scam SMS. Consultado el 13 de mayo de 2026. Disponible en: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/enhanced-measures-against-scam-sms

[66] Europe Economics. Scam Calls and Texts in Ireland – Costs and Benefits of Interventions (2023, United Kingdom). Disponible en: https://www.comreg.ie/media/2023/06/ComReg-2352a.pdf

[67] TELECOM REGULATORY AUTHORITY OF INDIA (TRAI). Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018. [en línea]. Nueva Delhi: TRAI, 19 de julio de 2018. [citado 14 de mayo, 2026]. Disponible en: https://www.trai.gov.in/sites/default/files/2024-09/RegulationUcc19072018.pdf.

significativas en tráfico no autorizado y spam comercial[68], especialmente después de estabilizar los procesos de registro y validación. Sin embargo, resulta razonable que el modelo distribuido presenta niveles similares de efectividad al centralizado al considerar que, aunque utilizan distintas, comparten una lógica regulatoria funcionalmente equivalente, basada en la validación previa de originadores; autenticación de remitentes; trazabilidad de campañas; registro de actores autorizados y bloqueo preventivo de comunicaciones no verificadas.

En consecuencia, desde el punto de vista de la mitigación del fraude mediante smishing, resulta razonable asumir que los niveles potenciales de efectividad de ambos modelos son comparables, dado que actúan sobre los mismos mecanismos causales de reducción del riesgo de suplantación y circulación de tráfico fraudulento:

País	Intervención	Supuesto	Efectividad	
			Inicial	Declive
India	SMS Registry blockchain-based Distributed Ledger Technology (DLT)	La medida implementa un esquema distribuido de registro, validación y trazabilidad de originadores de contenido basado en tecnología DLT, mediante autenticación previa de remitentes, plantillas y campañas antes del envío de mensajes SMS A2P. Dado que este modelo persigue funcionalmente los mismos objetivos preventivos de los esquemas centralizados de validación de remitentes, se asume un nivel de efectividad equivalente.	**-65%**	**-60%**

Así mismo, es importante aclarar que dada las características de este modelo de validación los escenarios de efectividad se tomarán como similares al del modelo centralizado.

Alternativa 4: Identificación exclusiva mediante códigos cortos y numeración E.164.

La revisión internacional evidencia que la asignación exclusiva de códigos cortos, numeración dedicada o identificadores de remitente para tráfico A2P contribuye a mejorar la identificación visible del remitente, reducir el anonimato y fortalecer la trazabilidad básica de las comunicaciones empresariales. Sin embargo, la experiencia comparada también muestra que los países que inicialmente permitieron el uso de identificadores dedicados o Sender ID sin validación robusta evolucionaron hacia mecanismos complementarios de registro, validación y autenticación de remitentes o campañas.

Australia identificó que el uso no registrado de Sender ID permitía la suplantación de entidades legítimas y, por ello, avanzó hacia un esquema obligatorio de registro en el que los mensajes enviados

[68] DEPARTMENT OF TELECOMMUNICATIONS (DoT). DOT and TRAI have taken widespread action for curbing Unsolicited Commercial Communication (UCC). [en línea]. Nueva Delhi: DoT, 6 de febrero de 2026. [citado 14 de mayo, 2026]. Disponible en: https://www.dot.gov.in/static/uploads/2026/02/2f35b2d58f60cbbeb8fe3447f609445c.pdf

con identificadores no registrados serían marcados como «Likely SCAM». En su análisis de impacto[69], el Gobierno australiano tomó como referencia la experiencia de Singapur, destacando reducciones del 64% en fraudes SMS bajo el esquema voluntario y reducciones cercanas al 70% después de la transición hacia un registro obligatorio.

En Reino Unido e Irlanda, el Mobile Ecosystem Forum[70] desarrolló registros de protección de Sender ID orientados a validar marcas y compartir información entre empresas y operadores para bloquear mensajes fraudulentos. Aunque estas experiencias no reportan un porcentaje oficial comparable de reducción de pérdidas económicas, sí muestran que los esquemas basados únicamente en identificación del remitente tienden a complementarse con registros de validación, intercambio de inteligencia y bloqueo coordinado, precisamente porque la exclusividad de numeración o identificador no elimina por sí sola los riesgos de spoofing, suplantación o uso indebido de remitentes legítimos.

En consecuencia, se considera que la alternativa de identificación exclusiva mediante códigos cortos o numeración E.164 presenta una efectividad inferior frente a los modelos centralizados o distribuidos de validación de originadores, dado que mejora la identificación del remitente, pero no incorpora mecanismos robustos de validación previa de contenido, campañas o autenticación integral de entidades. Para efectos del análisis, se propone utilizar escenarios prudenciales de efectividad:

- Escenario pesimista: 30%
- Escenario moderado: 40%
- Escenario optimista: 50%

País	Intervención	Supuesto	Efectividad	
			Inicial	Declive
Australia, Reino Unido y experiencias de códigos cortos A2P en Estados Unidos y Canadá	Identificación exclusiva mediante códigos cortos y numeración E.164 para tráfico A2P	Esquema basado en la asignación exclusiva de identificadores de envío. El nivel de efectividad para esta alternativa se estima aplicando un descuento frente a los resultados observados en modelos robustos de validación centralizada o distribuida	**-40%**	**-30%**

Estos valores reflejan un descuento frente a los niveles observados en modelos con registro y validación robusta, reconociendo que la numeración exclusiva actúa sobre la identificación visible y la trazabilidad básica, pero no reproduce plenamente los efectos de un validador centralizado o distribuido. En efecto, aunque la asignación exclusiva de numeración mejora significativamente la identificación del remitente, no elimina completamente el riesgo de uso fraudulento de numeración

[69] AUSTRALIA. DEPARTMENT OF INFRASTRUCTURE, TRANSPORT, REGIONAL DEVELOPMENT, COMMUNICATIONS AND THE ARTS. *SMS Sender ID Register: Cost-Benefit Analysis* [en línea]. Canberra: Australian Government, 2024 [consultado: 14 de mayo de 2026]. Disponible en: https://oia.pmc.gov.au/sites/default/files/posts/2024/12/Appendix%20A%20-%20SMS%20Sender%20ID%20Register%20Cost-Benefit%20Analysis.pdf

[70] MOBILE ECOSYSTEM FORUM. *SMS SenderID Protection Registry* [en línea]. Londres: MEF, s. f. [consultado: 14 de mayo de 2026]. Disponible en: https://mobileecosystemforum.com/sms-senderid-protection-registry/

legítima comprometida o campañas registradas de manera irregular dado que las medidas que se pueden implementar se basan en un esquema reactivo.

Enfoque de costos de las alternativas regulatorias.

La estimación de costos para las alternativas regulatorias asociadas a la temática «Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude» se desarrolló mediante un modelo de costeo regulatorio modular, construido específicamente para evaluar los requerimientos técnicos, operativos, administrativos y de supervisión asociados a la implementación de mecanismos de validación, autenticación y trazabilidad del tráfico SMS A2P.

La construcción de los costos parte de la identificación detallada de los módulos tecnológicos y operativos necesarios para implementar las distintas alternativas regulatorias, diferenciando entre inversiones iniciales (CAPEX), costos operativos recurrentes (OPEX), costos de integración, costos de supervisión y costos de transición regulatoria. A continuación, se realiza una breve descripción de los principales elementos empleados para el costeo de las alternativas, en la sección de ANEXOS se presenta de forma amplia el modelo desarrollado para la estimación de estos costos:

- Variables y parámetros base del modelo: La estimación económica se construyó utilizando variables macroeconómicas, operativas y tecnológicas que alimentan transversalmente todos los módulos del modelo.
- Construcción de costos por alternativa regulatoria: El modelo incorpora componentes diferenciados de infraestructura, integración, supervisión y operación para cada alternativa regulatoria.
- Alternativa 2: Considera la implementación de una plataforma centralizada administrada por un tercero o por la CRC.
- Alternativa 3: Se basa en tecnología DLT incorpora costos adicionales derivados de la complejidad técnica y operativa de una arquitectura blockchain distribuida.
- Alternativa 4: Considerar los costos asociados a asignación y administración de identificadores y plataformas de registro Sender ID.
- Clasificación de costos: El modelo diferencia entre costos CAPEX y OPEX, permitiendo estimar inversiones iniciales y gastos recurrentes.
- Costos de supervisión y administración regulatoria: El modelo incorpora costos específicos asociados a la supervisión, auditoría y gestión regulatoria por parte de la CRC.
- Consideración de sinergias y economías de escala: Se identifican las sinergias entre plataformas regulatorias con el propósito de evitar doble contabilización de costos.
- Horizonte temporal y enfoque de evaluación: Los costos fueron proyectados bajo un horizonte de análisis de tres (3) años.
- Variables y parámetros base del modelo: La estimación económica se construyó utilizando un conjunto de variables macroeconómicas, operativas y tecnológicas que alimentan transversalmente todos los módulos del modelo. En conjunto, este enfoque metodológico permite construir una estimación consistente, comparable y trazable de los costos regulatorios asociados a las alternativas para fortalecer la trazabilidad y autenticación de comunicaciones A2P.

Resultados

Los resultados de la evaluación costo-beneficio para esta temática evidencian diferencias significativas entre las alternativas regulatorias evaluadas, tanto en términos de costos de implementación como de beneficios esperados asociados a la reducción de las pérdidas económicas ocasionadas por smishing. En la Tabla 5 se presentan los resultados de esta evaluación, en términos del valor presente neto de las medidas, usando como factor de descuente el wacc sectorial, que corresponde a 11,57%.

Tabla 5. Resultados del ACB, VPN sobre tres años (cifra en millones)

	Alt 1: Statu Quo	Alt 2: Proceso de validación centralizado de originadores de contenido.	Alt 3: Proceso de validación distribuido (DLT) de originadores de contenido.	Alt 4: Identificación exclusiva mediante códigos cortos y numeración E.164.
Costos				
PRST	-	7.832,4	26.552,1	6.481,9
PCA/IT	-	21.629,2	91.522,1	20.973,6
Administración y operación	-	2.650,3	7.392,0	2.407,1
Beneficio				
Pérdidas económicas potencialmente evitadas	(158.009,2)	99.785,0	99.785,0	60.282,7
Beneficio Neto	(158.009,2)	67.673,1	-25.711,2	30.420,2
RCB	-	3,1	0,8	2,0

Fuente: Elaboración CRC.

En primer lugar, la Alternativa 1: Statu Quo presenta un beneficio neto negativo equivalente a pérdidas económicas potencialmente evitadas no materializadas por $158.00,2 millones, lo cual refleja que mantener el esquema regulatorio actual no permitiría mitigar de manera efectiva el crecimiento proyectado de las afectaciones económicas derivadas del fraude mediante SMS A2P. En consecuencia, esta alternativa no genera una relación beneficio-costo positiva. Por su parte, la Alternativa 2: «Proceso de validación centralizado de originadores de contenido» una Relación Beneficio-Costo (RBC) potencial de 3,1. Esto implica que, por cada peso invertido en la implementación de la medida, se obtendrían aproximadamente $3,1 pesos de beneficio económico derivado de la mitigación del fraude.

En relación con la Alternativa 3: se observan un incremente significativo en costos de implementación en relación con las demás alternativas. Estos costos se explican principalmente por las inversiones requeridas para desplegar y operar una infraestructura basada en tecnología Distributed Ledger Technology (DLT), así como por las integraciones necesarias entre múltiples actores del ecosistema. Sin embargo, esta alternativa alcanzaría un nivel de efectividad similar al modelo centralizado en la mitigación del fraude dada su capacidad apoyar la trazabilidad en el envío de mensajes y desarrollo campañas publicitaras por medio de este canal de comunicación. A pesar de ello, la relación beneficio-costo obtenida es de 0,8, lo cual indica que los beneficios económicos esperados no alcanzan a compensar completamente los costos requeridos para su implementación bajo el horizonte de evaluación considerado. En este punto, también es importante señalar que este resultado se encuentra

influenciado por la dificulta de extender el periodo de tiempo para realizar la proyección de las reclamaciones económicas por smishing.

Finalmente, la Alternativa 4 presenta una relación beneficio-costo de 2,0. Estos resultados indican que la medida genera beneficios superiores a sus costos, aunque con una efectividad menor frente a las alternativas de validación integral de originadores, debido a que la asignación exclusiva de identificadores mejora la trazabilidad básica del remitente, pero no incorpora mecanismos robustos de autenticación previa de campañas y validación de contenido.

En términos comparativos, los resultados evidencian que la Alternativa 2: «Proceso de validación centralizado de originadores de contenido» presenta el mejor balance entre costos de implementación y beneficios económicos esperados, al alcanzar la mayor relación beneficio-costo entre las alternativas evaluadas. La Alternativa 4 también presenta resultados económicamente favorables, aunque con una menor capacidad de mitigación del fraude. Por el contrario, aunque la Alternativa 3 ofrece altos niveles potenciales de efectividad regulatoria, los elevados costos asociados a la implementación de un ecosistema DLT reducen significativamente su desempeño económico bajo el horizonte temporal analizado.

Análisis de sensibilidad.

Con el propósito de evaluar la robustez de los resultados obtenidos en la evaluación costo-beneficio de la temática «Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude», se desarrolló un análisis de sensibilidad sobre el principal parámetro de incertidumbre del modelo: la efectividad de las medidas regulatorias para reducir las pérdidas económicas ocasionadas por smishing.

Para ello, se construyeron tres escenarios de efectividad «pesimista, moderado y optimista» considerando la evidencia internacional disponible y las limitaciones asociadas a la extrapolación de experiencias regulatorias implementadas en otros países hacia el contexto colombiano, para la construcción de estos escenarios se contempló una variación de 15 puntos porcentuales con respecto al escenario base de evaluación. En todos los escenarios se asumió un declive gradual de cinco (5) puntos porcentuales en la efectividad de las medidas durante el horizonte de evaluación, con el propósito de reflejar posibles procesos de adaptación de los actores fraudulentos, desplazamiento de tráfico hacia otros canales o reducción progresiva de la capacidad preventiva de las medidas en el tiempo.

Tabla 6. Análisis de sensibilidad frente a diferentes escenarios de niveles de efectividad

	Alt 2: Proceso de validación centralizado de originadores de contenido.	Alt 3: Proceso de validación distribuido (DLT) de originadores de contenido.	Alt 4: Identificación exclusiva mediante códigos cortos y numeración E.164.
Escenarios			
Pesimista	50%	50%	25%
Moderado	65%	65%	40%
Optimista	80%	80%	55%
RCB			

Pesimista	2,4	0,6	1,2
Moderado	3,1	0,8	2,0
Optimista	4,2	1,1	3,1

Fuente: Elaboración CRC.

Bajo el escenario moderado, utilizado como escenario base de evaluación, se asumieron niveles iniciales de efectividad del 65% para las Alternativas 2 y 3, correspondientes a los modelos de validación centralizada y distribuida de originadores de contenido, respectivamente, mientras que para la Alternativa 4 se consideró una efectividad inicial del 40%, asociada a la identificación exclusiva mediante códigos cortos y numeración E.164. Posteriormente, estos niveles de efectividad disminuyen gradualmente en cinco puntos porcentuales durante el horizonte de análisis.

Los resultados del análisis muestran que la Alternativa 2 un desempeño económico robusto en todos los escenarios evaluados. En el escenario pesimista, esta alternativa alcanza una Relación Beneficio-Costo (RBC) de 2,4, mientras que en el escenario optimista la RBC aumenta hasta 4,2. Estos resultados indican que incluso bajo supuestos conservadores de efectividad, los beneficios económicos asociados a la reducción de pérdidas por smishing continúan siendo significativamente superiores a los costos de implementación y operación de la medida.

Por su parte, la Alternativa 3 presenta una alta sensibilidad frente a variaciones en el indicador de efectividad. Aunque esta alternativa logra beneficios económicos similares a los del modelo centralizado, sus elevados costos de implementación reducen considerablemente su desempeño económico. En el escenario pesimista la RBC se reduce a 0,6, mientras que en el escenario optimista apenas alcanza un valor cercano a 1,1, permaneciendo por debajo de la unidad en todos los casos analizados. Esto evidencia que, bajo las condiciones consideradas en el modelo, la magnitud de las inversiones requeridas por un ecosistema DLT no logra compensarse plenamente con los beneficios económicos derivados de la mitigación del fraude.

En relación con la Alternativa 4, los resultados muestran un comportamiento intermedio. En el escenario pesimista la medida alcanza una RBC de 1,2, mientras que en el escenario optimista este indicador aumenta a 3,1. Lo anterior evidencia que, aunque la efectividad esperada de esta alternativa es inferior frente a los modelos de validación integral de originadores, sus menores costos de implementación permiten mantener resultados económicamente positivos en todos los escenarios analizados. Aunque una reducción en los niveles de efectividad podría generar un resultado inviable.

Conclusión

A partir del análisis técnico y operativo realizado, esta Comisión identificó que las distintas alternativas propuestas comprenden un conjunto de medidas complementarias que responden a diferentes capas de control dentro del ecosistema A2P. En particular, se encontró que los mecanismos de validación de identidad, los sistemas de registro y trazabilidad, las herramientas de monitoreo y las medidas de identificación verificable pueden operar de manera articulada para fortalecer las capacidades de prevención y detección de fraude.

Asimismo, se evidenció que una parte importante de los costos asociados a las alternativas corresponde a componentes tecnológicos y operativos que podrían compartirse mediante arquitecturas unificadas, especialmente en lo relacionado con plataformas centralizadas, APIs, motores analíticos, sistemas de reportería y equipos de monitoreo. Por otro lado, la CRC identificó que la

alternativa propuesta como solución considerara criterios de proporcionalidad, interoperabilidad, protección de datos personales, gestión de falsos positivos y gradualidad en la implementación, teniendo en cuenta tanto las capacidades técnicas de los actores involucrados como la evolución dinámica de las modalidades de fraude asociadas al ecosistema de mensajería A2P.

En términos generales, un análisis complementario sobre sensibilidad a los cambios en los niveles de efectividad permitió concluir que los resultados obtenidos para la Alternativa 2 son consistentes y relativamente estables frente a cambios en los supuestos de efectividad, consolidándose como la alternativa con mejor desempeño económico bajo los distintos escenarios evaluados. Por el contrario, la Alternativa 3 presenta una alta dependencia de supuestos de efectividad y una fuerte sensibilidad a los costos tecnológicos asociados al despliegue de infraestructura DLT, mientras que la Alternativa 4 constituye una medida de menor complejidad y costo, aunque también con una capacidad de mitigación del fraude relativamente más limitada.

9.2.1.2.7 Propuesta regulatoria «Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude»

Teniendo en cuenta la evaluación expuesta, para materializar en la regulación la alternativa ganadora, se realizarán los siguientes ajustes regulatorios:

- Se incluirán en el Título I de la Resolución CRC 5050 de 2016 las definiciones de KYC, Plantillas de Contenido A2P (TEMPLATE ID), tráfico A2P, tráfico P2P y validador centralizado.

- Se modificarán las definiciones de código corto, integrador tecnológico y PCA a fin de establecer claridades frente a los actores de la cadena de valor y sus obligaciones regulatorias.

- Se subrogará el Capítulo 4 del TÍTULO VI — Régimen de Administración de Recursos de Identificación — de la Resolución CRC 5050 de 2016 a partir del vencimiento de un período de transición de seis (6) meses. A partir de ese momento, el Capítulo 4 del TÍTULO VI, que regula la forma en la que actualmente funcionan los códigos cortos, cambiará de enfoque respecto de la forma en la que ese recurso de identificación será utilizado en el ecosistema A2P.

  En particular, el código corto A2P será el recurso de identificación administrado por la CRC que identifica de manera exclusiva e individual a cada agente que, en virtud de una relación contractual con un PRST, tiene conexión directa con este para cursar tráfico A2P de mensajería de texto (SMS). A través de un único código corto A2P, el asignatario cursará el tráfico A2P de todas las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID.

- Se adicionará el Capítulo 13 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, el cual contendrá las reglas comunes a los recursos de identificación denominados código corto A2P y SENDER ID. En ese capítulo se regulará (i) el funcionamiento del validador centralizado; (ii) los requerimientos técnicos y operativos del sistema de validación; (iii) el proceso de KYC; (iv) el régimen de plantillas de

contenidos A2P y las obligaciones de cada uno de los actores; y (v) la creación de un comité técnico de seguimiento del nuevo régimen.

- En la resolución que se expida se regulará la forma de escoger a la persona jurídica que cumplirá las funciones de validador centralizado. En concreto, los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM) serán responsables de la selección del validador centralizado, bajo la supervisión de la CRC. Lo anterior, en atención a que el validador centralizado deberá integrarse técnicamente con las redes de los PRSTM, razón por la cual son estos proveedores quienes se encuentran en mejor posición para evaluar los requerimientos técnicos, la capacidad operativa y la idoneidad del candidato seleccionado. La participación en el proceso de selección es una obligación regulatoria de todos los PRSTM.

- Para efectos de garantizar un tránsito e implementación ordenados y sin traumatismos de los cambios implementados en el Capítulo 4 del Título VI de la Resolución CRC 5050 de 2016 (versión subrogada que aplicará luego del periodo de transición) y de las adiciones de los Capítulos 12 y 13 al TÍTULO VI de la Resolución CRC 5050 de 2016, se dispondrá de un período de transición de seis (6) meses. Este periodo de transición empezará a contarse a partir de la publicación en el Diario Oficial de la resolución por medio de la cual la CRC defina la nueva remuneración aplicable al ecosistema A2P.

La propuesta regulatoria es la siguiente:

Adiciónese las siguientes definiciones al TÍTULO I de la Resolución CRC 5050 de 2016:

«(…)

CONOCIMIENTO DEL CLIENTE — KYC (KNOW YOUR CUSTOMER): Proceso de debida diligencia mediante el cual los asignatarios del código corto A2P verifican la identidad, legitimidad y perfil de riesgo de los agentes con quienes celebran contratos para cursar el tráfico de mensajería A2P, con el propósito de prevenir el uso indebido de los recursos de identificación para la comisión de fraudes mediante mensajes cortos de texto (SMS). El proceso de KYC comprende como mínimo la verificación de la existencia jurídica y representación legal del agente, la identificación del beneficiario final de la relación contractual, la acreditación del objeto social compatible con el servicio a prestar, la evaluación del perfil de riesgo del solicitante y el monitoreo continuo de la relación contractual durante su vigencia, conforme a las obligaciones establecidas en el Capítulo 13 del TÍTULO VI de la presente resolución.

LISTA DNO (DO NOT ORIGINATE): Lista de numeración E.164 nacional que no debe ser utilizada como identificador de línea llamante (CLI) en la originación de llamadas de voz, por tratarse de numeración no atribuida, no asignada, no adjudicada por la CRC, o reservada exclusivamente para la recepción de llamadas. Los PRST deberán implementar en sus redes mecanismos para bloquear las llamadas originadas desde números incluidos en la lista DNO, conforme a las condiciones establecidas en el artículo 2.1.10.7.2.2.3 de la presente resolución y en concordancia con la Recomendación UIT-T E.164.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PLANTILLA DE CONTENIDO A2P (TEMPLATE ID): Estructura base del mensaje corto de texto (SMS) que un asignatario del SENDER ID somete a aprobación del validador centralizado antes de cursarla a los usuarios finales, y que define el contenido fijo y los campos variables autorizados del mensaje, la modalidad de contenido aplicable, las condiciones de consentimiento requeridas y, cuando corresponda, las URLs o dominios de destino autorizados. Si bien la plantilla de contenido A2P se debería asociar con un número único denominado TEMPLATE ID, dicho número no es un recurso de identificación administrado por la CRC. El mal uso de la plantilla por parte del asignatario del SENDER ID o del asignatario del código corto A2P constituye causal de recuperación del respectivo recurso de identificación conforme a las reglas de atribución de responsabilidad establecidas en el Capítulo 13 del TÍTULO VI de la presente resolución. Ningún mensaje A2P podrá ser cursado a través de las redes de los PRST si no está respaldado por una plantilla de contenido aprobada y vigente en el sistema del validador centralizado.

SENDER ID: Recurso de identificación administrado por la CRC, que identifica de manera única e inequívoca a la persona natural o jurídica responsable directa por la producción y generación de contenidos o aplicaciones enviados a través de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD). El SENDER ID es visible para el usuario final en el encabezado del mensaje recibido y permite la identificación clara e inmediata del originador del contenido. A cada persona natural o jurídica le será asignado un único SENDER ID. El SENDER ID podrá utilizarse para una o varias de las modalidades de contenido establecidas en el artículo 6.12.1.3 del Capítulo 12 del TÍTULO VI. El tráfico A2P identificado con el SENDER ID se cursa a través del código corto A2P del agente intermediario con quien el asignatario del SENDER ID mantiene relación contractual. La asignación del SENDER ID confiere exclusivamente el derecho de uso del recurso de identificación, pero no otorga derecho de propiedad sobre el mismo, ni tendrá costo alguno para el asignatario. El régimen de administración del SENDER ID se encuentra establecido en el Capítulo 12 del TÍTULO VI de la presente resolución.

TRÁFICO A2P (APPLICATION TO PERSON): Modalidad de tráfico de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD) en la que el mensaje es originado por una aplicación, plataforma o sistema automatizado y tiene como destinatario a un usuario final de un servicio de telecomunicaciones móviles. Para efectos del régimen de administración de recursos de identificación establecido en el TÍTULO VI de la presente resolución, el tráfico A2P es aquel cursado mediante la utilización de un código corto A2P y un SENDER ID debidamente asignados por la CRC, respaldado por una plantilla de contenido aprobada por el validador centralizado conforme al Capítulo 13 del TÍTULO VI de la presente resolución.

TRÁFICO P2P (PERSON TO PERSON): Modalidad de tráfico de mensajes cortos de texto (SMS) en la que el mensaje es originado y recibido por usuarios finales de servicios de telecomunicaciones móviles, utilizando la numeración E.164 no geográfica de redes para la comunicación directa entre personas. El tráfico P2P está sujeto a las condiciones de monitoreo y control establecidas en el artículo 2.1.10.7.2.1 de la presente resolución.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

VALIDADOR CENTRALIZADO: Persona jurídica que tiene a su cargo la administración, gestión e integridad del proceso de validación de los agentes, marcas y plantillas de contenido que participan en el ecosistema de tráfico A2P. Sus funciones comprenden la verificación del proceso de KYC adelantado por los asignatarios del código corto A2P respecto de los potenciales asignatarios del SENDER ID, la aprobación de las plantillas de contenido A2P, y la emisión de las certificaciones requeridas en el proceso de asignación de los recursos de identificación código corto A2P y SENDER ID. La actuación del validador centralizado se enmarca dentro de los lineamientos regulatorios que para el efecto expida la CRC y bajo la supervisión permanente del Administrador de los Recursos de Identificación.

(…)».

Modifíquese las siguientes definiciones del TÍTULO I de la Resolución CRC 5050 de 2016, las cuales quedarán así:

«(…)

CÓDIGO CORTO A2P: ~~Tipo de numeración asignada por la CRC para la prestación de servicios de contenidos y aplicaciones basados en el envío o recepción de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD). La naturaleza de esta numeración está circunscrita al posicionamiento e identificación de un tipo de servicio de contenidos y aplicaciones para los usuarios, a través de un código numérico que informe claramente el tipo de servicio, el contenido, la modalidad de compra y los costos asociados, y no para la creación de un canal de comunicación dedicado de SMS entre los usuarios finales del servicio de telefonía móvil y sus clientes~~. Recurso de identificación administrado por la CRC que corresponde a un código corto asignado de manera exclusiva e individual a cada agente que, en virtud de una relación contractual con un PRST, tiene conexión directa con este para cursar tráfico A2P de mensajería de texto (SMS). A través de un único código corto A2P, el asignatario cursará el tráfico A2P de todas las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID. El régimen de administración del código corto A2P se encuentra establecido en el Capítulo 4 del TÍTULO VI de la presente resolución.

INTEGRADOR TECNOLÓGICO (IT): Agente responsable de la provisión de infraestructura de conexión y de soporte técnico entre los PRST y los PCA (asignatarios de SENDER ID) sin conexión directa con los PRST, a través de una relación contractual de acceso directo con al menos un PRST. En su calidad de responsable de la infraestructura de conexión, el IT es el asignatario del recurso de identificación denominado código corto A2P conforme al Capítulo 4 del TÍTULO VI de la presente resolución. Cuando el IT sea también responsable directo por la producción o generación de contenidos o aplicaciones propios que curse a través de su propia infraestructura de conexión, deberá ser asignatario tanto del código corto A2P, así como del recurso de identificación denominado SENDER ID conforme al Capítulo 12 del TÍTULO VI de la presente resolución, en su calidad de PCA.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PROVEEDOR DE CONTENIDOS Y APLICACIONES (PCA): Agente~~s~~ responsable~~s~~ directo~~s~~ por la producción o generación ~~o consolidación~~ de contenidos o aplicaciones cursados a través de redes de telecomunicaciones hacia usuarios finales de servicios de telecomunicaciones móviles. En su calidad de responsable del contenido, el PCA es el asignatario del recurso de identificación denominado SENDER ID conforme al Capítulo 12 del TÍTULO VI de la presente resolución. Estos actores pueden o no estar directamente conectados con el o los PRST sobre los cuales prestan sus servicios, por lo que el PCA puede cursar su tráfico a través de la infraestructura de conexión de un IT o por intermedio de su propia infraestructura de conexión con acceso directo a un PRST, caso en el cual deberá ser asignatario tanto del SENDER ID como del recurso de identificación denominado código corto A2P conforme al Capítulo 4 del TÍTULO VI de la presente resolución. ~~Quedan comprendidos bajo esta definición todos aquellos actores que presten sus funciones como productores, generadores o agregadores de contenido.~~

(…)».

Subróguese el Capítulo 4 del TÍTULO VI — Régimen de Administración de Recursos de Identificación — de la Resolución CRC 5050 de 2016 a partir del vencimiento del período de transición establecido en el respectivo proyecto de resolución. A partir de ese momento, el Capítulo 4 del TÍTULO VI quedará así:

«CAPÍTULO 4
CÓDIGO CORTO PARA SERVICIOS DE MENSAJERÍA A2P

SECCIÓN 1.
PLANIFICACIÓN Y FUNCIONAMIENTO DEL CÓDIGO CORTO A2P

ARTÍCULO 6.4.1.1. NATURALEZA DEL CÓDIGO CORTO A2P. El código corto A2P es el recurso de identificación administrado por la CRC que identifica de manera exclusiva e individual a cada agente que, en virtud de una relación contractual con un PRST, tiene conexión directa con este para cursar tráfico A2P de mensajería de texto (SMS). A través de un único código corto A2P, el asignatario cursará el tráfico A2P de todas las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID.

ARTÍCULO 6.4.1.2. ESTRUCTURA DEL CÓDIGO CORTO A2P. El código corto A2P se compone por cadenas de 5 y 6 dígitos que identifican de manera única al agente asignatario.

ARTÍCULO 6.4.1.3. ASIGNATARIOS DEL CÓDIGO CORTO A2P. Podrán solicitar y ser asignatarios de un código corto A2P los agentes que, en virtud de una relación contractual con un PRST, tienen conexión directa con este para cursar el tráfico de mensajería A2P. Estos agentes pueden ser integradores tecnológicos o PCA que cuenten con dicha conexión directa. También podrán ser asignatarios los PRST que lo requieran para soportar sus servicios, en su calidad de integrador tecnológico.

PARÁGRAFO 1. Los PCA con conexión directa al PRST que sean a su vez responsables directos por la producción y generación de sus propios contenidos o aplicaciones deberán ser asignatarios tanto de código corto A2P como de SENDER ID. En este caso, el agente podrá

presentar directamente la solicitud de asignación del SENDER ID sin intermediación de un tercero.

PARÁGRAFO 2. Los agentes que únicamente provean infraestructura de conexión para cursar el tráfico de mensajería de terceros, sin ser responsables directos por la producción del contenido, serán integradores tecnológicos asignatarios únicamente de código corto A2P.

ARTÍCULO 6.4.1.4. UNICIDAD DEL CÓDIGO CORTO A2P. Cada solicitante tendrá derecho a la asignación de un único código corto A2P, el cual lo identificará de manera inequívoca en el ecosistema de mensajería A2P. Un mismo agente no podrá ser titular de más de un código corto A2P asignado simultáneamente.

SECCIÓN 2.
ASIGNACIÓN DEL CÓDIGO CORTO A2P

ARTÍCULO 6.4.2.1. REQUISITOS PARA LA ASIGNACIÓN DEL CÓDIGO CORTO A2P. Para solicitar la asignación de un código corto A2P, el solicitante deberá remitir al Administrador de los Recursos de Identificación, a través del trámite unificado de recursos de identificación, la siguiente información:

6.4.2.1.1. Constancia de inscripción previa en el RPCAI, con indicación de si actúa en calidad de PCA con conexión directa al PRST o de integrador tecnológico.

6.4.2.1.2. Código corto A2P solicitado, de conformidad con la estructura del artículo 6.4.1.2 y la disponibilidad en el SIGRI.

6.4.2.1.3. Descripción detallada del servicio o función que desempeñará como asignatario del código corto A2P, que incluya como mínimo la descripción de la infraestructura técnica de conexión con el o los PRST, y la identificación de los PRST con quienes mantendrá o mantiene relaciones de acceso.

6.4.2.1.4. Justificación detallada de la necesidad del código corto A2P solicitado.

6.4.2.1.5. Certificado de existencia y representación legal vigente, expedido con no más de noventa (90) días de anterioridad.

6.4.2.1.6. Copia del contrato de acceso suscrito con al menos un PRST, o declaración juramentada de que se encuentra en proceso de negociación y que presentará copia dentro de los treinta (30) días hábiles siguientes a la firmeza del acto de asignación. En este último caso, la asignación quedará condicionada a la presentación oportuna del contrato.

6.4.2.1.7. Certificación expedida por el validador centralizado, en los términos del Capítulo 13 del TÍTULO VI de esta resolución, en la que conste la verificación de la identidad del agente, su objeto social y el cumplimiento de los requisitos de debida diligencia.

6.4.2.1.8. Descripción en detalle de las medidas de control y herramientas tecnológicas para prevenir fraudes mediante los accesos a sus plataformas o herramientas para el envío de SMS,

así como los mecanismos de trazabilidad del tráfico de mensajería A2P desde el asignatario de SENDER ID hasta la terminación en el usuario final.

ARTÍCULO 6.4.2.2. PROCEDIMIENTO DE ASIGNACIÓN DEL CÓDIGO CORTO A2P. Una vez presentada la solicitud conforme al artículo 6.4.2.1, el Administrador de los Recursos de Identificación resolverá en un término de quince (15) días hábiles conforme al siguiente procedimiento:

6.4.2.2.1. Se verificará que la solicitud cumpla con todos los requisitos del artículo 6.4.2.1. Si no los cumple, se negará la asignación.

6.4.2.2.2. Se verificará que el solicitante no tenga un código corto A2P previamente asignado en el SIGRI. Si existe uno previo asignado, se negará la asignación salvo solicitud simultánea de devolución del anterior.

6.4.2.2.3. Se verificarán que en el año inmediatamente anterior no se recuperó un código corto A2P del solicitante por las causales de los numerales 6.4.3.2.5. y 6.4.3.2.6. del artículo 6.4.3.2. Si hubo recuperación por esas causales, se negará la asignación.

6.4.2.2.4. Se llevará a cabo el análisis de las solicitudes según el orden de llegada.

6.4.2.2.5. Se verificará la consistencia entre la descripción del servicio, los mecanismos de trazabilidad y la certificación del validador centralizado.

6.4.2.2.6. Se verificará la disponibilidad y viabilidad en el SIGRI. Si se cumplen todos los requisitos, se cambiará el estado a «Preasignado».

6.4.2.2.7. Se expedirá el acto administrativo de asignación y cambio de estado a «Asignado» en el SIGRI, una vez quede en firme.

PARÁGRAFO. El término de quince (15) días hábiles se suspende cuando se requiera información adicional y se reanuda al recibo de la respuesta completa.

SECCIÓN 3.
USO DEL CÓDIGO CORTO A2P

ARTÍCULO 6.4.3.1. CRITERIOS DE USO EFICIENTE. El Administrador de los Recursos de Identificación verificará el uso eficiente del código corto A2P asignado en observancia de los siguientes criterios:

6.4.3.1.1. Cumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6.

6.4.3.1.2. Cumplimiento de las obligaciones especiales de los asignatarios de código corto A2P establecidas en el Capítulo 13 del TÍTULO VI.

6.4.3.1.3. El código corto A2P debe ser implementado en un término máximo de seis (6) meses desde la firmeza del acto de asignación. Se entiende implementado cuando el asignatario ha

establecido la conexión técnica operativa con al menos un PRST y puede cursar tráfico de mensajería A2P.

6.4.3.1.4. El código corto A2P implementado no deberá reportar ausencia de tráfico en períodos consecutivos iguales o superiores a seis (6) meses, salvo suspensión temporal ordenada por el Administrador de los Recursos de Identificación.

6.4.3.1.5. El asignatario deberá mantener vigente en todo momento al menos una relación contractual de acceso con un PRST. La terminación de todas las relaciones sin devolución del recurso constituirá indicio de uso ineficiente.

6.4.3.1.6. El asignatario deberá mantener actualizada su información de contacto en el RPCAI y en la respectiva matrícula mercantil que proporciona información al RUES.

6.4.3.1.7. A través del código corto A2P únicamente podrá cursarse tráfico A2P de personas naturales o jurídicas que cuenten con un SENDER ID previamente asignado y vigente vinculado al mismo, respaldado por una plantilla de contenido aprobada y vigente en el sistema del validador centralizado.

ARTÍCULO 6.4.3.2. CAUSALES DE RECUPERACIÓN DEL CÓDIGO CORTO A2P. El Administrador de Recursos de Identificación podrá recuperar el código corto A2P conforme al artículo 6.1.1.8 cuando el asignatario incumpla los criterios del artículo 6.4.3.1 o incurra en las siguientes causales:

6.4.3.2.1. Incumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6.

6.4.3.2.2. Incumplimiento de las obligaciones especiales de los asignatarios de código corto A2P establecidas en el Capítulo 13 del TÍTULO VI de esta resolución.

6.4.3.2.3. No implementación dentro de los seis (6) meses siguientes a la firmeza del acto de asignación.

6.4.3.2.4. Ausencia de tráfico durante seis (6) meses consecutivos.

6.4.3.2.5. Envío de mensajes de texto (SMS) en nombre de personas naturales o jurídicas que no cuenten con SENDER ID asignado y vigente vinculado al código corto A2P, o envío de mensajes sin respaldo de plantilla de contenido previamente aprobada y vigente en el sistema del validador centralizado.

6.4.3.2.6. Envío de mensajes de texto (SMS) que potencialmente pueden ser atribuibles al mal uso de las plantillas y que sea imputable al asignatario del código corto A2P conforme al artículo 6.13.4.4 de la presente resolución.

6.4.3.2.7. No presentación del contrato de acceso con el PRST dentro del plazo del numeral 6.4.2.1.6 cuando la asignación quedó condicionada a ello.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.4.3.2.8. Imposibilidad de continuar ejerciendo su objeto social, incluyendo liquidación judicial o voluntaria, o cancelación de matrícula mercantil.

6.4.3.2.9. Razones de interés general o seguridad nacional.

6.4.3.2.10. Establecimiento, mediante decisión ejecutoriada, de incumplimiento de disposiciones en materia de protección de datos personales o propiedad intelectual.

PARÁGRAFO 1. La recuperación del código corto A2P tiene efectos sobre todos los SENDER ID vinculados. Simultáneamente con la notificación del acto administrativo que ordena la recuperación del código corto A2P, el Administrador de Recursos de Identificación notificará a todos los asignatarios de SENDER ID vinculados, de conformidad con la información que el validador centralizado le proporcione a la CRC, otorgándoles a los asignatarios de SENDER ID treinta (30) días hábiles para acreditar una nueva relación comercial con un titular de un código corto A2P.

PARÁGRAFO 2. Cuando la causal de recuperación sea la del numeral 6.4.3.2.5 o la del numeral 6.4.3.2.6, la CRC podrá ordenar, en el acto de apertura de la actuación administrativa, o en cualquier estado de la actuación administrativa, la suspensión temporal del uso del recurso de identificación denominado código corto A2P. Dicha suspensión se mantendrá durante el trámite administrativo y no podrá exceder un plazo máximo de seis (6) meses».

Adiciónese el Capítulo 13 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, en los siguientes términos:

«CAPÍTULO 13
REGLAS COMUNES A LOS RECURSOS DE IDENTIFICACIÓN DENOMINADOS CÓDIGO CORTO A2P Y SENDER ID

SECCIÓN 1.
VALIDADOR CENTRALIZADO

ARTÍCULO 6.13.1.1. NATURALEZA Y FUNCIÓN DEL VALIDADOR CENTRALIZADO. El validador centralizado es la persona jurídica seleccionada por los PRSTM, que tiene a su cargo la administración, gestión e integridad del proceso de validación de los agentes, marcas y plantillas de contenido que participan en el ecosistema de tráfico de mensajería A2P. El validador centralizado garantiza que únicamente los agentes que hayan acreditado su legitimidad y el cumplimiento de los requisitos de debida diligencia puedan acceder a los recursos de identificación denominados código corto A2P y SENDER ID, y que únicamente los mensajes cortos de texto, asociados a las plantillas aprobadas conforme al presente capítulo, puedan ser entregados a los usuarios finales.

El validador centralizado no tiene competencias de Administrador de los Recursos de Identificación ni actúa en nombre de la CRC. Sus funciones son de naturaleza técnica, operativa y de verificación documental, y se circunscriben a los lineamientos regulatorios establecidos en el presente capítulo y en los actos administrativos que para el efecto expida el Administrador de los Recursos de Identificación. Las decisiones de asignación, recuperación y devolución de los recursos de

identificación son competencia exclusiva de la CRC en su calidad de Administrador de Recursos de Identificación.

ARTÍCULO 6.13.1.2. FINANCIAMIENTO DEL VALIDADOR CENTRALIZADO. Los costos de implementación, gestión, operación y mantenimiento del validador centralizado serán remunerados por parte de los asignatarios de código corto A2P en favor de la persona jurídica que sea seleccionada como validador centralizado, aplicando el principio de orientación a costos más utilidad razonable.

El pago de la tarifa o tarifas acordadas será incorporado al contrato de operación que suscribirá cada asignatario de código corto A2P con el validador centralizado.

La tarifa o tarifas deberán reflejar los costos reales de operación, incluyendo infraestructura tecnológica, personal, garantías y sistemas de seguridad.

La tarifa podrá ser diferenciada según el volumen de tráfico A2P cursado por cada asignatario de código corto A2P o la cantidad de SENDER ID vinculados a su infraestructura, o cualquier otro criterio objetivo acordado, siempre que no genere discriminación injustificada entre los asignatarios de código corto A2P.

ARTÍCULO 6.13.1.3. REQUISITOS DEL VALIDADOR CENTRALIZADO. Para ser seleccionado, el candidato deberá acreditar como mínimo:

6.13.1.3.1. Ser persona jurídica legalmente constituida en Colombia o con sucursal establecida en el país conforme a las disposiciones legales y reglamentarias vigentes.

6.13.1.3.2. Contar con capacidad técnica y operativa suficiente para administrar en tiempo real el proceso de validación de agentes, marcas y plantillas de contenido en los volúmenes del ecosistema A2P nacional, incluyendo disponibilidad de sistemas de información, las interfaces de acceso y la infraestructura de seguridad.

6.13.1.3.3. Acreditar experiencia previa en la administración de sistemas de registro y validación de identidades en el sector de telecomunicaciones o sectores afines, o demostrar capacidad técnica equivalente mediante los estudios, certificaciones y referencias que puedan presentar.

6.13.1.3.4. No tener vínculos accionarios, contractuales o de control con ninguno de los asignatarios de código corto A2P ni con sus matrices, filiales o subordinadas, que puedan comprometer su independencia e imparcialidad. Tampoco podrá tener vínculos accionarios, contractuales o de control con ninguno de los PRSTM ni con sus matrices, filiales o subordinadas, que puedan comprometer su independencia e imparcialidad. En el marco del proceso de selección, el candidato presentará declaración juramentada de ausencia de conflictos de interés, acompañada de certificación del representante legal con la estructura de propiedad y control hasta el nivel del beneficiario final.

6.13.1.3.5. Contar con mecanismos robustos de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de los datos de los agentes registrados, conforme

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

a los estándares internacionales aplicables y a las disposiciones de la Ley 1581 de 2012 y sus normas reglamentarias.

ARTÍCULO 6.13.1.4. VIGENCIA Y CAUSALES DE TERMINACIÓN. La selección de validador centralizado tendrá una vigencia de cinco (5) años. Un año antes del vencimiento de ese plazo, los PRSTM, con acompañamiento de la CRC, adelantarán un nuevo proceso de selección con antelación suficiente para garantizar la continuidad sin interrupciones, ya sea para ratificar al mismo validador centralizado o votar por cambiarlo.

Son causales de revisión anticipada de la decisión de selección las siguientes:

6.13.1.4.1. El incumplimiento grave o reiterado de las obligaciones establecidas en el presente capítulo o en los respectivos contratos.

6.13.1.4.2. La pérdida sobreviniente de alguno de los requisitos del numeral 6.13.1.3. de esta resolución, incluyendo la configuración de un conflicto de interés que comprometa la imparcialidad en el ejercicio de sus funciones.

6.13.1.4.3. La solicitud voluntaria del validador centralizado de dar por terminadas sus funciones, presentada con antelación mínima de un año ante la CRC, la cual tendrá que ser justificada.

6.13.1.4.4. La imposibilidad sobreviniente de continuar ejerciendo sus funciones, incluyendo los casos de liquidación judicial o voluntaria, o la cancelación o suspensión de su matrícula mercantil por autoridad competente.

PARÁGRAFO. En los casos de revisión anticipada que conduzca a la selección de un nuevo validador, o cuando los PRSTM decidan no continuar con el validador actual, el validador saliente garantizará la transferencia ordenada de toda la información, los sistemas y los procesos al nuevo validador o a la CRC, en los términos y plazos que la CRC establezca, con plena observancia de las disposiciones aplicables en materia de protección de datos personales.

ARTÍCULO 6.13.1.5. FUNCIONES DEL VALIDADOR CENTRALIZADO. Son funciones del validador centralizado:

6.13.1.5.1. Recibir, revisar y procesar las solicitudes de registro de los agentes que pretendan ser asignatarios de código corto A2P o SENDER ID, verificando el cumplimiento de los requisitos de debida diligencia establecidos en el presente capítulo.

6.13.1.5.2. Adelantar el proceso de KYC respecto de los potenciales asignatarios de código corto A2P conforme a la Sección 3 del presente capítulo.

6.13.1.5.3. Verificar que los asignatarios de código corto A2P hayan adelantado el proceso de KYC respecto de los potenciales asignatarios de SENDER ID conforme a la Sección 3 del presente capítulo.

6.13.1.5.4. Recibir, revisar y aprobar o rechazar las plantillas de contenido A2P que los asignatarios de SENDER ID sometan a su consideración conforme a la Sección 4 del presente

capítulo. La revisión implica la validación del contenido estático y el sentido del contenido dinámico de la plantilla, para que corresponda con la modalidad declarada de los mensajes.

6.13.1.5.5. Expedir las certificaciones requeridas en los procesos de asignación de código corto A2P y SENDER ID conforme a los artículos 6.4.2.1.7. y 6.12.2.1.8. de la presente resolución.

6.13.1.5.6. Mantener actualizado el registro de los agentes, marcas y plantillas de contenido validadas, con indicación del estado de cada una y del historial de novedades, en los sistemas de información del validador, con base en la información que aparece en el SIGRI y de conformidad con la ejecución de las actividades del validador centralizado.

6.13.1.5.7. Reportar al Administrador de Recursos de Identificación de manera inmediata sobre cualquier indicio de uso indebido de los recursos de identificación, o la existencia de tráfico potencialmente engañoso, o de incumplimiento de las obligaciones de los asignatarios detectado en el ejercicio de sus funciones.

6.13.1.5.8. Mantener listas dinámicas de URLs y dominios utilizados para actividades que incumplen el régimen de recursos de identificación y ponerlas a disposición de los PRST y de los asignatarios de código corto A2P a través de las interfaces definidas para el efecto.

6.13.1.5.9. Atender los requerimientos de información que le formule el Administrador de Recursos de Identificación dentro de los plazos que este establezca.

6.13.1.5.10. Garantizar la disponibilidad permanente del servicio de consulta en tiempo real del estado de los agentes y plantillas registrados, para efectos de que los PRST puedan verificar la validez de los recursos de identificación y de las plantillas antes del enrutamiento de cada mensaje corto de texto en el ecosistema A2P.

6.13.1.5.11. Participar en el Comité Técnico de Seguimiento previsto en la Sección 5 del presente capítulo y en los espacios de coordinación que convoque el Administrador de Recursos de Identificación.

6.13.1.5.12. Ejecutar el proceso de validación anual del SENDER ID previsto en el artículo 6.12.3.3 de la presente resolución, emitiendo las certificaciones de validación correspondientes y notificando al Administrador de Recursos de Identificación los casos de incumplimiento.

ARTÍCULO 6.13.1.6. PROHIBICIONES DEL VALIDADOR CENTRALIZADO. El validador centralizado tiene las siguientes prohibiciones en el ejercicio de sus funciones:

6.13.1.6.1. Compartir, divulgar o comercializar la información de los agentes registrados con terceros distintos del Administrador de los Recursos de Identificación o de las autoridades judiciales o administrativas competentes que la requieran mediante orden escrita motivada.

6.13.1.6.2. Otorgar certificaciones sin haber completado el proceso de verificación documental y de KYC, o expedir certificaciones con información falsa, incompleta o inconsistente.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.13.1.6.3. Establecer vínculos contractuales, accionarios o de control con los agentes que registra y valida, o recibir contraprestaciones distintas a la tarifa o tarifas pactadas en el contrato.

6.13.1.6.4. Delegar en terceros las funciones de verificación documental y de KYC sin autorización expresa del Administrador de los Recursos de Identificación.

6.13.1.6.5. Negar injustificadamente o retardar el procesamiento de solicitudes de registro, de aprobación de plantillas o de expedición de certificaciones que cumplan con los requisitos establecidos en el presente capítulo.

SECCIÓN 2.
REQUERIMIENTOS TÉCNICOS Y OPERATIVOS DEL SISTEMA DE VALIDACIÓN

ARTÍCULO 6.13.2.1. SISTEMA DE INFORMACIÓN DEL VALIDADOR CENTRALIZADO. El validador centralizado deberá disponer de un sistema de información que cumpla como mínimo con las siguientes condiciones técnicas y operativas:

6.13.2.1.1. Disponibilidad. El sistema deberá operar con una disponibilidad mínima del noventa y nueve coma cinco por ciento (99,5%) mensual, medida en ventanas de treinta (30) días calendario. Las ventanas de mantenimiento programado deberán ser notificadas al Administrador de Recursos de Identificación y a los PRST con antelación mínima de setenta y dos (72) horas y no podrán realizarse en horarios de alta demanda de tráfico A2P.

6.13.2.1.2. Capacidad de procesamiento. El sistema deberá tener capacidad suficiente para procesar en tiempo real el volumen de consultas concurrentes del tráfico A2P nacional, con tiempos de respuesta máximos de doscientos (200) milisegundos promedio en condiciones normales y de quinientos (500) milisegundos en condiciones de alta demanda. El validador presentará al Administrador de Recursos de Identificación, con periodicidad semestral, un informe de capacidad del sistema que demuestre el cumplimiento de estos parámetros y proyecte la capacidad necesaria para los doce (12) meses siguientes.

6.13.2.1.3. Interfaces de programación de aplicaciones (APIs). El sistema deberá disponer de APIs seguras y estandarizadas para la integración con los sistemas de los PRST, los asignatarios de código corto A2P y el SIGRI del Administrador de Recursos de Identificación. Las APIs deberán implementar mecanismos de autenticación robusta, cifrado mediante protocolos vigentes y trazabilidad completa de las transacciones realizadas.

6.13.2.1.4. Seguridad de la información. El sistema deberá implementar como mínimo: autenticación multifactor para el acceso administrativo; cifrado de extremo a extremo para la transmisión de datos sensibles; registros de auditoría completos e inmutables de todas las operaciones; mecanismos de detección y respuesta ante incidentes de seguridad; y planes de continuidad del negocio y recuperación ante desastres con tiempos de recuperación compatibles con las exigencias de disponibilidad del servicio. Los registros de auditoría deberán conservarse por un período mínimo de cinco (5) años y contar con mecanismos de integridad criptográfica verificable.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.13.2.1.5. Redundancia y continuidad operativa. El sistema deberá operar sobre infraestructura redundante y contar con mecanismos automáticos de recuperación y conmutación ante fallas, a fin de evitar puntos únicos de falla y garantizar la continuidad de la validación del tráfico A2P nacional.

ARTÍCULO 6.13.2.2. PLAN DE CONTINGENCIA. El validador dispondrá de un plan de contingencia que establezca los mecanismos alternos de validación para casos de falla total o parcial del sistema principal, garantizando continuidad operativa y la trazabilidad de las operaciones realizadas durante la contingencia. El plan deberá incluir como mínimo:

6.13.2.2.1. Listas de emergencia de los agentes y plantillas validadas, disponibles para consulta offline por parte de los PRST durante el tiempo que dure la falla.

6.13.2.2.2. Procedimientos de escalamiento y tiempos máximos de resolución para diferentes tipos de fallas, diferenciando entre fallas parciales y fallas totales del sistema y eventos de degradación del servicio, así como los tiempos máximos de recuperación y restablecimiento de la operación.

6.13.2.2.3. Canales de comunicación alternativos para la notificación de fallas al Administrador de Recursos de Identificación, a los PRST y a los asignatarios de código corto A2P, con tiempos máximos de notificación no superiores a treinta (30) minutos desde la detección de la falla.

6.13.2.2.4. Mecanismos de sincronización para garantizar que las actualizaciones realizadas durante el período de contingencia sean incorporadas al sistema principal una vez restablecida la operación normal.

6.13.2.2.5 Procedimientos para la activación, gestión y finalización del estado de contingencia, incluyendo la identificación de los responsables autorizados para declarar el inicio y terminación de la contingencia.

6.13.2.2.6. Mecanismos de continuidad operativa que permitan a los PRST cursar únicamente tráfico asociado a registros previamente validados y sincronizados antes de la activación de la contingencia.

6.13.2.2.7. Ejercicios de prueba y validación del plan de contingencia, que deberán realizarse como mínimo una (1) vez cada seis (6) meses, dejando evidencia documental de los resultados, incidentes identificados y acciones correctivas implementadas.

SECCIÓN 3.
PROCESO DE CONOCIMIENTO DEL CLIENTE (KYC)

ARTÍCULO 6.13.3.1. OBLIGACIONES DE DEBIDA DILIGENCIA DE LOS ASIGNATARIOS DE CÓDIGO CORTO A2P. Los asignatarios del código corto A2P adelantarán el proceso de conocimiento del cliente (KYC) respecto de cada agente con quien celebren contratos para cursar tráfico A2P, con carácter previo al inicio de la relación contractual y de manera continua durante su vigencia. Este proceso es condición necesaria para que el validador centralizado pueda expedir la certificación requerida para la asignación del SENDER ID conforme al artículo 6.12.2.1.8. de la presente resolución.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

El proceso de KYC comprende como mínimo las siguientes obligaciones:

6.13.3.1.1. Identificación del agente. Verificación de la identidad de la persona natural o jurídica contratante mediante revisión de: certificado de existencia y representación legal con vigencia no superior a noventa (90) días; documento de identidad del representante legal y demás firmantes del contrato; RUT actualizado; y constancia de inscripción en el RPCAI cuando corresponda.

6.13.3.1.2. Identificación del beneficiario final. Identificación de la persona natural que en última instancia ejerce el control sobre la persona jurídica contratante. El potencial asignatario del SENDER ID diligenciará el formato de declaración de beneficiario final que disponga el validador centralizado, el cual será elaborado por este con base en criterios de identificación del beneficiario en materia de prevención del lavado de activos y financiación del terrorismo.

6.13.3.1.3. Verificación del objeto social. Verificación de que el objeto social del agente contratante es compatible con el tipo de contenido que pretende cursar a través del SENDER ID solicitado, y que las actividades comerciales declaradas son coherentes con el volumen y la modalidad de tráfico que se pretende generar.

6.13.3.1.4. Acreditación del derecho al uso del identificador alfanumérico. Verificación de que el agente contratante acredita el derecho al uso de la denominación comercial, marca, razón social o nombre que pretende registrar como SENDER ID, conforme a los documentos del numeral 6.12.2.1.3. del artículo 6.12.2.1. de la presente resolución.

6.13.3.1.5. Evaluación del perfil de riesgo. Evaluación del perfil de riesgo del agente contratante considerando como mínimo: historial de cumplimiento regulatorio en el sector de telecomunicaciones, incluyendo antecedentes de recuperación de recursos de identificación por la CRC; naturaleza del contenido que pretende cursar y su coherencia con el objeto social declarado; volumen de tráfico proyectado y su razonabilidad; y existencia de sanciones, investigaciones o procesos administrativos y/o judiciales en curso relacionados con fraudes a través de servicios de telecomunicaciones.

6.13.3.1.6. Formalización contractual. Celebración de contrato escrito con el agente contratante que establezca expresamente: la obligación del asignatario del SENDER ID de usar el recurso exclusivamente para los fines declarados y aprobados; la obligación de cursar tráfico únicamente a través de plantillas aprobadas y vigentes en el sistema del validador; la obligación de respetar el régimen de consentimiento del usuario por modalidad de contenido; la facultad del asignatario del código corto A2P de suspender el curso de tráfico de manera inmediata ante indicios de uso fraudulento y de reportar dicha suspensión al validador y al Administrador de Recursos de Identificación; y las consecuencias contractuales por incumplimiento, incluyendo la terminación del contrato por reincidencia.

6.13.3.1.7. Conservación de la información. Conservación de la totalidad de la información del KYC durante la vigencia de la relación contractual y por un período mínimo de cinco (5) años contados a partir de la terminación del contrato. Esta información deberá suministrarse al validador y al Administrador de Recursos de Identificación cuando sea requerida.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ARTÍCULO 6.13.3.2. DEBIDA DILIGENCIA CONTINUA. El proceso de KYC no se agota con la verificación inicial. Los asignatarios del código corto A2P adelantarán debida diligencia continua durante toda la vigencia de la relación contractual, que incluya como mínimo:

6.13.3.2.1. Actualización anual de la información del agente contratante, con verificación de la vigencia de los documentos presentados, del mantenimiento de las condiciones de elegibilidad y de la ausencia de nuevos factores de riesgo.

6.13.3.2.2. Monitoreo del tráfico cursado a través de los SENDER ID del agente contratante, conforme a los parámetros de la Sección 4 del presente capítulo, con el propósito de detectar patrones anómalos indicativos de uso fraudulento.

6.13.3.2.3. Revisión de las plantillas de contenido activas del agente contratante, para verificar que el contenido cursado corresponde a las plantillas aprobadas.

6.13.3.2.4. Reporte inmediato al validador y al Administrador de Recursos de Identificación de cualquier novedad relevante en la situación jurídica, financiera o comercial del agente contratante que pueda afectar su elegibilidad como asignatario del SENDER ID o el correcto uso del recurso de identificación.

SECCIÓN 4.
RÉGIMEN DE PLANTILLAS DE CONTENIDO A2P Y OBLIGACIONES DE LOS ACTORES

ARTÍCULO 6.13.4.1. NATURALEZA Y FUNCIÓN DE LAS PLANTILLAS DE CONTENIDO A2P. Las plantillas de contenido A2P son autorizaciones técnicas del validador centralizado que condicionan el envío de tráfico A2P por parte de los asignatarios del SENDER ID.

La aprobación de una plantilla por el validador centralizado es condición necesaria e indispensable para que el asignatario del SENDER ID pueda cursar tráfico A2P. Ningún mensaje A2P podrá ser enrutado por los PRST si no está respaldado por una plantilla aprobada y vigente en el sistema del validador, conforme a las obligaciones del artículo 6.13.4.7. de la presente resolución.

El mal uso de una plantilla aprobada genera consecuencias sobre los recursos de identificación código corto A2P y SENDER ID a través de los cuales se cursó el tráfico indebido, conforme a las causales de recuperación de los artículos 6.4.3.2.6. y 6.12.3.2.12 de esta resolución y a las reglas de atribución de responsabilidad del artículo 6.13.4.4 de la presente resolución.

ARTÍCULO 6.13.4.2. INFORMACIÓN QUE CONTENDRÁN LAS PLANTILLAS DE CONTENIDO A2P. Toda plantilla sometida a aprobación del validador centralizado deberá contemplar como mínimo la siguiente información:

6.13.4.2.1. Identificación del SENDER ID al que se vinculará la plantilla, acreditando que se encuentra asignado e implementado en el SIGRI.

6.13.4.2.2. Identificación del código corto A2P del agente que gestiona la solicitud en nombre del asignatario del SENDER ID, con acreditación de la relación contractual vigente.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.13.4.2.3. Declaración de la modalidad de contenido aplicable conforme a las categorías del artículo 6.12.1.3. de esta resolución, con la justificación correspondiente y la indicación del tipo de consentimiento del usuario aplicable.

6.13.4.2.4. Texto base del mensaje de texto (SMS), con indicación expresa de los campos variables permitidos y la descripción del tipo de información que podrá insertarse en dichos campos.

6.13.4.2.5. Indicación de si el mensaje incluye URLs o dominios y, en caso afirmativo, especificación de cada URL o dominio autorizado, incluyendo los casos de enlaces acortados con indicación del dominio original.

6.13.4.2.6. Declaración expresa de que el contenido de la plantilla no es engañoso, no suplanta identidades de terceros no autorizados y no induce al usuario en error.

6.13.4.2.7. Para las plantillas de modalidad de autenticación y seguridad y de mensajes transaccionales e informativos cuando involucren entidades del sector financiero, acreditación de que el asignatario del SENDER ID es entidad sometida a inspección de la Superintendencia Financiera o que cuenta con autorización expresa del Administrador.

6.13.4.2.8. Para las plantillas de modalidad regulatoria y de interés público, acreditación de la habilitación de la autoridad competente o de la calidad de entidad pública del asignatario del SENDER ID.

ARTÍCULO 6.13.4.3. PROCEDIMIENTO DE APROBACIÓN, MODIFICACIÓN, VIGENCIA Y DESACTIVACIÓN DE PLANTILLAS.

6.13.4.3.1. Procedimiento de aprobación. El validador recibirá las solicitudes de aprobación presentadas por los asignatarios del código corto A2P en nombre de los asignatarios del SENDER ID y las resolverá conforme al siguiente procedimiento:

(i) verificará que la solicitud cumple todos los requisitos del artículo 6.13.4.2; si no los cumple, la rechazará mediante comunicación motivada, como máximo, dentro de las veinticuatro (24) horas siguientes a su recibo;

(ii) verificará que el contenido de la plantilla es coherente con la modalidad de contenido declarada y con el tipo de consentimiento indicado;

(iii) verificará que las URLs o dominios incluidos no figuren en las listas dinámicas del numeral 6.13.1.5.8. de esta resolución y que no presenten indicadores objetivos de actividad potencialmente engañosa;

(iv) verificará que el identificador alfanumérico del SENDER ID vinculado a la plantilla es consistente con el contenido del mensaje y no induce al usuario en error;

(v) si la plantilla cumple todos los requisitos, la aprobará y le asignará un código de identificación interno dentro de las cuarenta y ocho (48) horas siguientes al recibo de la solicitud completa;

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

(vi) si no cumple los requisitos de los literales ii), iii) o iv), la rechazará mediante comunicación motivada dentro de las mismas cuarenta y ocho (48) horas.

PARÁGRAFO 1. Los tiempos de respuesta son máximos. El validador establecerá en su reglamento interno objetivos de tiempo promedio compatibles con los ciclos operativos del ecosistema A2P.

PARÁGRAFO 2. El validador no podrá rechazar una plantilla por razones distintas a las establecidas en el presente numeral. Salvo que el rechazo sea consecuencia de actividad potencialmente engañosa, caso en el cual el validador reportará al Administrador de Recursos de Identificación conforme al numeral 6.13.1.5.7. de esta resolución.

6.13.4.3.2. Modificación de plantillas aprobadas. El asignatario del SENDER ID podrá solicitar la modificación de una plantilla aprobada cuando se presenten cambios en el contenido, en las URLs o dominios, o en la modalidad de contenido. El validador la procesará conforme al numeral 6.13.4.3.1 de esta resolución con los mismos tiempos de respuesta. Durante el trámite de la modificación, la plantilla original continuará vigente. Si la modificación implica un cambio de modalidad incompatible con el SENDER ID vinculado, el validador rechazará la modificación e informará al asignatario que deberá solicitar autorización para la adición de esa modalidad conforme al Parágrafo del artículo 6.12.1.3. de esta resolución.

6.13.4.3.3. Vigencia y desactivación de plantillas. Las plantillas aprobadas tendrán vigencia mensual. La vigencia mensual se renovará automáticamente al vencimiento de cada período, salvo que ocurra alguna de las siguientes circunstancias que den lugar a su desactivación:

i) El asignatario del SENDER ID solicite expresamente al validador la desactivación cuando la campaña o servicio asociado haya concluido y no se prevea su reutilización.

ii) El validador detecte un escenario de mal uso de la plantilla en los términos del artículo 6.13.4.4, caso en el cual procederá a desactivar la plantilla de manera inmediata y reportará el hecho al Administrador de Recursos de Identificación.

iii) El SENDER ID al que está vinculada la plantilla sea recuperado por el Administrador de Recursos de Identificación, caso en el cual todas las plantillas vinculadas al mismo SENDER ID serán desactivadas simultáneamente conforme al Parágrafo 1 del artículo 6.12.3.2. de esta resolución.

iv) El código corto A2P a través del cual fue gestionada la aprobación sea recuperado y no exista otro código corto A2P con relación contractual vigente con el asignatario del SENDER ID, caso en el cual se aplicará el procedimiento del Parágrafo 1 del artículo 6.4.3.2. de esta resolución.

ARTÍCULO 6.13.4.4. ATRIBUCIÓN DE RESPONSABILIDAD POR MAL USO DE PLANTILLAS. La atribución de responsabilidad por mal uso de las plantillas funcionará de conformidad con las siguientes reglas:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.13.4.4.1. Se entiende que existe mal uso de una plantilla cuando el contenido efectivamente cursado difiere del aprobado por el validador, incluyendo: el contenido cursado corresponde a una modalidad distinta a la aprobada; se incluyen URLs o dominios no declarados en la solicitud de aprobación o en su última modificación aprobada; se introduce información que induce al usuario en error; o se cursan mensajes a usuarios inscritos en el RNE en contravención de las restricciones de la modalidad de la plantilla.

6.13.4.4.2. Cuando el mal uso sea directamente imputable al asignatario del SENDER ID, sin intervención ni conocimiento del asignatario del código corto A2P, las consecuencias regulatorias recaerán exclusivamente sobre el SENDER ID conforme a las causales del artículo 6.12.3.2. de esta resolución.

6.13.4.4.3. Cuando el mal uso sea directamente imputable al asignatario del código corto A2P, por haber permitido o facilitado el envío de tráfico no autorizado sin conocimiento del asignatario del SENDER ID, las consecuencias regulatorias recaerán exclusivamente sobre el código corto A2P conforme a las causales del artículo 6.4.3.2. de esta resolución.

6.13.4.4.4. Cuando el mal uso sea imputable de manera concurrente a ambos asignatarios, el Administrador de Recursos de Identificación podrá iniciar procedimientos de recuperación simultáneos o sucesivos sobre ambos recursos, con plena observancia del derecho a la defensa y al debido proceso.

6.13.4.4.5. A efectos de la atribución de responsabilidad, el validador conservará los registros de auditoría de todas las plantillas aprobadas, los mensajes cursados por cada SENDER ID y los eventos de divergencia entre el contenido aprobado y el contenido cursado, y los pondrá a disposición del Administrador de los Recursos de Identificación cuando sean requeridos.

ARTÍCULO 6.13.4.5. OBLIGACIONES ESPECIALES DE LOS ASIGNATARIOS DEL CÓDIGO CORTO A2P. Los asignatarios de código corto A2P tienen las siguientes obligaciones especiales:

6.13.4.5.1. Garantizar que únicamente cursen tráfico A2P a través de su infraestructura los asignatarios de SENDER ID que cuenten con certificación vigente del validador, con los recursos de identificación en estado asignado e implementado en el SIGRI, y con al menos una plantilla de contenido previamente aprobada y vigente.

6.13.4.5.2. Integrar sus plataformas de mensajería con el sistema del validador centralizado a través de las APIs disponibles para la consulta en tiempo real del estado de los recursos de identificación y de las plantillas.

6.13.4.5.3. Notificar al asignatario del SENDER ID, al validador centralizado y al Administrador de Recursos de Identificación, dentro de las veinticuatro (24) horas siguientes a su detección, cualquier incidente de uso indebido del tráfico A2P cursado a través de su infraestructura.

6.13.4.5.4. Suspender de manera inmediata el envío de tráfico de un asignatario de SENDER ID cuando el Administrador de Recursos de Identificación así lo indique.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.13.4.5.5. Informar previamente al Administrador de Recursos de Identificación cualquier cambio en su infraestructura técnica de conexión con los PRST que pueda afectar la trazabilidad del tráfico A2P.

6.13.4.5.6. Mantener actualizado el registro de los asignatarios de SENDER ID que cursan tráfico a través de su infraestructura, con indicación del estado de la relación contractual y de las plantillas activas vinculadas a cada SENDER ID.

ARTÍCULO 6.13.4.6. OBLIGACIONES ESPECIALES DE LOS ASIGNATARIOS DEL SENDER ID. Los asignatarios de SENDER ID tienen las siguientes obligaciones especiales:

6.13.4.6.1. Garantizar que todos los mensajes cursados a través de su SENDER ID correspondan exclusivamente al contenido de las plantillas aprobadas y vigentes en el sistema del validador.

6.13.4.6.2. Obtener, documentar y conservar el consentimiento de los usuarios para el envío de mensajes en las modalidades que lo requieran, conforme a las categorías del artículo 6.12.1.3. de esta resolución.

6.13.4.6.3. Respetar en todo momento las restricciones del RNE aplicables a cada modalidad de contenido conforme al artículo 6.12.1.3. de la presente resolución.

6.13.4.6.4. Garantizar que las URLs y dominios incluidos en los mensajes cursados correspondan exclusivamente a los declarados y aprobados en la plantilla vigente, y que no redirijan a sitios web fraudulentos, maliciosos o no verificados.

6.13.4.6.5. Notificar al asignatario del código corto A2P y al validador, dentro de las veinticuatro (24) horas siguientes a su conocimiento, cualquier indicio de uso indebido de su SENDER ID por parte de terceros no autorizados.

6.13.4.6.6. Mantener actualizada su información en el RPCAI, en la matrícula mercantil que alimenta el RUES y ante el validador.

6.13.4.6.7. Solicitar la desactivación de las plantillas cuando las campañas o servicios asociados hayan concluido y no se prevea su reutilización.

6.13.4.6.8. Completar oportunamente la validación anual ante el validador centralizado conforme al artículo 6.12.3.3 de la presente resolución.

ARTÍCULO 6.13.4.7. OBLIGACIONES ESPECIALES DE LOS PRST. Los PRST tienen las siguientes obligaciones especiales:

6.13.4.7.1. Integrar sus plataformas de mensajería (SMSC) con el sistema del validador centralizado a través de las APIs disponibles, de modo que puedan consultar en tiempo real, previo al enrutamiento de cada mensaje A2P, la validez del código corto A2P, del SENDER ID y de la plantilla de contenido asociados al mensaje.

6.13.4.7.2. Verificar, previo al enrutamiento de cada mensaje A2P, que cuente con un código corto A2P y un SENDER ID en estado asignado e implementado en el SIGRI, y con una plantilla de contenido aprobada y vigente en el sistema del validador. En ausencia de alguno de estos elementos, el PRST deberá bloquear el mensaje impidiendo su entrega al usuario final o, alternativamente, y a elección del PRST, marcarlo con la etiqueta «sin verificar».

6.13.4.7.3. Reportar mensualmente al validador centralizado los mensajes bloqueados por ausencia o invalidez de identificadores o de plantilla. El Administrador de Recursos de Identificación podrá acceder a esa información, previo requerimiento de información enviado al validador centralizado o al PRST.

6.13.4.7.4. Suspender de manera inmediata el envío de tráfico A2P asociado a un código corto A2P, SENDER ID o plantilla de contenido A2P cuando el Administrador así lo indique en el marco de una actuación administrativa de recuperación o de una medida de suspensión preventiva conforme al Parágrafo 3o. del artículo 6.1.1.8. de la presente resolución.

SECCIÓN 5.
COMITÉ TÉCNICO DE SEGUIMIENTO Y COORDINACIÓN OPERATIVA

ARTÍCULO 6.13.5.1. COMITÉ TÉCNICO DE SEGUIMIENTO (CTS). Créase el Comité Técnico de Seguimiento del régimen de recursos de identificación asociados al ecosistema A2P, en adelante CTS, como instancia permanente de carácter consultivo bajo la dirección de la CRC.

6.13.5.1.1. Objeto. El CTS es la instancia mediante la cual la CRC realizará el seguimiento a la implementación y operación del régimen de código corto A2P, SENDER ID y plantillas de contenido A2P, y coordinará la respuesta del ecosistema frente a incidentes de fraude.

6.13.5.1.2. Conformación. El CTS estará conformado por todos los asignatarios de código corto A2P. La CRC presidirá el Comité y ejercerá la secretaría técnica. El validador centralizado participará como invitado permanente, con derecho a voz, pero sin derecho a voto. Podrán ser invitados a sesiones específicas representantes de los PRST, asignatarios de SENDER ID, asociaciones gremiales del sector, entidades del orden nacional con competencias en prevención del fraude cibernético y organismos internacionales de referencia.

6.13.5.1.3. Presidencia. La Presidencia del CTS será ejercida por un Comisionado de la Sesión de Comunicaciones de la CRC o por quien este designe. Ante la ausencia del Presidente actuará quien este designe.

6.13.5.1.4. Secretaría. La Secretaría del CTS será ejercida por la CRC. El Secretario tendrá a su cargo la convocatoria a las sesiones, el levantamiento de actas, el registro y control de la documentación y la información de contacto de los miembros, y el seguimiento a las determinaciones adoptadas.

6.13.5.1.5. Funciones del CTS. Son funciones del CTS:

i) Hacer seguimiento a la implementación del nuevo régimen.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ii) Revisar y proponer la actualización de los parámetros técnicos de monitoreo de tráfico A2P, incluyendo los umbrales de detección de patrones anómalos y los criterios de gestión de las listas dinámicas de URLs y dominios fraudulentos.

iii) Analizar los incidentes de fraude detectados durante el período y proponer acciones correctivas y preventivas.

iv) Facilitar el intercambio de información relevante sobre fraude cibernético entre los actores del ecosistema, con plena observancia de las disposiciones aplicables en materia de protección de datos personales y de confidencialidad de información comercialmente sensible.

v) Proponer a la CRC los ajustes regulatorios que la experiencia de operación del nuevo régimen haga necesarios.

vi) Documentar en actas de sesión las determinaciones técnicas y operativas adoptadas.

6.13.5.1.6. Funciones de la Presidencia del CTS. Son funciones de la Presidencia: presidir las sesiones del CTS; proponer el orden del día; facilitar y dar por terminada la discusión de los temas tratados; proponer al CTS la conformación y realización de mesas de trabajo; e invitar a participar en las sesiones a otras autoridades cuando los temas a tratar así lo requieran.

6.13.5.1.7. Funciones de la Secretaría del CTS. Son funciones de la Secretaría: convocar las sesiones y remitir la documentación pertinente; verificar la asistencia y las facultades de los representantes; consultar el sentido de la votación de los miembros con derecho a voto; levantar las actas de cada sesión; llevar el registro y control de la documentación generada; y llevar el registro de la información de contacto de los miembros del CTS.

6.13.5.1.8. Convocatoria. La Secretaría convocará las sesiones mediante comunicación escrita o correo electrónico a los representantes de los asignatarios de código corto A2P y, cuando sea el caso, al validador centralizado y a otras autoridades invitadas, con antelación mínima de diez (10) días hábiles a la fecha de la sesión. La convocatoria estará disponible en la página web de la CRC. El CTS se reunirá, por lo menos, dos veces al año (una por semestre), sin perjuicio de que la CRC lo convoque de manera extraordinaria cuando las circunstancias del caso lo ameriten.

6.13.5.1.9. Sesiones. Las sesiones iniciarán con la verificación de la asistencia y de las facultades de los representantes. Los temas que se someterán a consideración de los miembros se pondrán en su conocimiento al menos dos (2) días hábiles antes de la sesión. Cuando la Presidencia considere que la discusión de un tema ha sido agotada, lo someterá a votación.

En el acta de cada sesión se incluirán las propuestas que hayan obtenido mayoría simple de los miembros asistentes con derecho a voto, contando un voto por asignatario de código corto A2P. Los votos de abstención sólo se contabilizarán para registro y no se sumarán a ninguna de las opciones. Las posturas cuya votación resulte empatada quedarán incluidas en el acta junto con los argumentos de cada posición.

El acta de cada sesión se cerrará con su lectura y la firma de los representantes presentes. La falta de firma de algún representante no viciará el acta ni las votaciones alcanzadas en la sesión; la Secretaría dejará constancia del hecho e indicará las razones cuando las hubiere.

6.13.5.1.10. Actas. De cada sesión se levantará un acta en la que se especificarán como mínimo: fecha, hora, lugar, orden del día, temas tratados y resultados. Las actas se conservarán en archivo de libre consulta para los miembros del CTS en la CRC y serán publicadas en la página web de la CRC, por vía de una circular, salvo la información que tenga carácter de confidencial o reservado, la cual se mantendrá en archivo independiente.

6.13.5.1.11. Naturaleza y vinculatoriedad de las determinaciones del CTS. Las determinaciones del CTS son de naturaleza consultiva y técnica en relación con la CRC y no limitan su competencia regulatoria. De otra parte, las determinaciones que establezcan parámetros técnicos de operación entre los participantes del ecosistema, tales como especificaciones de las APIs de integración, formatos de reporte de incidentes, protocolos de comunicación entre sistemas, umbrales de monitoreo de tráfico y procedimientos de gestión de contingencias, serán de cumplimiento obligatorio para los asignatarios de código corto A2P, los PRST y el validador centralizado en los términos y plazos establecidos en la respectiva acta de sesión. Esta vinculatoriedad deriva de la obligación regulatoria de participar en el CTS e implementar las condiciones técnicas necesarias para el funcionamiento del nuevo régimen, así como de la autonomía de la voluntad privada entre los actores. Las actas que documenten estas determinaciones no constituyen actos administrativos de carácter particular ni general y no son susceptibles de los recursos de la vía gubernativa. Estas determinaciones deberán ser implementadas por los agentes en los respectivos contratos que se hayan suscrito con el validador centralizado.

6.13.5.1.12. Incumplimiento de las determinaciones técnicas del CTS. El incumplimiento injustificado de las determinaciones técnicas y operativas adoptadas conforme al numeral 6.13.5.1.11 será reportado por la CRC, en su condición de secretaría técnica, a las entidades de control y vigilancia competentes para la imposición de las sanciones que correspondan, sin perjuicio de las demás consecuencias regulatorias establecidas en la presente resolución.

6.13.5.1.13. Vigencia del CTS. El CTS tendrá una vigencia indefinida.

ARTÍCULO 6.13.5.2. SEGUIMIENTO Y REPORTE DE INCIDENTES.

6.13.5.2.1. Ante la detección de un incidente de uso potencialmente engañoso de un recurso de identificación o de mal uso de una plantilla, el validador o el asignatario de código corto A2P que lo detecte notificará al Administrador de Recursos de Identificación a más tardar dentro de las dos (2) horas siguientes.

6.13.5.2.2. La notificación de incidente incluirá como mínimo: la identificación del recurso de identificación y la plantilla involucrados; la descripción de la conducta detectada; la fecha y hora de detección; el volumen de tráfico potencialmente afectado; y las medidas de contención adoptadas de manera inmediata.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.13.5.2.3. Dentro de las cuarenta y ocho (48) horas siguientes a la notificación inicial, el validador centralizado y el asignatario de código corto A2P reportante presentarán al Administrador de Recursos de Identificación un informe completo del incidente que incluya el análisis de causa raíz, la descripción detallada de las medidas de contención y corrección adoptadas y las recomendaciones para prevenir la recurrencia.

6.13.5.2.4. El Administrador de Recursos de Identificación consolidará los reportes de incidentes recibidos y los pondrá a disposición del CTS en cada sesión ordinaria, con indicación de las tendencias identificadas ».

Adiciónese el siguiente formato al TÍTULO REPORTES DE INFORMACIÓN de la Resolución CRC 5050 de 2016:

FORMATO T.5.9 — INFORMACIÓN DE SENDER ID

Periodicidad: Trimestral.

Contenido: Mensual.

Plazo: Hasta 30 días calendario después de finalizado el trimestre.

Este formato deberá ser diligenciado por el Validador Centralizado encargado de la administración, validación y trazabilidad de LOS SENDER ID utilizados en servicios de mensajería SMS A2P, y contendrá la información asociada a los SENDER ID que cursen tráfico a través del esquema de validación centralizado, con el fin de reportar el uso, tráfico, implementación y cumplimiento del recurso asignado.

Vigencia: A partir del vencimiento del período de transición establecido en el artículo 19 de la resolución que adoptó este formato.

Contenido del reporte:

A. Identificación, Relación de Entidades y Tráfico General

Esta parte consolida los datos de control temporal, la caracterización del recurso (SENDER ID), su vinculación con los códigos cortos A2P y los volúmenes de tráfico de red.

1	2	3	4	5	6	7	8	9
						Tráfico cursado SMS		
Año	***Trimestre***	***Mes***	***Sender ID***	***Código corto A2P asociado***	***Razón social del asignatario del código corto A2P***	***Tráfico MT***	***Tráfico MO***	***Cantidad de campañas o contenidos utilizados***

1. Año: Corresponde al año para el cual se reporta la información. Campo numérico entero de 4 dígitos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2. Trimestre: Corresponde al trimestre del año para el cual se reporta la información. Campo numérico entero con valores entre 1 y 4.

3. Mes: Corresponde al mes del trimestre reportado. Campo numérico entero con valores entre 1 y 3.

4. Sender ID: Identificador alfanumérico utilizado para el envío de mensajes SMS y sobre el cual versa la información reportada.

5. Código corto A2P asociado: Código corto A2P habilitado para el uso del Sender ID durante el período reportado.

6. Razón social del asignatario del código corto A2P: Razón social del asignatario del código corto A2P habilitado para el uso del Sender ID.

7. Tráfico cursado SMS MT: Número total de mensajes SMS terminados en terminales móviles y cursados mediante el Sender ID reportado.

8. Tráfico cursado SMS MO: Número total de mensajes SMS originados desde terminales móviles asociados al Sender ID reportado.

9. Cantidad de campañas o contenidos utilizados: Número de campañas, templates, contenidos o estructuras de mensajes asociados al Sender ID durante el período reportado.

B: Validación de Plantillas, Gestión de Fraude y Cumplimiento

Esta parte se enfoca en la operación técnica del Validador Centralizado: la trazabilidad, aprobación o rechazo de plantillas A2P, las alarmas de seguridad y el estado operativo.

1	2	3	4	5	6	7	8	9	10	11	12	13
			Plantillas									
Sender ID	Coincidencias validadas	Rechazos de validación	Pre aprobadas	Aprobadas y vigentes	Solicitudes de aprobación	Aprobadas	Rechazadas y causal	Desactivadas y causa	Incidentes de uso potencialmente fraudulento	Reportes de uso indebido	Estado de implementación	Observación

1. Sender ID: Identificador alfanumérico utilizado para el envío de mensajes SMS y sobre el cual versa la información reportada.

2. Coincidencias validadas: Número de mensajes que cumplieron satisfactoriamente las reglas del esquema de validación centralizada.

3. Rechazos de validación: Número de mensajes rechazados por inconsistencias de validación, trazabilidad o incumplimiento de reglas definidas por el esquema centralizado.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4. Plantillas pre aprobadas: Estructuras base de mensajes validados de forma previa en el sistema antes de su puesta en producción.

5. Plantillas aprobadas y vigentes: Número total de plantillas de contenido A2P aprobadas y vigentes al cierre del período, discriminadas por modalidad de contenido.

6. Solicitudes de aprobación de plantillas: Número de solicitudes de aprobación de plantillas recibidas durante el período reportado.

7. Plantillas aprobadas: Número de plantillas aprobadas durante el período reportado.

8. Plantillas rechazadas y causal: Número de plantillas rechazadas durante el período reportado y causal de rechazo asociada.

9. Plantillas desactivadas y causa: Número de plantillas desactivadas durante el período reportado y causa asociada.

10. Incidentes de uso potencialmente fraudulento: Número de incidentes detectados relacionados con posibles usos fraudulentos de recursos de identificación durante el período reportado.

11. Reportes de uso indebido: Número de reportes remitidos al Administrador de Recursos de Identificación sobre indicios de uso indebido, discriminados por tipo de conducta detectada.
12.Estado de implementación: Estado de utilización efectiva y operativa del Sender ID durante el período reportado.

13. Observación: Campo destinado al registro de incidencias, novedades o situaciones relevantes asociadas al Sender ID reportado».

9.2.1.3 Subtemática 3: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

Situación identificada:	En el mercado colombiano, no se contempla un control sobre el tráfico SMS P2P, especialmente en planes que incluyen mensajes ilimitados. Esta situación abre la puerta a la creación de un mercado secundario, donde usuarios comercializan el saldo de SMS disponibles en su plan, facilitando prácticas como envío masivo de mensajes no autorizados, phishing y suplantación de identidad esta vía. La ausencia de mecanismos de supervisión y límites claros incrementa el riesgo de que las redes móviles se utilicen para actividades ilícitas, afectando la confianza del usuario y la integridad del ecosistema.
Causas relacionadas:	Causa 1: Los desarrollos regulatorios sobre recursos de identificación se han enfocado en su mayoría en la administración y el uso eficiente de dichos recursos escasos. Causa 2: Las medidas de gestión y control frente al contacto fraudulento implementadas por los PRST y asignatarios son insuficientes.
Alternativa 1: Statu quo	Se mantiene el esquema actual, sin introducir controles adicionales sobre el tráfico P2P.

Alternativa 2: Control de patrones de tráfico atípicos	Establece condiciones regulatorias orientadas a la detección, gestión y mitigación del riesgo de uso indebido del servicio de mensajería entre personas (SMS P2P), basado en el análisis del comportamiento del servicio, a mediante la implementación de un enfoque híbrido que combine obligaciones mínimas verificables con un esquema de regulación por objetivos, garantizando la flexibilidad necesaria para la adaptación a la evolución de las tipologías de fraude. Incluye la adopción de alertas automáticas y bloqueos temporales para prevenir el uso fraudulento de planes ilimitados y reducir el mercado secundario.
Alternativa 3: Límite de SMS P2P por usuario	Establecimiento de un tope máximo de mensajes P2P por usuario en un periodo determinado, incluso en planes ilimitados. Una vez alcanzado el límite, se bloquea el envío de nuevos mensajes hasta el siguiente ciclo.

9.2.1.3.1 Alternativa 1: Statu quo

Esta alternativa mantiene el esquema actual, sin introducir controles adicionales sobre el tráfico P2P. Esta opción evita costos de implementación, pero no mitiga el riesgo de mercado secundario ni el uso fraudulento de planes ilimitados.

9.2.1.3.2 Alternativa 2: Control de patrones de tráfico atípicos

Esta alternativa propone la adopción de un enfoque regulatorio híbrido orientado a la gestión del riesgo del fraude en el tráfico SMS P2P, mediante la combinación de obligaciones verificables con un esquema basado en resultados, que brinde la suficiente flexibilidad para que los operadores adapten sus mecanismos y herramientas en función de la evolución dinámica del fenómeno del fraude. Bajo este enfoque, la intervención regulatoria no se centra en proponer soluciones específicas, sino en definir condiciones que aseguren la detección oportuna de comportamientos atípicos y la implementación de acciones eficaces para su mitigación, garantizando al mismo tiempo la posibilidad de supervisión por parte de la CRC.

Esta alternativa es útil porque permite discriminar entre el uso legítimo y el uso abusivo del canal P2P. Al detectar patrones irregulares, como el envío masivo de SMS (usualmente mediante SIM boxes o SIM farms) soportado en planes con SMS ilimitados o de grandes volúmenes, los operadores pueden actuar antes de que se materialice un fraude, evitando que actores maliciosos implemente esquemas de uso irregular que puedan evadir los controles sobre el servicio SMS A2P, por medio de la migración sus acciones con fines de fraude al servicio de SMS P2P.

En el marco de esta alternativa se plantea establecer un conjunto de condiciones regulatorias para que los PRST cuenten con capacidades de monitoreo y gestión del tráfico SMS P2P, asegurando que estos mecanismos sean auditables, trazables y orientados a resultados, sin limitar la posibilidad de innovación tecnológica. De manera específica, tanto los operadores móviles de red (OMR) como los operadores móviles virtuales (OMV) deberán implementar:

- Sistemas de monitoreo del tráfico SMS P2P que permitan identificar comportamientos atípicos[71].

[71] En el marco del análisis de los patrones de tráfico los operadores móviles deberán considerar variables como el volumen de mensajes enviados, la frecuencia de envío por unidad de tiempo, la dispersión de los destinatarios, comportamiento atípico por franjas horarias, tasas de envío superiores a patrones humanos normales, concentración de mensajes en ventanas de tiempo

Los PRST podrán definir e implementar los mecanismos técnicos pertinentes, incluyendo, entre otros:

- analítica de comportamiento,
- modelos de detección de anomalías, basados en modelos probabilísticos, machine learning o redes neuronales.
- variables asociadas a volumen, frecuencia, dispersión o dispositivos utilizados.

- Disponer de procedimientos documentados para la gestión de eventos sospechosos.

Los operadores deberán contar con un procedimiento estandarizado para la gestión de eventos, por medio del cual se describan los pasos a seguir para la mitigación del incidente identificado.

- Mantener registros trazables de:

  - Eventos detectados
  - Análisis realizados
  - Decisiones adoptadas
  - Medidas implementadas.

- Mecanismos de atención a usuarios frente a medidas de control aplicadas y protocolos de gestión escalonada para evitar la limitación del tráfico legítimo.

Cuando se identifiquen patrones atípicos o se superen los umbrales definidos, los PRST deberán implementar un esquema escalonado de gestión del riesgo, que incluya, según el nivel de riesgo identificado:

- Generación de alertas internas.
- Notificación al usuario.
- Validación o autenticación adicional del usuario.
- Restricciones temporales al envío de mensajes.
- Suspensión preventiva del servicio.

- Coordinar con otros PRST y autoridades competentes el intercambio de información relevante sobre el fraude, alertas tempranas e incidentes detectados, así como definir lineamientos técnicos que sirvan como estándar de referencia pare el análisis de los patrones de tráfico del servicio SMS P2P.

El enfoque de ajuste dinámico de los mecanismos de control de esta alternativa implica que, en reconocimiento de la evolución constante de las tipologías y formas de fraude, se plantea que los PRST deberán revisar y actualizar periódicamente sus parámetros de detección, incluyendo los

---

reducidas, envío masivo a múltiples destinatarios únicos, distribuciones geográficas inusuales y picos de tráfico inconsistentes con el perfil histórico del usuario.

Adicionalmente, se deben considerar criterios técnicos como la rotación de tarjetas SIM asociadas a un mismo dispositivo (SIM farms), el uso de equipos con identificadores estáticos (IMEI) vinculados a múltiples líneas, y patrones de localización celular que evidencian comportamientos automatizados. Así como crear un score de confianza del originador de la comunicación basada en enfoques de análisis probabilístico y umbrales dinámicos ajustados a los perfiles normales de consumo

umbrales de referencia y los modelos de análisis, con base en la evolución del tráfico, la aparición de nuevas modalidades de fraude y la efectividad de las medidas implementadas. Es importante señalar que las medidas adoptadas y acuerdos realizados serían elementos vinculantes sujetos de seguimiento en el marco de las funciones de inspección, vigilancia y control. En otras palabras, todas las actividades y plazos detallados dentro de los comités serán vinculantes para sus participantes y cualquier incumplimiento por parte de estos será informado por la CRC a las entidades de control y vigilancia para la imposición de las sanciones correspondientes.

En este contexto, para la materialización de la revisión y actualización periódica de los parámetros de detección de comportamientos atípicos, la CRC promoverá la creación o fortalecimiento de un espacio periódico o recurrente de coordinación, con el fin de:

- Facilitar el intercambio de información relevante sobre fraude.
- Definir lineamientos técnicos y buenas prácticas.
- Realizar seguimiento a la evolución del fenómeno.
- Apoyar la formulación y ajuste de medidas regulatorias.
- Documentar los acuerdos desarrollados para su seguimiento efectivo.

En el anterior contexto, las condiciones de seguimiento y reporte para verificar el cumplimiento de las medidas adoptadas bajo esta propuesta se orientan a que los operadores deberán conservar registros detallados de los eventos detectados, las decisiones adoptadas y las acciones implementadas, así como remitir a la CRC información periódica sobre el desempeño de sus mecanismos de control. Este esquema permitirá evaluar la efectividad de las medidas, identificar posibles brechas y aplicar un enfoque de supervisión basado en riesgo. Los PRST deberán remitir, en el marco del espacio de coordinación, la siguiente información:

- Reporte periódico de desempeño, con contenido mensual:
  - número de eventos detectados,
  - medidas implementadas,
  - tiempos de respuesta.

- Reporte de incidentes relevantes, de manera informativa cuando aplique:
  - eventos de fraude masivo,
  - nuevas tipologías identificadas.

- Reporte de ajustes metodológicos, de manera informativa cuando aplique:
  - cambios en los umbrales definidos,
  - ajustes en los mecanismos de detección.

9.2.1.3.3 Alternativa 3: Límite de SMS P2P por usuario

Esta alternativa propone establecer un límite máximo de mensajes P2P que un usuario puede enviar en un periodo determinado (por ejemplo, por día o por hora), incluso si tiene un plan ilimitado. El objetivo es evitar que las líneas personales se usen como canales masivos de envío.

Esta alternativa se considera útil porque previene el uso comercial o automatizado de líneas personales, sin afectar el uso legítimo de los usuarios comunes. Además, es una medida sencilla de implementar y fácil de monitorear por parte de los operadores.

Como efecto de esta medida se espera una disminución del uso indebido de planes ilimitados, una contención del mercado informal de reventa de tráfico, y una mejora en la seguridad del canal P2P, sin comprometer la experiencia del usuario legítimo.

Con el anterior contexto, esta alternativa propone de manera específica la imposición de un tope máximo de mensajes P2P por usuario en un periodo determinado, incluso en planes que actualmente ofrecen SMS ilimitados. El límite se definiría con base en patrones de uso normal, por ejemplo, estableciendo un umbral diario o mensual que cubra las necesidades típicas de comunicación personal. Una vez alcanzado el límite, el sistema bloquearía automáticamente el envío de nuevos mensajes hasta el siguiente ciclo.

Esta medida busca cerrar la posibilidad de explotación masiva del canal P2P para fines fraudulentos, ofreciendo un mecanismo simple y directo para controlar el volumen de tráfico sin requerir análisis complejos. Aunque este enfoque puede implicar ajustes en la percepción de los planes ilimitados, contribuye a reducir el riesgo de mercado secundario y a proteger la integridad del servicio.

9.2.1.3.4 Evaluación de alternativas

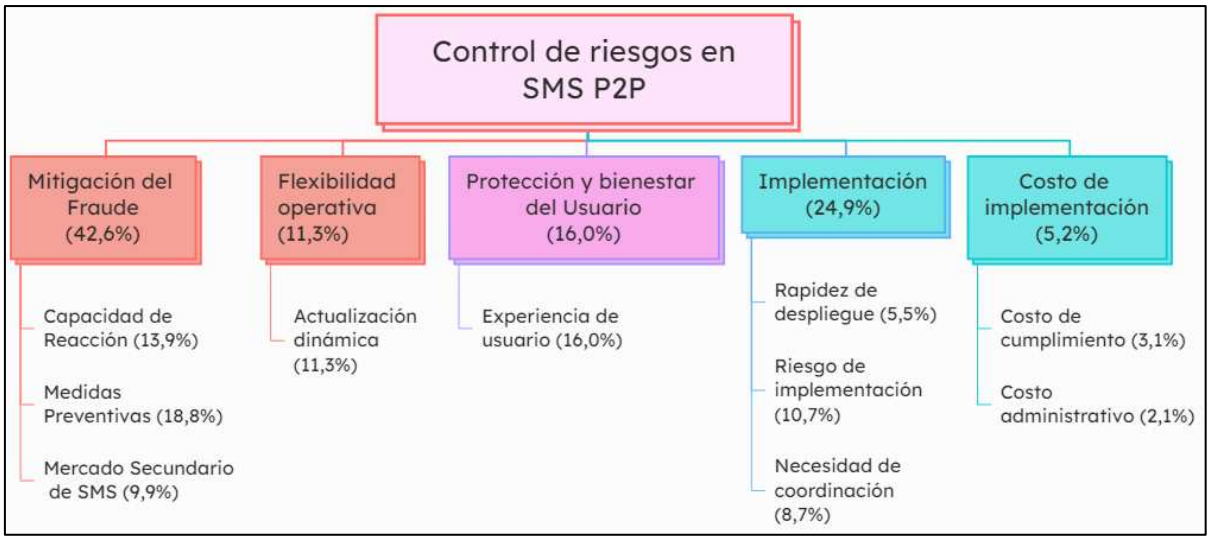
La evaluación de alternativas regulatorias para la temática «Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados» se desarrolló bajo un enfoque basado en el Análisis de Decisión Multicriterio, siguiendo los lineamientos metodológicos definidos para el presente proyecto regulatorio. Este enfoque resulta pertinente dada la necesidad de evaluar de manera integral distintas alternativas regulatorias que presentan efectos diferenciados sobre la mitigación del fraude, la operación del servicio, la experiencia de los usuarios y los costos asociados a su implementación y supervisión.

En este contexto, la aplicación de la metodología requirió evaluar el desempeño relativo de las alternativas regulatorias frente a un conjunto de criterios técnicos, operativos y regulatorios orientados a identificar la capacidad de cada medida para prevenir el uso indebido del servicio SMS P2P, reducir la comercialización irregular de planes con SMS ilimitados y fortalecer la capacidad de reacción frente a nuevas tipologías de fraude, procurando al mismo tiempo preservar el uso legítimo del servicio y evitar cargas desproporcionadas para los operadores y usuarios.

Para el ejercicio de evaluación desarrollado se consideraron cinco criterios y diez subcriterios, los cuales cumplen con los principios fundamentales para la construcción de criterios dentro de ejercicios de evaluación multicriterio, garantizando independencia conceptual, pertinencia frente al problema regulatorio y capacidad de diferenciación entre alternativas. El árbol jerárquico de decisión que ilustra el problema sujeto de evaluación se presenta en la Ilustración 18. Así mismo, la matriz de comparación, el resultado de la prueba de consistencia y la tabulación de ponderadores de los subcriterios se encuentran incluidos en la sección de ANEXOS del presente documento.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 18. Árbol jerárquico de la temática: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados



Fuente: Elaboración CRC

Criterios y Subcriterios

A continuación, se presentan las definiciones de los subcriterios que se establecieron para la evaluación de las diferentes alternativas:

Mitigación del Fraude:

- Capacidad de Reacción: Grado en que la alternativa permite identificar comportamientos anómalos en el tráfico SMS P2P con el fin de gestionar medidas correctivas
- Medidas Preventivas: Medida en que la alternativa reduce la probabilidad de que los usuarios utilicen los accesos móviles para actividades como smishing o envío masivo no autorizado.
- Mercado Secundario de SMS: Grado en que la alternativa desincentiva o limita la comercialización de la capacidad de SMS de planes ilimitados por parte de los usuarios.

Flexibilidad operativa:

- Actualización dinámica: Grado en que la alternativa permite ajustar de manera dinámica y rápida las metodologías de monitoreo y seguimiento de SMS P2P, a fin de adaptarse a nuevas tipologías de fraude.

Protección y bienestar del usuario:

- Experiencia de usuario: Nivel en que la alternativa evita afectar a los usuarios que hacen uso legítimo del servicio.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Implementación:

- Rapidez de despliegue: Tiempo estimado requerido para implementar la alternativa desde su adopción regulatoria hasta su operación efectiva en el mercado.

- Riesgo de implementación: Grado en que la alternativa presenta incertidumbres técnicas, operativas y de gestión del servicio que puedan afectar su adopción efectiva en el control del tráfico SMS P2P, considerando la necesidad de desarrollar o adaptar capacidades de monitoreo de comportamiento, la implementación de reglas de control o limitación del servicio, la afectación sobre la operación normal del tráfico y la posibilidad de aplicación consistente entre usuarios y operadores.

- Necesidad de coordinación: Grado en que la alternativa requiere articulación entre múltiples actores de tal manera que presenta, con mecanismos de coordinación simples, una menor dependencia de acuerdos entre actores.

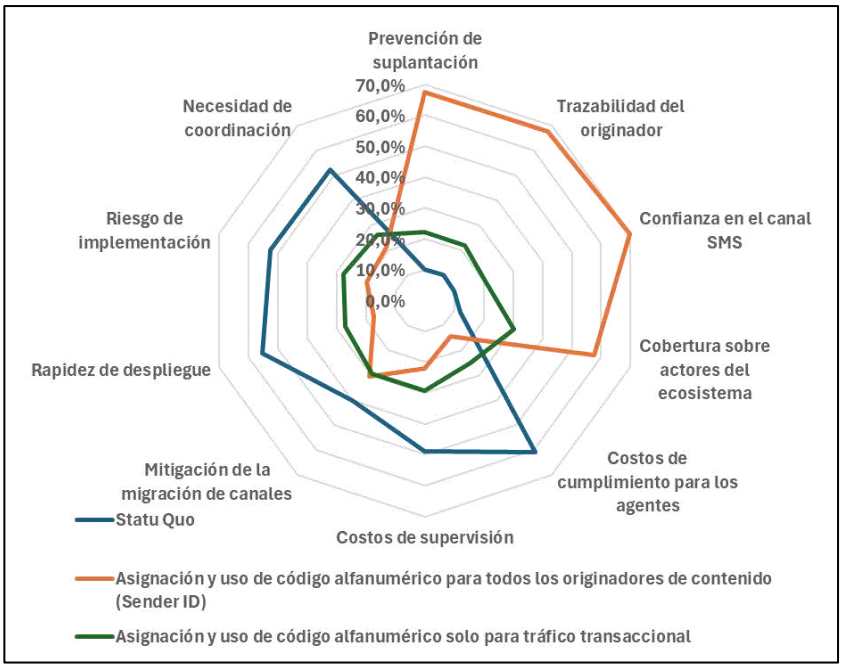
Costos de implementación

- Costos de cumplimiento para PRST: Costos técnicos, operativos y administrativos que deben asumir los operadores para implementar mecanismos de control, monitoreo o limitación.

- Costos de supervisión: Nivel de recursos que la autoridad regulatoria debe destinar para monitorear, verificar y hacer cumplir la medida.

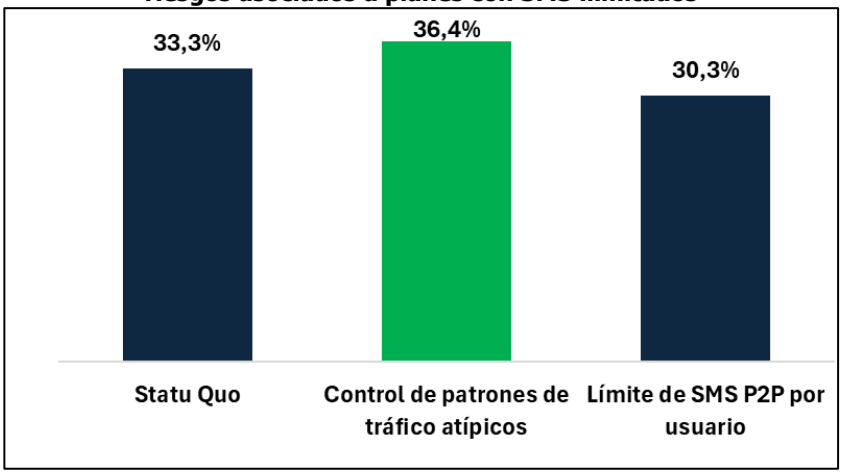
Los resultados que se exponen en la Ilustración 19 corresponden al porcentaje de desempeño relativo alcanzado por cada alternativa regulatoria en cada uno de los subcriterios evaluados, una vez aplicado el respectivo ponderador definido dentro del modelo de Análisis de Decisión Multicriterio. Por su parte, en la Ilustración 20 se presenta el desempeño global agregado obtenido por cada alternativa para la temática «Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados». De esta manera, la evaluación permite identificar la alternativa que ofrece el mejor balance integral entre la capacidad de mitigación del uso indebido del servicio SMS P2P, la flexibilidad para adaptarse a nuevas tipologías de fraude, la protección de la experiencia de los usuarios legítimos y los costos e implicaciones asociados a su implementación y supervisión.

Ilustración 19. Desempeño relativo de las alternativas de la temática: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados



Fuente: Elaboración CRC.

Ilustración 20. Puntaje agregado de cada alternativa de la temática: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados



Fuente: Elaboración CRC.

A continuación, se presenta la descripción del desempeño de las alternativas regulatorias evaluadas frente a cada uno de los criterios considerados.

a. En cuanto al criterio de capacidad de reacción, este evalúa el grado en que las alternativas permiten identificar comportamientos anómalos en el tráfico SMS P2P con el propósito de gestionar medidas correctivas frente a posibles usos fraudulentos. La alternativa de «Statu Quo» presenta el menor desempeño relativo (18,9%), dado que mantiene el esquema actual sin incorporar capacidades adicionales de monitoreo, detección o gestión de eventos sospechosos asociados al tráfico P2P.

   La alternativa de «Límite de SMS P2P por usuario» presenta un desempeño intermedio (22,8%), en la medida en que introduce una restricción preventiva sobre el volumen de mensajes enviados, aunque sin incorporar mecanismos dinámicos de análisis o reacción frente a nuevas tipologías de fraude.

   Por su parte, la alternativa de «Control de patrones de tráfico atípicos» presenta el mejor desempeño en este criterio (58,2%), debido a que incorpora capacidades permanentes de monitoreo, analítica de comportamiento y gestión escalonada de eventos sospechosos, permitiendo identificar y reaccionar oportunamente frente a patrones irregulares o anomalías en el tráfico SMS P2P.

b. Respecto del criterio de medidas preventivas, este evalúa el grado en que las alternativas reducen la probabilidad de utilización de accesos móviles para actividades asociadas a smishing, envío masivo no autorizado o explotación fraudulenta de planes ilimitados. La alternativa de «Statu Quo» presenta el menor desempeño relativo (12,5%), debido a que no incorpora controles específicos orientados a prevenir el uso indebido del servicio SMS P2P.

   Las alternativas regulatorias propuestas presentan desempeños superiores. La alternativa de «Control de patrones de tráfico atípicos» alcanza un desempeño de 42,7%, mientras que la alternativa de «Límite de SMS P2P por usuario» obtiene el mejor desempeño relativo (44,8%). Este resultado se explica porque la imposición de límites explícitos sobre el volumen de mensajes constituye una medida preventiva directa frente a esquemas de envío masivo o comercialización irregular del servicio, reduciendo estructuralmente la posibilidad de utilización abusiva de líneas móviles personales.

c. En relación con el criterio de mercado secundario de SMS, este evalúa el grado en que las alternativas desincentivan o limitan la comercialización de la capacidad de SMS de planes ilimitados. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (36,8%), debido a que evita restricciones adicionales que puedan alterar el funcionamiento actual del mercado minorista de servicios móviles, aunque mantiene abiertos incentivos para la explotación irregular del canal P2P.

   La alternativa de «Límite de SMS P2P por usuario» presenta un desempeño de 33,9%, debido a que introduce restricciones explícitas sobre el volumen de tráfico permitido, limitando parcialmente la posibilidad de comercialización masiva de mensajes.

   Por su parte, la alternativa de «Control de patrones de tráfico atípicos» obtiene un desempeño de 29,3%, considerando que, si bien permite detectar y gestionar comportamientos sospechosos, depende de la efectividad de los modelos de monitoreo y de la actualización continua de parámetros de detección para contener de manera efectiva el mercado secundario de SMS.

d. En cuanto al criterio de actualización dinámica, este evalúa la capacidad de las alternativas para adaptarse de manera rápida y flexible a nuevas tipologías de fraude y patrones de comportamiento irregular. La alternativa de «Statu Quo» presenta un desempeño limitado (16,8%), debido a que no incorpora mecanismos regulatorios específicos orientados a la actualización periódica de metodologías de control.

   La alternativa de «Límite de SMS P2P por usuario» alcanza un desempeño intermedio (24,4%), dado que la medida se basa principalmente en umbrales fijos de tráfico, lo que limita su capacidad de adaptación dinámica frente a nuevas modalidades de fraude.

   Por su parte, la alternativa de «Control de patrones de tráfico atípicos» presenta el mayor desempeño relativo (58,8%), debido a que incorpora explícitamente mecanismos de ajuste periódico de umbrales, modelos de detección y parámetros de monitoreo, permitiendo adaptar las medidas de control a la evolución constante de las tipologías fraudulentas.

e. Respecto del criterio de experiencia de usuario, este evalúa el nivel en que las alternativas evitan afectar a los usuarios que hacen uso legítimo del servicio SMS P2P. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (52,2%), dado que mantiene intactas las condiciones actuales de uso del servicio sin introducir restricciones adicionales sobre el tráfico de los usuarios.

   La alternativa de «Control de patrones de tráfico atípicos» presenta un desempeño intermedio (31,2%), debido a que incorpora mecanismos escalonados de gestión del riesgo y protocolos orientados a evitar la afectación del tráfico legítimo, aunque existe la posibilidad de generar restricciones temporales derivadas de eventos sospechosos.

   Finalmente, la alternativa de «Límite de SMS P2P por usuario» presenta el menor desempeño relativo (16,6%), considerando que la imposición de topes máximos de mensajes puede afectar usuarios con patrones intensivos de uso legítimo y modificar la percepción asociada a los planes ilimitados.

f. En relación con el criterio de rapidez de despliegue, este evalúa el tiempo requerido para implementar las alternativas desde su adopción regulatoria hasta su operación efectiva. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (56,2%), dado que no requiere adecuaciones técnicas ni regulatorias adicionales.

   La alternativa de «Límite de SMS P2P por usuario» alcanza un desempeño intermedio (26,9%), debido a que requiere ajustes relativamente simples sobre plataformas de gestión del tráfico y definición de umbrales de envío.

   Por su parte, la alternativa de «Control de patrones de tráfico atípicos» presenta el menor desempeño relativo (16,8%), considerando que implica el desarrollo e integración de capacidades avanzadas de monitoreo, analítica de comportamiento y gestión dinámica del riesgo.

g. En cuanto al criterio de riesgo de implementación, este evalúa el nivel de incertidumbre técnica, operativa y de gestión asociado a la adopción efectiva de las medidas regulatorias. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (46,8%), debido a que no incorpora cambios técnicos u operativos sobre las redes y plataformas actuales.

La alternativa de «Límite de SMS P2P por usuario» presenta un desempeño intermedio (37,6%), dado que su implementación se basa principalmente en mecanismos de control volumétrico relativamente simples.

Por el contrario, la alternativa de «Control de patrones de tráfico atípicos» presenta el menor desempeño relativo (15,5%), debido a la complejidad asociada al despliegue de capacidades de monitoreo avanzado, ajuste continuo de parámetros y gestión homogénea de medidas de control entre operadores.

h. Respecto del criterio de necesidad de coordinación, este evalúa el grado de articulación requerido entre múltiples actores para implementar las alternativas regulatorias. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (40,1%), debido a que mantiene el esquema actual sin requerir mecanismos adicionales de coordinación sectorial.

   La alternativa de «Límite de SMS P2P por usuario» presenta un desempeño intermedio (33,9%), dado que requiere principalmente coordinación interna por parte de los operadores para la definición y aplicación de límites.

   Por su parte, la alternativa de «Control de patrones de tráfico atípicos» presenta el menor desempeño relativo (26,0%), debido a la necesidad de articular mecanismos de intercambio de información, definición de buenas prácticas y espacios de coordinación sectorial para el seguimiento y actualización de los mecanismos de detección y gestión del riesgo.

i. En relación con el criterio de costos de cumplimiento para PRST, este evalúa los costos técnicos, operativos y administrativos que deben asumir los operadores para implementar mecanismos de control, monitoreo o limitación del servicio. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (51,2%), dado que no requiere inversiones adicionales ni adecuaciones sobre las capacidades actuales de operación.

   La alternativa de «Límite de SMS P2P por usuario» alcanza un desempeño intermedio (30,6%), considerando que requiere ajustes limitados sobre plataformas de gestión y facturación.

   Por el contrario, la alternativa de «Control de patrones de tráfico atípicos» presenta el menor desempeño relativo (18,2%), debido a la necesidad de desarrollar capacidades avanzadas de monitoreo, analítica y gestión dinámica del tráfico SMS P2P.

j. Finalmente, el criterio de costos de supervisión evalúa el nivel de recursos requeridos por la autoridad regulatoria para monitorear y verificar el cumplimiento de las medidas. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (60,3%), dado que mantiene los mecanismos actuales de supervisión sin incorporar nuevas cargas regulatorias.

   La alternativa de «Límite de SMS P2P por usuario» presenta un desempeño intermedio (23,7%), mientras que la alternativa de «Control de patrones de tráfico atípicos» obtiene el menor desempeño relativo (16,0%), considerando que el enfoque basado en monitoreo dinámico y regulación orientada a resultados implica mayores necesidades de seguimiento, verificación y análisis por parte de la autoridad regulatoria.

En resumen, el análisis multicriterio evidencia que la alternativa «Control de patrones de tráfico atípicos» presenta el mejor desempeño global entre las opciones evaluadas, alcanzando un puntaje agregado de 36,4%. Esta alternativa sobresale particularmente en criterios asociados a capacidad de reacción, actualización dinámica y fortalecimiento de mecanismos preventivos, debido a que incorpora un enfoque flexible y adaptativo orientado a la detección temprana y mitigación de nuevas tipologías de fraude sobre el canal SMS P2P.

No obstante, esta alternativa también implica mayores costos de implementación y supervisión, así como mayores necesidades de coordinación sectorial frente a las demás opciones analizadas. Por su parte, la alternativa de «Statu Quo» presenta ventajas importantes en términos de simplicidad operativa, menores costos y rapidez de despliegue, aunque mantiene las limitaciones actualmente identificadas frente al uso indebido del servicio.

Finalmente, la alternativa de «Límite de SMS P2P por usuario» presenta desempeños intermedios en la mayoría de los criterios evaluados, reflejando un enfoque preventivo más restrictivo y de implementación relativamente simple, aunque con mayores riesgos de afectación sobre usuarios legítimos y menor capacidad de adaptación dinámica frente a nuevas modalidades de fraude.

Conclusión

Así las cosas, de acuerdo con los resultados obtenidos, la alternativa que presenta el mejor desempeño global corresponde a la alternativa 2, «Control de patrones de tráfico atípicos», con un puntaje agregado de 36,4%. En segundo lugar, se ubica la alternativa 1, correspondiente al «Statu Quo», con 33,3%, seguida de la alternativa 3, «Límite de SMS P2P por usuario», con 30,3%.

Este resultado se explica porque la alternativa ganadora obtiene los mejores desempeños en los criterios más directamente relacionados con la solución del problema regulatorio identificado, particularmente en capacidad de reacción (58,2%), actualización dinámica (58,8%) y medidas preventivas (42,7%), atributos que resultan fundamentales para enfrentar esquemas de fraude que evolucionan continuamente y que utilizan patrones de tráfico cada vez más complejos.

Si bien el Statu Quo presenta ventajas en experiencia de usuario, costos de cumplimiento, costos de supervisión y facilidad de implementación, dichos resultados obedecen principalmente a la ausencia de nuevas obligaciones regulatorias, por lo que no generan mejoras sustanciales frente a las causas que originan la problemática identificada. En consecuencia, su buen desempeño se concentra en criterios asociados a menores costos y riesgos regulatorios, más que en la capacidad efectiva de mitigar el fraude.

Por su parte, la alternativa de «Límite de SMS P2P por usuario» muestra fortalezas en la reducción preventiva de usos indebidos del servicio y en la simplicidad de implementación; sin embargo, su enfoque basado en umbrales fijos limita su capacidad de adaptación frente a nuevas tipologías de fraude y genera mayores riesgos de afectación sobre usuarios con patrones legítimos de uso intensivo.

En este contexto, la evaluación evidencia que la alternativa de «Control de patrones de tráfico atípicos» ofrece el mejor equilibrio entre efectividad regulatoria, capacidad de adaptación y sostenibilidad de largo plazo, al incorporar mecanismos dinámicos de monitoreo y gestión del riesgo que permiten responder de manera más flexible a la evolución de los comportamientos fraudulentos en el ecosistema

SMS, razón por la cual se identifica como la alternativa con mejor desempeño integral para atender la problemática analizada.

9.2.1.3.5 Propuesta regulatoria «Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados»

La propuesta regulatoria para la alternativa ganadora implicará modificar el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016, que actualmente regula la obligación general de los operadores de hacer uso de herramientas tecnológicas para prevenir la comisión de fraude, con la finalidad de incluir obligaciones particulares relacionadas con la prevención del fraude en el tráfico P2P.

Específicamente, se dispondrá que los PRST deberán implementar sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P) orientados a la detección oportuna de patrones de uso atípico que sean indicativos de un posible uso fraudulento del servicio, incluyendo en particular los patrones asociados al uso masivo de planes con SMS ilimitados o con alto saldo para cursar tráfico de naturaleza A2P disfrazado de P2P, al funcionamiento de granjas de SIM o a la comercialización del saldo de mensajes de texto entre usuarios.

En consecuencia, cada PRST podrá seleccionar libremente las herramientas técnicas, los algoritmos y las metodologías de análisis que considere más eficientes para alcanzar los objetivos de detección y respuesta establecidos en el presente artículo, siempre que acredite ante la CRC que los sistemas de monitoreo implementados tienen la capacidad de detectar, como mínimo: (i) Volumen inusual de mensajes salientes por usuario; (ii) Alta dispersión de destinatarios; (iii) Homogeneidad del contenido; (iv) Periodicidad mecánica[72]; (v) Ausencia de tráfico entrante correlacionado; y (vi) Concentración geográfica o de red. Estas obligaciones estarán acompañadas de un procedimiento de verificación de alertas y unos plazos particulares para cumplir con las medidas impuestas.

Seguidamente se incorpora la propuesta regulatoria:

Modificar el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, el cual quedará así:

«**ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES.** Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude:

2.1.10.7.1. Obligaciones generales:

2.1.10.7.1.1. Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y debe hacer controles periódicos respecto a la efectividad de estos mecanismos.

2.1.10.7.1.2. Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) que pueda tener relación con un presunto fraude, el operador debe investigar sus causas; y en caso de que determine la no existencia de un fraude, le debe demostrar al usuario las razones por las cuales no procede su PQR (petición, queja/ reclamo o recurso). Sin embargo, si se demuestra

[72] Se refiere a un patrón de envío de mensajes que se repite en intervalos regulares, constantes o altamente predecibles, típicamente generado por sistemas automatizados (máquinas) y no por un comportamiento humano normal.

que el usuario actuó diligentemente en el uso del servicio contratado, no habrá lugar al cobro de los consumos objeto de reclamación.

2.1.10.7.2. Obligaciones particulares:

2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.

2.1.10.7.2.1.1. Los Proveedores de Redes y Servicios de Telecomunicaciones deberán implementar sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P) orientados a la detección oportuna de patrones de uso atípico que sean indicativos de un posible uso fraudulento del servicio, incluyendo en particular los patrones asociados al uso masivo de planes con SMS ilimitados o con alto saldo para cursar el tráfico de naturaleza A2P simulado como P2P, al funcionamiento de granjas de SIM o a la comercialización del saldo de mensajes de texto entre usuarios. En consecuencia, cada PRST podrá seleccionar libremente las herramientas técnicas, los algoritmos y las metodologías de análisis que considere más eficientes para alcanzar los objetivos de detección y respuesta establecidos en el presente artículo, siempre que acredite ante la CRC que los sistemas de monitoreo implementados tienen la capacidad de detectar, como mínimo: (i) Volumen inusual de mensajes salientes por usuario; (ii) Alta dispersión de destinatarios; (iii) Homogeneidad del contenido; (iv) Periodicidad mecánica[73]; (v) Ausencia de tráfico entrante correlacionado; y (vi) Concentración geográfica o de red.

2.1.10.7.2.1.2. Una vez el sistema de monitoreo detecte en una línea o conjunto de líneas la configuración de alguno de los patrones descritos anteriormente, el operador aplicará el siguiente esquema de respuesta escalonado, progresando de una etapa a la siguiente cuando la etapa anterior no haya resultado en la cesación del patrón detectado dentro del plazo establecido:

> **Primera etapa — Alerta interna y análisis.** El sistema de monitoreo registrará el evento de detección en los logs del PRST con la identificación de la línea o líneas involucradas, el patrón detectado, la fecha y hora de inicio y el volumen de tráfico asociado. El PRST analizará el evento con el propósito de descartar falsas alarmas, para lo cual podrá considerar el historial de comportamiento de la línea, el tipo de plan contratado y cualquier otro factor de contexto relevante. Esta etapa no podrá exceder de veinticuatro (24) horas desde la detección del evento.
>
> **Segunda etapa — Notificación al usuario.** Si superada la primera etapa el PRST concluye que el patrón detectado no corresponde a una falsa alarma, notificará al usuario titular de la línea o líneas afectadas, a través del canal de atención que el usuario haya habilitado, informándole sobre el comportamiento atípico detectado en su línea, las posibles consecuencias para la prestación del servicio si el patrón continúa, y los canales disponibles para que el usuario manifieste la existencia de una causa legítima que explique el comportamiento. El usuario tendrá un plazo de cuarenta y ocho (48) horas desde la notificación para manifestarse. Si el usuario acredita una causa legítima a satisfacción del PRST, este registrará el hecho en su sistema y no procederá a las etapas siguientes.

[73] Se refiere a un patrón de envío de mensajes que se repite en intervalos regulares, constantes o altamente predecibles, típicamente generado por sistemas automatizados (máquinas) y no por un comportamiento humano normal.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tercera etapa — Autenticación adicional. Si vencido el plazo de la segunda etapa el usuario no se ha manifestado o la causa alegada no es satisfactoria, o si el patrón de tráfico continúa o se intensifica, el PRST podrá exigir al usuario la realización de una autenticación adicional para continuar usando el servicio de mensajería, a través de los mecanismos que el PRST defina para el efecto. Si el usuario no completa la autenticación dentro de las cuarenta y ocho (48) horas siguientes al requerimiento, el PRST procederá a la siguiente etapa.

Cuarta etapa — Restricción temporal del servicio de mensajería. Si superadas las etapas anteriores el patrón atípico persiste o el usuario no ha completado la autenticación requerida, el PRST podrá restringir temporalmente la capacidad de envío de mensajes de texto de la línea o líneas identificadas. La restricción tendrá una duración máxima de siete (7) días calendario, al vencimiento de los cuales se levantará automáticamente si no se han presentado nuevos eventos de detección. La restricción no afectará la capacidad del usuario de recibir mensajes de texto ni de realizar o recibir llamadas de voz.

Quinta etapa — Reporte a la CRC y decisión sobre continuidad de la relación contractual. Si la restricción temporal no elimina el patrón de uso atípico o si la línea vuelve a exhibir el mismo patrón dentro de los treinta (30) días calendario siguientes al levantamiento de la restricción, el PRST reportará el caso a la CRC y el PRST quedará habilitado para evaluar y decidir, conforme a las condiciones contractuales aplicables y a las disposiciones del régimen de protección de usuarios establecido en el presente título, la terminación del contrato de prestación del servicio con el usuario titular de la línea.

El esquema de respuesta escalonado previsto en el presente numeral no podrá ser aplicado de manera discriminatoria entre usuarios con el mismo perfil de comportamiento. El PRST deberá asegurar que los criterios de activación de cada etapa sean uniformes, objetivos y verificables.

2.1.10.7.2.1.3. La aplicación del esquema de respuesta escalonado no exime al PRST de su obligación de atender las PQR que el usuario afectado presente en relación con la restricción del servicio de mensajería, conforme al régimen de PQR vigente. El usuario tendrá derecho a solicitar en cualquier momento la revisión de la medida adoptada, acreditando que su comportamiento de uso responde a una causa legítima.

2.1.10.7.2.1.4. Los Proveedores de Redes y Servicios de Telecomunicaciones tienen la obligación de participar en el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles que se crea en virtud del artículo 2.1.10.7.3 de la presente resolución. En el referido comité los participantes podrán proponer y acordar la forma de mejorar los parámetros mínimos de detección descritos en el numeral 2.1.10.7.2.1.1 cuando la evolución de las modalidades de fraude así lo requiera. En caso de que no haya propuestas o acuerdos de actualización o mejora, aplicarán los estándares mínimos establecidos en el mencionado numeral.

2.1.10.7.2.1.5. Los PRST deberán implementar los sistemas de monitoreo previstos en el presente artículo y acreditar su puesta en operación ante la CRC dentro de los tres (3) meses siguientes a la publicación en el Diario Oficial de la resolución que los adoptó. La acreditación se realizará mediante la presentación ante la CRC de un informe técnico que describa la arquitectura

del sistema implementado, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas. Dentro de los seis (6) meses siguientes a la presentación de ese primer informe, los PRST remitirán un segundo informe a la CRC que contendrá lo siguiente:

a. El número de eventos de detección de patrones de tráfico P2P atípico registrados en el período transcurrido desde la implementación de las medidas, discriminado por tipo de patrón detectado.

b. El número de casos en que el sistema descartó el evento como falso positivo en la primera etapa del esquema de respuesta, con indicación de los factores de contexto que motivaron esa determinación.

c. El número de casos en que el usuario manifestó una causa legítima en la segunda etapa y el PRST aceptó dicha justificación, con indicación agregada del tipo de causa alegada.

d. El número de restricciones temporales del servicio de mensajería aplicadas en la cuarta etapa, discriminado por duración de la restricción.

e. El número de casos reportados a la CRC en la quinta etapa y el número de terminaciones contractuales derivadas de la aplicación del presente artículo.

f. Los umbrales y criterios aplicados por el PRST para la detección de cada uno de los patrones, con indicación de las actualizaciones realizadas a dichos criterios durante el período reportado.

g. Las PQR recibidas en relación con la aplicación del presente artículo, con indicación de su resultado».

9.2.2 Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

9.2.2.1 STIR/SHAKEN/RCD - Alternativa transversal para todas las subtemáticas

Esta alternativa propone exigir que todas las llamadas nacionales e internacionales entrantes estén firmadas digitalmente mediante el protocolo STIR/SHAKEN/RCD, garantizando la autenticidad del número mostrado al usuario en su dispositivo.

Bajo este escenario, debe entenderse como STIR/SHAKEN/RCD lo siguiente:

- **STIR** (Identidad Telefónica Segura Revisitada o en inglés *Secure Telephone Identity Revisited*): técnica / protocolo criptográfico base para autenticar el origen de la llamada.
- **SHAKEN** (Gestión Basada en Firmas de la Información Afirmada mediante Tokens o inglés *Signature-based Handling of Asserted information using tokens*): marco de implementación para que STIR funcione a escala operativa entre operadores, definiendo procedimientos y políticas de certificado digital.

- **RCD** (Datos Enriquecidos de la Llamada o en inglés *Rich Call Data*): capa adicional que permite mostrar al usuario receptor información enriquecida y verificada, construida sobre STIR/SHAKEN para incorporar metadatos verificados asociados al llamante —como nombre, logotipo o motivo de la llamada— con el fin de fortalecer la confianza del usuario receptor.

En este contexto, se incorpora la posibilidad de incluir información enriquecida de la llamada (RCD por sus siglas en inglés Rich Call Data)[74] en el token SHAKEN (PASSPorT), lo que permite implementar el identificador de llamadas con información de la marca (Branded Caller ID) que consiste en que el PRST receptor puede mostrar el nombre, logo y motivo de la llamada si el dispositivo del usuario lo soporta. El objetivo es fortalecer la verificación, autenticación e identificación del originador de la llamada (marca), reducir el *spoofing* y mejorar la trazabilidad y confianza en el canal de voz.

Los operadores de red deberían hacer las adecuaciones necesarias en sus plataformas de señalización y enrutamiento para soportar la autenticación criptográfica de llamadas mediante el protocolo STIR/SHAKEN, teniendo en cuenta que cada llamada originada debe ser firmada digitalmente por el operador de origen, generando un token PASSPorT que viaja en la señalización SIP.

El PRST receptor debe validar la firma digital y verificar el nivel de confianza en la identificación del originador, la cual estará definida en los siguientes tres (3) niveles:

- **Nivel A (Verificación completa)**: El operador de origen está seguro de que el número que aparece como remitente realmente pertenece a la persona que está haciendo la llamada.

- **Nivel B (Verificación parcial)**: El operador conoce a la persona que envía la llamada, pero no puede garantizar que el número mostrado realmente le pertenece.

- **Nivel C (Sin verificación)**: El operador simplemente está transmitiendo la llamada, pero no tiene información sobre el originador real.

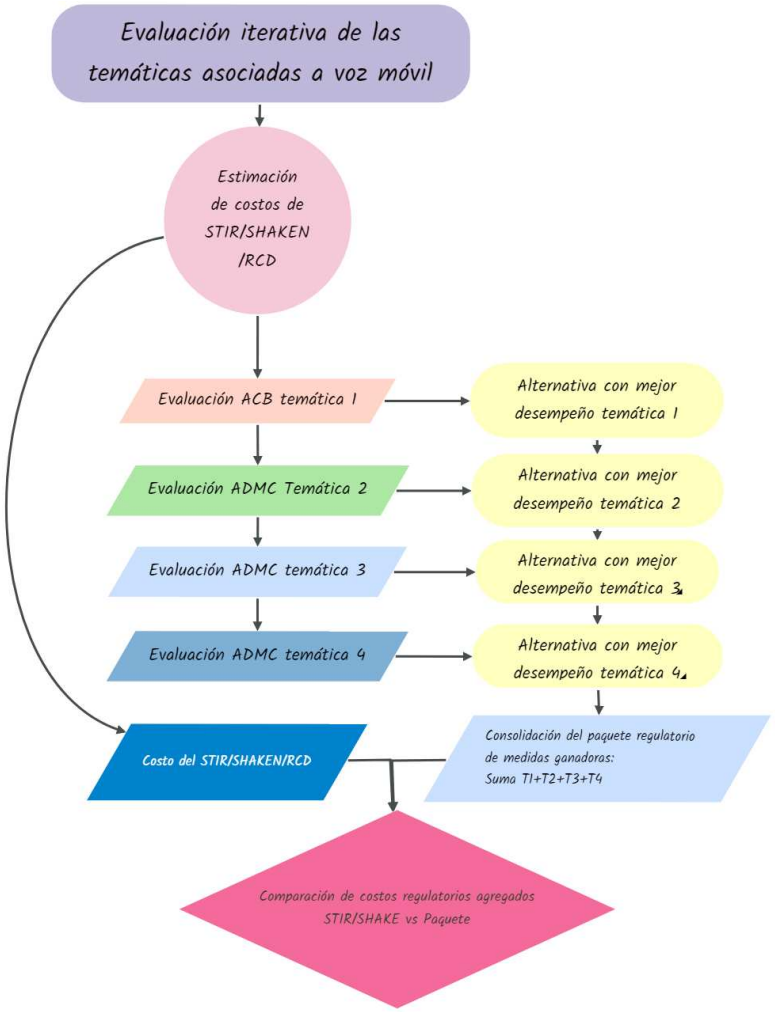
Las llamadas que no cuenten con firma válida o presenten bajo nivel de verificación pueden ser bloqueadas, marcadas como «No verificada» o «Probable fraude», o sujetas a revisión adicional.

Adicionalmente, si la llamada incluye Rich Call Data, el receptor debería poder mostrar el nombre, logo y motivo de la llamada definidos por el originador de la llamada en el dispositivo del usuario.

En consideración a que la alternativa «Implementación de STIR/SHAKEN/RCD» se encuentra incorporada transversalmente como opción regulatoria en las distintas subtemáticas evaluadas para el servicio de voz móvil, su evaluación requiere un tratamiento metodológico diferenciado frente a las demás alternativas regulatorias. Lo anterior obedece a que la implementación de esta arquitectura tecnológica genera importantes economías de escala y sinergias regulatorias entre las diferentes problemáticas asociadas al fraude mediante voz móvil, particularmente en materia de autenticación del identificador de línea llamante (CLI), trazabilidad del tráfico, etiquetado de llamadas y fortalecimiento de mecanismos de prevención del spoofing y el vishing.

[74] Según la Internet Engineering Task Force (IETF) Rich Call Data (RCD) es un objeto extensible de metadatos asociados con la identidad del llamante o con la sesión de llamada, que va más allá del número de teléfono — por ejemplo, el nombre del llamante, logotipo, foto, un objeto jCard representativo del llamante, o el motivo de la llamada.

Ilustración 21. Enfoque de evaluación para «STIR/SHAKEN/RCD» como alternativa transversal



Fuente: Elaboración CRC.

En este sentido, es necesario anotar que evaluar de manera independiente la alternativa STIR/SHAKEN/RCD dentro de cada temática podría conducir a una sobreestimación de sus costos regulatorios, debido a que una parte significativa de las inversiones requeridas en infraestructura, integración, operación y certificación serían compartidas entre múltiples funcionalidades regulatorias. Por esta razón, la CRC definió que la evaluación de esta alternativa se desarrollará mediante un enfoque complementario basado en Costos Administrativos, orientado a comparar el costo regulatorio agregado de implementar STIR/SHAKEN/RCD frente al costo total derivado del conjunto de medidas regulatorias que resulten ganadoras en las diferentes subtemáticas evaluadas para el servicio de voz móvil.

Bajo el enfoque metodológico presentado en la Ilustración 21, primero se realiza la evaluación individual de cada temática mediante ADMC, identificando la alternativa con mejor desempeño relativo

en cada caso. Posteriormente, las alternativas ganadoras se integran en un «paquete regulatorio de medidas», cuyo costo agregado de implementación es estimado de manera conjunta, considerando costos de adecuación técnica, operación, supervisión y coordinación. Finalmente, dicho paquete regulatorio es comparado frente al costo integral de implementar una solución unificada basada en STIR/SHAKEN/RCD, la cual incorpora mecanismos de autenticación, verificación y enriquecimiento del identificador de llamadas mediante Rich Call Data (RCD).

9.2.2.2 Subtemática 1: Limitaciones al enmascaramiento de la identidad de la línea llamante (CLI)[75] (Spoofing)

Situación identificada:	Actualmente no se cuenta con la obligación de implementar mecanismos de verificación, autenticación e identificación del originador de la llamada de voz, y al mismo tiempo no existe una prohibición explícita ni mecanismos robustos para impedir que llamadas internacionales entrantes utilicen números del Plan Nacional de Numeración (PNN) como identificador (CLI). Esta práctica, conocida como CLI masking o enmascaramiento, sin un mecanismo de verificación, autenticación e identificación del originador de la llamada, permite a los delincuentes simular llamadas locales en otros países, o suplantar la identidad de personas o instituciones públicas o privadas, aumentando la efectividad de fraudes como *vishing* y *phishing* telefónico, y dificultando posterior identificación de la trazabilidad por parte de las autoridades judiciales en las investigaciones.
Causa relacionada:	Causa 1: Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso. Causa 2: Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes.
Alternativa 1: Statu quo.	Mantiene el marco actual sin controles adicionales sobre el uso de numeración E.164. Los PRST cursan llamadas sin verificar la autenticidad de la identidad de la línea llamante (CLI) ni restringir el uso de números nacionales en tráfico internacional.
Alternativa 2: Prohibición total del enmascaramiento de la identidad de línea llamante (CLI)	Obliga a los operadores a bloquear todas las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número colombiano, salvo excepciones de roaming legítimo, eliminando un canal importante de suplantación. Los *carriers* internacionales que estén interconectados con operadores en Colombia para la terminación de tráfico en la red móvil nacional deberán cumplir con las recomendaciones de la UIT-T E.164 respecto a los formatos y longitudes de numeración que corresponden a cada país, respetando los códigos del país donde se origina la llamada, para limitar en lo posible el tráfico con numero A inconsistente o modificado. Los operadores nacionales bloquearán el tráfico internacional entrante cuando detecten que no se cumple esta condición.

[75] Recomendación UIT-T E.164 (11/2010) La Identidad de la Línea Llamante o Conectada (CLI/COLI) es una información de dirección utilizada por la red para habilitar servicios como la presentación del número de quien llama. En llamadas internacionales, debe seguir el formato E.164 completo (código de país, código nacional de destino y número de abonado), sin incluir prefijos ni símbolos adicionales. Puede asociarse una subdirección si aplica. El uso de números específicos de red o la autorización para transferir la CLI/COLI entre países son asuntos de regulación nacional. Además, el mecanismo NPI/TON debe especificar el tipo o categoría de numeración empleada.

Alternativa 3: Permitir enmascaramiento con obligación de identificación y etiquetado de llamadas para el usuario	Permite llamadas internacionales con identificador de línea llamante (CLI) nacional o uso de numeración con formatos o longitudes de numeración que no corresponden a la recomendación UIT-T E.164 para el país con el que se identifica al usuario llamante, pero exige que sean identificadas y etiquetadas como «Alerta de llamada sospechosa» o «Alerta de probable fraude» en el dispositivo del usuario, alertando sobre posible riesgo de suplantación.
Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional	Requiere que todas las llamadas estén firmadas digitalmente mediante STIR/SHAKEN, incorporando *Rich Call Data* (RCD) para autenticidad y visualización de información del originador, bloqueando o marcando llamadas no verificadas.

9.2.2.2.1 Alternativa 1: Statu quo

Esta alternativa consiste en mantener el marco regulatorio actual, en el cual no existe obligación para los PRST de implementar mecanismos de verificación, autenticación o identificación del originador de la llamada de voz. Asimismo, no se contemplaría una prohibición explícita ni herramientas robustas para impedir que llamadas internacionales entrantes utilicen números del Plan Nacional de Numeración (PNN) como identidad de la línea llamante (CLI), ni tampoco para impedir que llamadas internacionales deban cumplir con las recomendaciones de la UIT-T E.164 respecto a los formatos y longitudes de numeración que corresponden a cada país, respetando los códigos del país donde se origina la llamada.

Bajo este escenario, algunas llamadas internacionales podrían seguir presentándose ante el usuario como si fueran colombianas o utilizando numeración extranjera que no sigue los formatos E.164, sin que el PRST tenga la obligación de validar si existe evidencia de enmascaramiento de la identidad de línea llamante.

9.2.2.2.2 Alternativa 2: Prohibición total del enmascaramiento de la identidad de línea llamante (CLI)

Esta alternativa consiste en establecer una prohibición explícita y obligatoria para que los PRST bloqueen todas las llamadas de origen internacional que se identifiquen con un CLI colombiano, es decir, aquellas llamadas desde otros países que se presenten al usuario como números atribuidos en Colombia, salvo en aquellos casos justificados de itinerancia internacional (roaming legítimo).

En términos operativos, los operadores de red móvil deben implementar mecanismos automáticos en sus plataformas de señalización y enrutamiento para identificar llamadas de origen internacional que utilicen numeración nacional como identidad de línea llamante (CLI). Al detectar una llamada internacional con identidad llamante correspondiente a un CLI colombiano, el sistema debe verificar si corresponde a un caso de roaming internacional legítimo (por ejemplo, mediante listas de IMSI, registros de usuarios en roaming, o acuerdos de interconexión).

En caso de que la llamada no corresponda a un escenario de roaming internacional legítimo, el sistema deberá bloquearla antes de su terminación en el usuario final. En otras palabras, toda llamada proveniente del exterior que presente un identificador de llamada (CLI) colombiano no deberá completarse hacia el usuario receptor, sino ser retenida o bloqueada por el sistema.

Se exceptuarían de la obligación de bloqueo las llamadas originadas por usuarios en roaming internacional legítimo, siempre que se pueda verificar la autenticidad del origen y la CRC podría establecer excepciones para servicios críticos, emergencias o situaciones especiales.

También se establece la obligación que tendrán los carriers internacionales que estén interconectados con operadores en Colombia para la terminación de tráfico en la red móvil nacional, de cumplir con las recomendaciones de la UIT-T E.164 respecto a los formatos y longitudes de numeración que corresponden a cada país, respetando los códigos del país donde se origina la llamada, para limitar en lo posible el tráfico con numero A inconsistente o modificado.

Adicionalmente se establece la posibilidad que tendrán los operadores móviles nacionales que estén interconexiones con carriers internacionales para que bloqueen el tráfico internacional entrante en aquellos casos donde detecten que el CLI que identifica el número de origen de la llamada no cumple con la recomendación UIT-T E.164 respecto a los formatos y longitudes de numeración del país donde se origina la llamada.

Tal como lo indican los comentarios sectoriales, una de las modalidades principales mediante las cuales se contacta por vía telefónica a los usuarios de servicios móviles con fines fraudulentos es mediante llamadas de tráfico internacional entrante que enmascaran el origen real de la llamada haciendo uso de una identidad de línea llamante (CLI) que corresponde a un número que forma parte del plan nacional de numeración de Colombia. Esta modificación del origen real de la llamada tiene como propósito generar confianza en el usuario que la recibe para que atienda la comunicación y por se facilite el fraude. Al establecer un bloqueo de todo el tráfico internacional entrante que enmascare el origen real de la llamada haciendo uso de un número nacional, se elimina una de las fuentes principales de suplantación y se logra mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz móvil.

Por otra parte, al imponer dicha obligación a los carriers internacionales que estén interconectados con operadores en Colombia para la terminación de tráfico en la red móvil nacional, indicándoles que deben cumplir con las recomendaciones de la UIT-T E.164, en particular respecto a los formatos, longitudes y códigos de numeración del país donde se origina la llamada, se limitan las opciones de que los usuarios en Colombia reciban llamadas con número de identificación llamante inconsistente o modificado. Además, al facultar a los operadores móviles colombianos para que bloqueen el tráfico internacional entrante cuando detecten que no se cumple esta condición, se generan condiciones ciertas y verificables que permiten el cumplimiento de la medida.

En ese contexto, el efecto esperado de esta medida es eliminar la principal vía de suplantación y *spoofing*, asegurando que el número mostrado al usuario corresponda realmente al origen de la llamada, fortaleciendo la trazabilidad y la protección frente a fraudes como *vishing* y *phishing* telefónico.

9.2.2.2.3 Alternativa 3: Permitir enmascaramiento con obligación de identificación y etiquetado de llamadas para el usuario

Esta alternativa propone permitir que se cursen llamadas internacionales entrantes que utilizan números colombianos como identificador de llamada (CLI), o uso de numeración con formatos o longitudes de numeración que no corresponden a la recomendación UIT-T E.164 para el país con el que se identifica al usuario llamante, pero exige que dichas llamadas sean marcadas por el PRSTM

colombiano que recibe el tráfico internacional, de manera que se despliegue en el dispositivo del usuario final un mensaje como «Alerta de llamada sospechosa» o «Alerta de probable fraude». El objetivo es alertar al usuario sobre el posible riesgo de suplantación, sin bloquear el tráfico legítimo.

Para ello, los PRST deben usar sistemas que permitan identificar llamadas internacionales entrantes con identidad de línea llamante (CLI) nacional o que no cumplan con la recomendación UIT-T E.164 en su identificación de identidad de línea llamante, y al detectar este tipo de llamadas, añadir una etiqueta visible «Alerta de llamada sospechosa» o «Alerta de probable fraude») en el identificador de llamada o en inglés Caller ID del usuario receptor, siempre que el dispositivo lo soporte.

Se establecería adicionalmente un procedimiento para actualizar las reglas de etiquetado del identificador de la llamada en el dispositivo del usuario conforme evolucionen los patrones de fraude y las capacidades técnicas de los dispositivos.

Se exceptuarían de la obligación de bloqueo las llamadas originadas por usuarios en roaming internacional legítimo, siempre que se pueda verificar la autenticidad del origen, y la CRC podría establecer excepciones para servicios críticos, emergencias y/o situaciones especiales.

Esta alternativa resulta útil porque su principal característica es que no se genera bloqueo de tráfico. Esto impide que se rechacen llamadas que eventualmente puedan ser legítimas, y deja la decisión de contestar o no la llamada al usuario final, el cual al recibir la «Alerta de llamada sospechosa» o «Alerta de probable fraude» en su dispositivo, cuenta con información que lo previene sobre el posible riesgo de suplantación.

En este contexto, como los usuarios reciben una alerta al momento de recibir una llamada internacional entrante cuando está usando un número del plan nacional de numeración colombiano, o cuando se está usando un número internacional que no está conforme con la recomendación UIT-T E.164, se genera un mecanismo de mitigación en el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz móvil, fortaleciendo la protección frente a fraudes como *vishing* y *phishing* telefónico.

Para mejorar su efectividad, esta medida requiere de programas de educación a los usuarios para que puedan utilizar la información del etiquetado de llamadas en su proceso de toma de decisiones al momento de contestar la llamada.

9.2.2.2.4 Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional

Ver explicación completa de la alternativa en el numeral 9.2.2.1.

9.2.2.2.5 Evaluación de alternativas

La evaluación para seleccionar la alternativa regulatoria más adecuada para abordar las limitaciones al enmascaramiento de la identidad de la línea llamante (CLI Spoofing) se desarrolló bajo un enfoque de análisis costo-beneficio, siguiendo los lineamientos metodológicos descritos en la sección 9.1 del presente documento y manteniendo consistencia con el enfoque aplicado para la evaluación de la

temática «Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude», desarrollada en la sección 9.2.1

Este enfoque resulta pertinente considerando que las distintas alternativas regulatorias evaluadas presentan impactos diferenciados tanto en términos de efectividad para mitigar el fraude asociado al uso indebido del identificador de llamada, como en los costos de implementación, adecuación tecnológica, interoperabilidad y supervisión que deben asumir los distintos actores del ecosistema de voz móvil.

En este contexto, la aplicación de esta metodología requirió evaluar simultáneamente:

(i) la capacidad de cada alternativa para reducir los riesgos asociados al uso fraudulento del Caller Line Identification (CLI);
(ii) su capacidad para mejorar la autenticidad, confiabilidad y trazabilidad de las llamadas recibidas por los usuarios; y
(iii) los costos asociados a la implementación de mecanismos de validación, etiquetado, bloqueo, monitoreo y supervisión regulatoria.

Así las cosas, para estimar los beneficios derivados de las medidas orientadas a combatir el vishing en Colombia, se tomó como referencia el valor de las reclamaciones reportadas ante la Superintendencia Financiera de Colombia[76] asociadas a esquemas de ingeniería social soportados en llamadas telefónicas fraudulentas. En línea con lo desarrollado para el análisis de smishing en la sección 9.2.1, el beneficio económico asociado a las medidas regulatorias se define como el valor de las pérdidas económicas que potencialmente podrían evitarse mediante la reducción de acciones fraudulentas desarrolladas a través de comunicaciones de voz móvil.

En este sentido, el beneficio económico de cada alternativa regulatoria corresponde a los recursos financieros que dejarían de verse afectados por actividades de vishing como resultado de la implementación de mecanismos orientados a:

- reducir la posibilidad de spoofing o suplantación del CLI;
- fortalecer la identificación de llamadas sospechosas;
- mejorar la autenticidad del identificador de llamada;
- y aumentar la capacidad de los usuarios y operadores para detectar comunicaciones potencialmente fraudulentas.

Bajo esta lógica, la efectividad de las medidas regulatorias se refleja en su capacidad para disminuir el valor esperado de las reclamaciones asociadas a fraude mediante llamadas telefónicas reportadas al sistema financiero.

Ahora bien, en primera medida resulta necesario establecer cuáles podrían ser las pérdidas potenciales derivadas de este tipo de acciones fraudulentas. Para ello, se toma como línea base el valor de las reclamaciones realizadas por usuarios del sistema financiero como consecuencia de pérdidas ocasionadas mediante esquemas de ingeniería social asociados a la modalidad de vishing. De acuerdo con la información reportada por la Superintendencia Financiera de Colombia, analizada en la sección

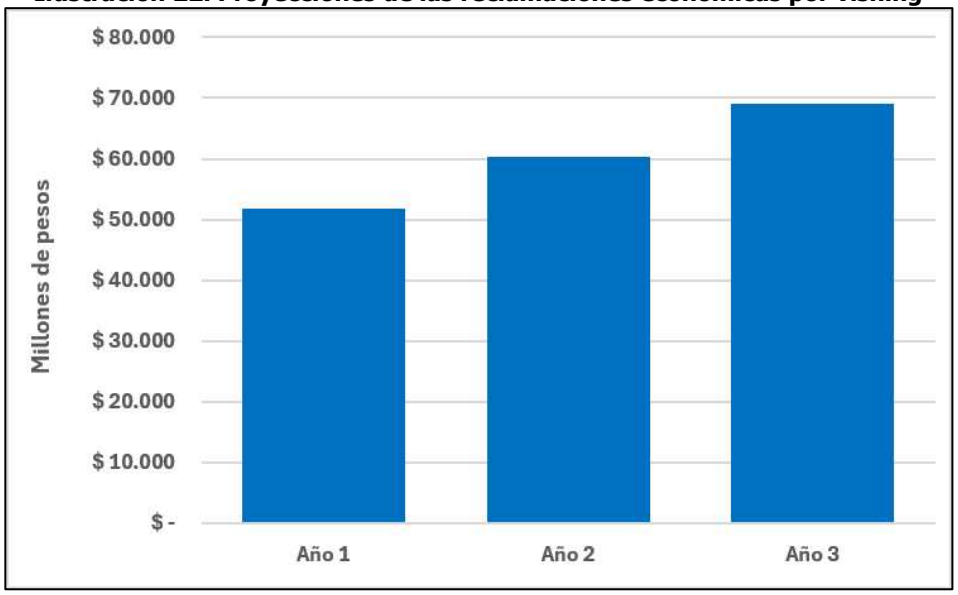
[76] Superfinanciera. Número de Radicación: 2025166778-000-000. Asunto: Radicado Remisión de información sobre la afectación económica de los usuarios por fraude cibernético (smishing y vishing)

correspondiente a ASPECTOS TÉCNICOS, ECONÓMICOS Y JURÍDICOS, las reclamaciones relacionadas con esta modalidad de fraude han presentado una tendencia creciente durante los últimos años, tanto en frecuencia como en valor económico reclamado.

Esta información permite aproximar el nivel de afectación económica atribuible al uso fraudulento de comunicaciones de voz y constituye un referente observable para estimar el beneficio potencial derivado de las medidas regulatorias propuestas. En consistencia con el enfoque metodológico aplicado en la evaluación de smishing, se tomó un periodo de tres (3) como horizonte temporal de análisis, proyectando la evolución esperada de las pérdidas económicas asociadas al vishing bajo un escenario sin intervención regulatoria.

La Ilustración 22 evidencia un incremento significativo de las reclamaciones asociadas a fraude mediante llamadas telefónicas a partir de 2023, seguido de una tendencia creciente y sostenida durante los períodos posteriores. En consecuencia, para estimar el comportamiento esperado de las pérdidas económicas asociadas al vishing se empleó un ejercicio de proyección basado en regresión lineal utilizando los períodos con mayor materialización observable del fenómeno, siguiendo el mismo enfoque desarrollado en la sección 9.2.1 para la proyección de las afectaciones económicas por smishing.

Ilustración 22. Proyecciones de las reclamaciones económicas por vishing



Fuente: Elaboración propia a partir de la Superintendencia Financiera de Colombia[77]

Los resultados de la proyección observados evidencian que, de mantenerse las tendencias actuales y en ausencia de medidas regulatorias o mecanismos efectivos de mitigación, las pérdidas económicas asociadas al vishing continuarían incrementándose de manera significativa durante los próximos años, consolidándose como una fuente creciente de afectación económica para los usuarios y para el ecosistema digital en general. Ahora bien, una vez estimado el escenario base de pérdidas económicas

[77] Ídem

asociadas al vishing en ausencia de intervención regulatoria, resulta necesario determinar el nivel de efectividad que podrían alcanzar las distintas alternativas propuestas para reducir dichas afectaciones.

En este sentido, y al igual que en el análisis desarrollado para smishing, debido a que no existe información estadística nacional que permita medir ex ante el impacto específico de cada medida sobre la reducción del fraude mediante spoofing o llamadas fraudulentas, la CRC recurrió al análisis de experiencias internacionales, estudios sectoriales, literatura académica, reportes técnicos y documentación elaborada por autoridades regulatorias, organismos multilaterales y entidades especializadas en fraude y ciberseguridad.

A partir de esta evidencia se construyeron escenarios prospectivos de efectividad que permiten aproximar el potencial de reducción de pérdidas económicas derivado de la implementación de las medidas regulatorias evaluadas.

Es importante señalar que la extrapolación de resultados internacionales al contexto colombiano presenta limitaciones metodológicas asociadas a diferencias en la arquitectura de redes, los niveles de adopción tecnológica, los mecanismos de autenticación implementados, las capacidades de supervisión, los patrones de comportamiento de los usuarios, y las tipologías predominantes de fraude.

Por esta razón, la CRC adoptó un enfoque basado en escenarios de sensibilidad, consistente con el utilizado para la evaluación de las medidas orientadas a combatir el smishing, con el propósito de capturar distintos niveles posibles de desempeño de las alternativas regulatorias y reducir la incertidumbre inherente al ejercicio de estimación.

Bajo esta aproximación, para cada alternativa regulatoria se definieron tres escenarios de efectividad:

- un escenario pesimista, que representa condiciones de implementación con menores niveles de adopción, efectividad parcial de los controles o adaptación rápida de los esquemas de fraude;
- un escenario moderado o base, que representa un nivel de efectividad esperado bajo condiciones normales de implementación y operación;
- y un escenario optimista, que representa condiciones de implementación robusta, alta coordinación sectorial y mayor efectividad de los mecanismos de prevención, autenticación y validación del identificador de llamada.

En términos generales, la literatura y la experiencia internacional analizada permitieron sustentar los siguientes resultados:

Alternativa 2: Prohibición total del enmascaramiento de la identidad de línea llamante (CLI)

La principal referencia internacional para esta alternativa corresponde a las medidas implementadas en Irlanda y Australia para reducir llamadas fraudulentas asociadas a suplantación de identidad mediante el uso indebido del identificador de llamada. En el caso de Irlanda, el estudio elaborado por

Europe Economics para ComReg[78] identificó el CLI spoofing como uno de los mecanismos más relevantes mediante los cuales las personas fraudulentas inducen a los usuarios a creer que reciben llamadas de organizaciones legítimas o números familiares. El estudio señala que los tipos más prominentes de scam calls involucran la suplantación del CLI, incluyendo números fijos y móviles de organizaciones de confianza.

Para efectos de la modelación de beneficios, el estudio de ComReg estimó que las medidas de bloqueo asociadas al CLI podrían tener una efectividad inicial elevada, iniciando en un 90% de efectividad, con un declive posterior asociado a la adaptación de las personas fraudulentas hacia otros mecanismos de contacto hasta llegar al 80%[79]. En línea con esta aproximación, y considerando que la alternativa propuesta se orienta a bloquear llamadas internacionales entrantes que utilizan CLI nacional enmascarado o numeración no conforme con la recomendación UIT-T E.164, se considera que esta medida tiene una relación causal directa con la reducción del vishing originado mediante spoofing.

De manera complementaria, en Australia la implementación del *Reducing Scam Calls Code* fue asociada por la *Australian Competition and Consumer Commission* (ACCC) con una reducción de casi el 50% en los reportes de estafas telefónicas recibidos por dicha autoridad en 2022. La ACCC destaca que este resultado estuvo asociado al trabajo desarrollado por *Australian Communications and Media Authority* (ACMA), la industria de telecomunicaciones y otras entidades para combatir las llamadas fraudulentas.

País	Intervención	Supuesto	Efectividad	
			Inicial	Declive
Irlanda	Mobile CLI blocking	Se establece un valor intermedio entre las medidas de efectividad reportadas en las experiencias internacionales analizadas, con un declive posterior asociado a la adaptación de las personas fraudulentas.	**-75%**	**-65%**
Australia	Reducing Scam Calls Code			

Con fundamento en estas referencias, se propone utilizar un valor intermedio entre estos resultados como base para el análisis de esta alternativa, para posteriormente establecer los siguientes escenarios de efectividad para esta alternativa:

Escenarios propuestos para el análisis de sensibilidad

Pesimista 60%

Moderado 75%

[78] COMREG. Economic assessment of measures to address CLI spoofing and scam calls [en línea]. Irlanda: Commission for Communications Regulation, 2023 [consultado: 14 de mayo de 2026]. Disponible en: https://www.comreg.ie/media/2023/06/ComReg-2352a.pdf.com

[79] Esta estimación se basa en el análisis de la experiencia en Finlandia en la implementación del bloqueo de CLI enmascarado en los servicios móviles.

Optimista 90%

Estos valores reflejan que la medida actúa directamente sobre el vector técnico que habilita el spoofing del CLI, pero reconocen que su efectividad puede disminuir en el tiempo por desplazamiento del fraude hacia números internacionales no falsificados, llamadas sobre otros canales o nuevas modalidades de suplantación.

Alternativa 3: Permitir enmascaramiento con obligación de identificación y etiquetado de llamadas para el usuario.

La alternativa de etiquetado de llamadas presenta una lógica distinta a las medidas de bloqueo o autenticación fuerte. En este caso, la intervención no impide necesariamente que la llamada llegue al usuario, sino que introduce una señal visible en el identificador de llamada para advertir sobre un posible riesgo de suplantación, fraude o irregularidad en el CLI. Por tanto, su efectividad depende no solo de la capacidad técnica de detección de llamadas sospechosas, sino también de la reacción del usuario frente a la advertencia desplegada.

La evidencia académica disponible muestra que el etiquetado de llamadas puede modificar el comportamiento de los usuarios. En particular, el estudio *Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators*[80], presentado en NDSS, encontró que ciertos diseños de advertencia redujeron en 43% el número de llamadas falsas contestadas cuando la alerta eliminaba el nombre del llamante y utilizaba un fondo rojo en la pantalla.

País	Intervención	Supuesto	Efectividad	
			Inicial	Declive
Estado Unidos (Florida)	Spam call warning	El diseño de la etiqueta elimina el nombre del llamante y utiliza un fondo rojo en la pantalla. Se asume un declive de la efectividad dada la dependencia de la educación de los usuarios, saturación de información, precisión de la advertencia y la existencia de falsos positivos.	**-43%**	**-33%**

No obstante, literatura posterior muestra que la efectividad del etiquetado depende de la precisión de la advertencia, el diseño de la señal y la existencia de falsos positivos o falsos negativos. Un estudio de USEC/NDSS de 2024 concluyó que el diseño de advertencias y su precisión influyen en las expectativas del usuario sobre la intención de la llamada, aunque no siempre generan cambios conductuales uniformes. El mismo estudio advierte que, si un adversario logra enmascarar el Caller ID y evitar la advertencia, la probabilidad de éxito puede aumentar porque los usuarios modifican sus expectativas frente al sistema de etiquetado.

[80] MIRAMIRKANI, Niloofar; STAROV, Oleksii; et al. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators [en línea]. En: Network and Distributed System Security Symposium (NDSS), 2020 [consultado: 14 de mayo de 2026]. Disponible en: https://www.ndss-symposium.org/wp-content/uploads/2020/02/24286.pdf

En consecuencia, esta alternativa debe valorarse como un mecanismo de mitigación conductual: reduce la probabilidad de interacción con llamadas sospechosas, pero no elimina el tráfico fraudulento ni impide completamente la exposición del usuario. Así mismo, requiere acompañarse de campañas de educación para que los usuarios comprendan el significado de las etiquetas y ajusten su comportamiento frente a llamadas marcadas como sospechosas o de probable fraude.

Con fundamento en la evidencia académica disponible, se propone utilizar los siguientes escenarios de efectividad:

Escenarios propuestos para el análisis de sensibilidad

Pesimista	28%
Moderado	43%
Optimista	58%

Estos valores toman como referencia el resultado experimental de reducción del 43% en llamadas falsas contestadas bajo ciertos diseños de advertencia, ajustado por la incertidumbre asociada a compatibilidad de terminales, comprensión del usuario, precisión del sistema de etiquetado y posibles efectos de fatiga por alertas.

Enfoque de costos de las alternativas regulatorias.

La estimación de costos para las alternativas regulatorias asociadas a la temática «Limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)» se desarrolló bajo el mismo enfoque metodológico descrito en la sección 9.2.1 para la evaluación de la «Subtemática 2: Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude», manteniendo un modelo de costeo regulatorio modular orientado a identificar los requerimientos técnicos, operativos, regulatorios y de supervisión asociados a la implementación de mecanismos de autenticación, bloqueo, monitoreo y etiquetado de llamadas en redes móviles.

En este contexto, el modelo incorpora componentes específicos relacionados con:

- adecuaciones sobre redes de voz y plataformas IMS/SBC;
- implementación de mecanismos anti-spoofing;
- motores de análisis y clasificación de llamadas;
- plataformas de intercambio de alertas;
- herramientas de autenticación y verificación del Caller ID;
- capacidades de etiquetado de llamadas;
- y recursos asociados a supervisión y cumplimiento regulatorio.

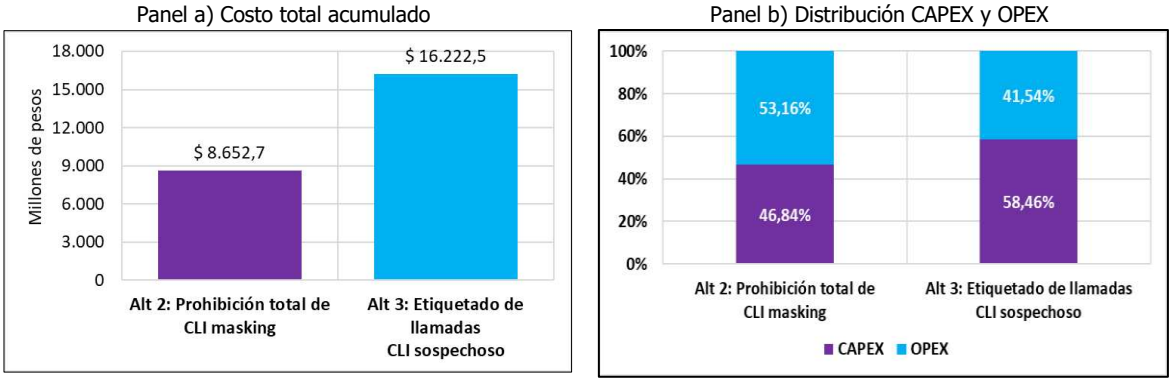
En este sentido, la construcción de los costos parte de la identificación de módulos tecnológicos y operativos requeridos para implementar cada alternativa regulatoria, diferenciando entre inversiones iniciales (CAPEX), costos operativos recurrentes (OPEX), costos de integración y costos regulatorios de supervisión. No obstante, dadas las particularidades técnicas del ecosistema de voz móvil y de las soluciones asociadas a autenticación y tratamiento del CLI, el modelo incorpora componentes especializados asociados a tráfico internacional, voice firewalls, motores de scoring y capacidades de autenticación de llamadas. A continuación, se presenta una comparación de los costos estimados de

implementación para cada alternativa bajo un horizonte de evaluación de tres (3) años para garantizar su comparabilidad con el horizonte temporal de las proyecciones de la afectación económica derivadas del smishing, mientras que en la sección de ANEXOS se describen los principales componentes considerados para la estimación de costos de las alternativas regulatorias evaluadas.

Es importante precisar que los resultados del modelo son sensibles al horizonte temporal de evaluación utilizado. En particular, las alternativas con mayores componentes operativos recurrentes (OPEX) presentan variaciones importantes en el costo total acumulado cuando se modifica el periodo de análisis. Así mismo, el modelo considera que las inversiones CAPEX asociadas a infraestructura tecnológica crítica presentan una vida útil promedio de seis (6) años, momento a partir del cual se requerirían procesos de reinversión o actualización tecnológica significativa. En consecuencia, bajo el horizonte de tres años utilizado en esta evaluación no se incorpora un nuevo ciclo de reinversión CAPEX, por lo que los resultados reflejan únicamente la primera etapa de implementación y operación inicial de las medidas.

Ahora, los resultados muestran diferencias relevantes en la complejidad tecnológica y en el nivel de transformación requerido por cada alternativa regulatoria. Mientras algunas alternativas se soportan principalmente en ajustes regulatorios y adecuaciones sobre infraestructura existente, otras requieren transformaciones profundas sobre redes IMS, mecanismos criptográficos de autenticación y plataformas avanzadas de análisis y señalización del tráfico.

Ilustración 23. Comparación del costo por alternativa regulatoria en pesos corrientes.



Fuente: Elaboración CRC.

Los resultados, presentados en el panel a) de la Ilustración 23 muestran el costo de las alternativas en precios corrientes. En este panel se puede observar que la Alternativa 2 presenta el menor costo total de implementación, debido a que se basa principalmente en ajustes regulatorios, reglas de filtrado y adecuaciones sobre plataformas existentes de monitoreo y control de tráfico internacional. En este caso, los costos se concentran en configuraciones de SBC/IMS, monitoreo de tráfico internacional y capacidades de bloqueo anti-spoofing.

Por su parte, la Alternativa 3 presenta un incremento importante en los costos frente a la alternativa anterior, explicado por la necesidad de incorporar motores de scoring, capacidades de etiquetado dinámico, plataformas de intercambio de alertas, modelos analíticos y herramientas de clasificación de llamadas sospechosas. Así mismo, esta alternativa requiere costos recurrentes asociados a

actualización de modelos analíticos, inteligencia de amenazas y operación de plataformas de monitoreo.

Por su parte, la distribución de costos presentada en el panel b) de la Ilustración 23 evidencia diferencias importantes en la naturaleza de las inversiones requeridas por cada alternativa. Tanto la alternativa 2 como la alternativa 3 incorporan componentes operativos asociados al monitoreo, actualización de reglas, análisis de tráfico y operación continua de mecanismos de control y clasificación. Sin embargo, al contrastar la composición de los costos, se observa que la alternativa 3 concentra una proporción significativamente mayor de costos CAPEX, 58,46% versus 46,84% de la alternativa 2, reflejando una mayor necesidad de infraestructura tecnológica, capacidades analíticas y desarrollos especializados para soportar los mecanismos de etiquetado y clasificación dinámica de llamadas.

Este aspecto resulta relevante debido a que el modelo contempla ciclos de reinversión de capital cada seis (6) años. En consecuencia, aunque una menor participación relativa del OPEX podría generar eficiencias operativas en el corto plazo, dichas eficiencias tienden a reducirse en horizontes temporales más amplios, en la medida en que se requieren nuevas inversiones para actualización o reemplazo de infraestructura tecnológica.

Resultados

En la Tabla 7 se presentan los resultados del análisis económico en términos del valor presente neto de las medidas. Estos resultados evidencian que tanto la alternativa 2 «Prohibición total del enmascaramiento de la identidad de línea llamante (CLI)» como la alternativa 3 «Permitir enmascaramiento con obligación de identificación y etiquetado de llamadas para el usuario» generan beneficios económicos netos positivos frente al escenario de statu quo, lo que indica que, bajo los supuestos considerados, ambas medidas presentan capacidad para reducir las pérdidas económicas asociadas al fraude mediante vishing en una magnitud superior a los costos requeridos para su implementación y operación.

Tabla 7. Resultados del ACB, VPN sobre tres años (cifra en millones)

	Alt 1: Statu Quo	Alt 2: Prohibición total de CLI masking	Alt 3: Etiquetado de llamadas CLI sospechoso
Costos			
PRST	-	7.976,22	15.547,8
CRC	-	215,97	-
Beneficio			
Pérdidas económicas potencialmente evitadas	-181.195,07	112.769,93	61.134,5
Beneficio Neto	-181.195,07	104.577,74	45.586,63
RCB	-	13,77	3,93

Fuente: Elaboración CRC

En el escenario base o moderado, la alternativa 2 alcanza un beneficio neto estimado de $104.577,74 millones de pesos en valor presente, mientras que la alternativa 3 obtiene un beneficio neto de $45.586,63 millones de pesos. Estos resultados reflejan que ambas alternativas permiten recuperar, en términos económicos, una proporción significativa de las pérdidas ocasionadas por el fraude asociado al enmascaramiento del CLI.

Particularmente, la alternativa 2 presenta el mejor desempeño económico relativo dentro del conjunto de alternativas evaluadas, alcanzando una relación beneficio-costo (RBC) de 13,77. Esto implica que, por cada peso invertido en la implementación de la medida, se obtendrían aproximadamente $13,77 pesos en beneficios económicos derivados de la reducción de pérdidas asociadas al fraude. Este resultado se explica principalmente por tres factores:

- En primer lugar, esta alternativa presenta los menores costos de implementación dentro de las medidas evaluadas, dado que se soporta principalmente en adecuaciones regulatorias, ajustes sobre SBC/IMS y mecanismos de bloqueo de tráfico internacional sospechoso, sin requerir transformaciones estructurales profundas sobre las redes móviles.

- En segundo lugar, la medida tiene una capacidad importante para reducir ataques de spoofing internacional, particularmente aquellos asociados a llamadas que utilizan numeración nacional colombiana como CLI en tráfico internacional entrante, lo cual constituye una de las modalidades más comunes utilizadas en esquemas de vishing y suplantación.

- En tercer lugar, aunque el modelo incorpora un declive progresivo de efectividad de la medida hasta deducir un 15% al final del horizonte de evaluación de tres años, la alternativa mantiene beneficios acumulados elevados debido a que el mayor impacto de mitigación ocurre durante las etapas iniciales de implementación, cuando el ecosistema fraudulento aún no ha desarrollado plenamente mecanismos de adaptación o evasión frente a las nuevas restricciones regulatorias.

Por su parte, la alternativa 3 también presenta resultados positivos desde el punto de vista económico, alcanzando una RBC de 3,93, lo que indica que los beneficios estimados superan ampliamente los costos de implementación. Sin embargo, su desempeño económico resulta inferior frente a la alternativa 2. Este resultado se encuentra asociado principalmente a que la alternativa 3 incorpora costos significativamente mayores.

Adicionalmente, aunque esta alternativa fortalece la información disponible para el usuario y evita el bloqueo potencial de tráfico legítimo, su efectividad depende en mayor medida del comportamiento del usuario final y de la capacidad de interpretación de las alertas mostradas en el dispositivo. En consecuencia, el impacto económico esperado sobre la reducción de pérdidas por fraude tiende a ser más gradual y parcialmente condicionado por factores de adopción y comportamiento humano.

Así mismo, el declive progresivo de efectividad incorporado en el modelo afecta relativamente más a esta alternativa, dado que los esquemas basados en etiquetado pueden perder capacidad preventiva en el tiempo a medida que los usuarios desarrollan fatiga frente a las alertas, o los actores fraudulentos ajustan sus patrones operativos para reducir la probabilidad de clasificación como tráfico sospechoso.

En contraste, el escenario de statu quo mantiene pérdidas económicas netas negativas por $60.398,36 millones de pesos en valor presente, reflejando la continuidad de las afectaciones económicas derivadas del fraude mediante vishing bajo ausencia de medidas regulatorias adicionales. Dado que este escenario no incorpora costos incrementales regulatorios, el valor negativo corresponde directamente a las pérdidas económicas proyectadas que continuarían siendo asumidas por los usuarios y el ecosistema económico en ausencia de intervención regulatoria.

Finalmente, es importante señalar que los resultados obtenidos son sensibles a los supuestos de efectividad y al horizonte temporal de evaluación utilizado. En particular, el modelo considera:

- un escenario moderado como referencia central del análisis;
- una reducción progresiva de la efectividad de las medidas hasta deducir 10 puntos porcentuales del nivel de efectividad planteado;
- y una tasa de descuento (WACC) del 11,57%, consistente con el valor adoptado en el proyecto regulatorio «Esquemas de remuneración mayorista de redes móviles»[81].

En consistencia, esta Comisión consideró pertinente realizar un análisis de sensibilidad, además de mantener el declive progresivo de este indicador, con el propósito de identificar las condiciones bajo las cuales alguna de las medidas podría verse afectadas en su viabilidad social frente a cambios en el alcance de las medidas para prevenir el fraude cibernético.

Análisis de sensibilidad.

El análisis de sensibilidad se desarrolló a partir del escenario moderado utilizado como caso base de evaluación, incorporando una variación de ±15 puntos porcentuales sobre el indicador de efectividad estimado con base en el benchmark internacional. Este ejercicio, cuyos resultados se presentan en la Tabla 8, permite observar la robustez de los resultados económicos frente a cambios razonables en la capacidad esperada de cada alternativa para reducir las pérdidas económicas asociadas al vishing.

Tabla 8. Análisis de sensibilidad frente a diferentes escenarios de niveles de efectividad

	Alt 2: Prohibición total de CLI masking	Alt 3: Etiquetado de llamadas CLI sospechoso
Escenarios		
Pesimista	60%	28%
Moderado	75%	43%
Optimista	90%	58%
RCB		
Pesimista	12,06	2,38
Moderado	13,77	3,93
Optimista	16,72	5,49

Fuente: Elaboración CRC.

[81] CRC. Documento soporte del proyecto regulatorio «Esquemas de remuneración mayorista de redes móviles». Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-9/Propuestas/documento-soporte-esquemas-remuneracion-mayorista-redes-moviles.pdf

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Bajo este enfoque, para la alternativa 2 «Prohibición total del enmascaramiento de la identidad de línea llamante (CLI)» se evaluaron tres escenarios de efectividad: 60% en el escenario pesimista, 75% en el escenario moderado y 90% en el escenario optimista. Por su parte, para la alternativa 3 «Permitir enmascaramiento con obligación de identificación y etiquetado de llamadas para el usuario» se evaluaron niveles de efectividad de 28%, 43% y 58%, respectivamente.

Los resultados evidencian que ambas alternativas mantienen una relación costo-beneficio superior a 1 en todos los escenarios analizados, lo que indica que, incluso bajo supuestos conservadores de efectividad, los beneficios económicos esperados superan los costos estimados de implementación y operación. En este sentido, los resultados son robustos frente a variaciones razonables del indicador de efectividad.

En el caso de la alternativa 2, la relación costo-beneficio pasa de 12,06 en el escenario pesimista a 13,77 en el escenario moderado y alcanza 16,72 en el escenario optimista. Este comportamiento evidencia que la medida presenta una alta capacidad de generación de beneficios netos aun cuando se reduce su efectividad esperada, lo cual se explica por su menor costo relativo de implementación y por su incidencia directa sobre el vector técnico que habilita el enmascaramiento del CLI en llamadas internacionales entrantes.

Por su parte, la alternativa 3 presenta una relación costo-beneficio de 2,38 en el escenario pesimista, 3,93 en el escenario moderado y 5,49 en el escenario optimista. Aunque estos resultados también son positivos, muestran una mayor sensibilidad frente al nivel de efectividad asumido, debido a que esta alternativa presenta mayores costos de implementación y su impacto depende en mayor medida de la capacidad del usuario para interpretar y reaccionar frente a las etiquetas desplegadas en el identificador de llamada.

La comparación entre alternativas muestra que la alternativa 2 conserva el mejor desempeño económico en todos los escenarios de sensibilidad. Incluso en el escenario pesimista, su relación costo-beneficio supera ampliamente la obtenida por la alternativa 3 en el escenario optimista. Esto sugiere que la prohibición total del CLI masking presenta una mayor robustez económica frente a la incertidumbre sobre la efectividad esperada de la medida.

En contraste, la alternativa 3, aunque económicamente viable bajo todos los escenarios, presenta una relación costo-beneficio menor, lo que refleja que su conveniencia económica depende en mayor medida de alcanzar niveles adecuados de precisión en el etiquetado, compatibilidad tecnológica con terminales y comprensión por parte de los usuarios. En consecuencia, su desempeño podría verse afectado si las alertas no son suficientemente visibles, si se generan falsos positivos o si los usuarios desarrollan fatiga frente a las advertencias.

En síntesis, el análisis de sensibilidad confirma que las dos alternativas evaluadas generan beneficios económicos superiores a sus costos bajo los escenarios considerados. No obstante, la alternativa 2 presenta mayor robustez, eficiencia económica y estabilidad frente a cambios en la efectividad esperada, mientras que la alternativa 3 mantiene resultados positivos, pero con una mayor dependencia de factores tecnológicos y conductuales para alcanzar los beneficios proyectados.

Conclusión

Desde el punto de vista operativo y tecnológico, la Alternativa 2 presenta el menor nivel de complejidad relativa, debido a que puede implementarse mediante adecuaciones sobre capacidades existentes de monitoreo y control de tráfico internacional, particularmente sobre plataformas IMS/SBC y mecanismos de análisis del tráfico entrante. Adicionalmente, esta alternativa presenta los menores costos de implementación dentro de las medidas evaluadas y los mejores resultados económicos en términos de beneficio neto y relación beneficio-costo bajo todos los escenarios analizados.

En efecto, incluso considerando un escenario conservador de efectividad y un declive progresivo de la medida hasta descontar 15 puntos porcentuales de forma progresiva hasta el final del horizonte de evaluación, la alternativa mantiene una relación beneficio-costo superior a 10, lo que evidencia una alta capacidad para reducir las pérdidas económicas asociadas al vishing frente a los costos requeridos para su implementación. Así mismo, la medida actúa directamente sobre uno de los principales mecanismos técnicos utilizados en esquemas de spoofing internacional, al impedir el uso de numeración nacional colombiana como identificador de llamadas originadas desde el exterior.

9.2.2.2.6 Propuesta regulatoria «Limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)»

La propuesta regulatoria para implementar la alternativa ganadora implicará modificar el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016, que actualmente regula la obligación general de los operadores de hacer uso de herramientas tecnólogas para prevenir la comisión de fraude, con la finalidad de incluir obligaciones particulares en materia de prevención del fraude en servicios tradicionales de voz.

Concretamente, mediante la adición de un numeral al referido artículo, se dispondrá que los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano, salvo cuando se trate de tráfico de roaming internacional debidamente identificado como tal por el carrier de origen. Los carriers internacionales interconectados con operadores colombianos para la terminación de tráfico en la red móvil nacional deberán cumplir con los formatos y longitudes de numeración establecidos en la Recomendación UIT-T E.164, respetando el código de país correspondiente al origen real de la llamada.

Seguidamente se incorpora la propuesta regulatoria:

Modificar el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, el cual quedará así:

«**ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES.** Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude:

2.1.10.7.1. Obligaciones generales:

2.1.10.7.1.1. Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y debe hacer controles periódicos respecto a la efectividad de estos mecanismos.

2.1.10.7.1.2. Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) que pueda tener relación con un presunto fraude, el operador debe investigar sus causas; y en caso de que determine la no existencia de un fraude, le debe demostrar al usuario las razones por las cuales no procede su PQR (petición, queja/ reclamo o recurso). Sin embargo, si se demuestra que el usuario actuó diligentemente en el uso del servicio contratado, no habrá lugar al cobro de los consumos objeto de reclamación.

2.1.10.7.2. Obligaciones particulares:

2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.

(…)

2.1.10.7.2.2. Obligaciones particulares en materia de prevención del fraude en los servicios tradicionales de voz. Los Proveedores de Redes y Servicios de Telecomunicaciones deberán implementar las siguientes medidas orientadas a prevenir el contacto fraudulento a usuarios a través de llamadas de voz:

2.1.10.7.2.2.1. Los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano, salvo cuando se trate de tráfico de roaming internacional debidamente identificado como tal por el carrier de origen. Los carriers internacionales interconectados con operadores colombianos para la terminación de tráfico en la red móvil nacional deberán cumplir con los formatos y longitudes de numeración establecidos en la Recomendación UIT-T E.164, respetando el código de país correspondiente al origen real de la llamada.

(…)».

9.2.2.3 Subtemática 2: Falta de una instancia de coordinación para la articulación y el intercambio de alertas

Situación identificada:	En Colombia no existe una instancia de coordinación para la articulación y el intercambio de alertas en tráfico de voz. Esta falta de coordinación genera vulnerabilidades y limita la capacidad de respuesta ante incidentes.
Causa relacionada:	Causa 1: Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto. Causa 2: Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes.
Alternativa 1: Statu quo	Cada PRST aplica controles internos y establece coordinaciones con otros operadores para el tráfico de voz, cuando lo considere necesario en forma bilateral o mediante esquemas ya existentes.
Alternativa 2: Creación de una plataforma nacional de intercambio de alertas	Esta alternativa propone la creación de una plataforma nacional centralizada, administrada por la CRC o por un tercero con base en lineamiento regulatorios que expida la CRC, que permita a los operadores reportar en tiempo real patrones sospechosos, incidentes de fraude y llamadas con posible enmascaramiento de la identidad de línea llamante (CLI). La

	plataforma funcionaría como un HUB o puerto de intercambio de alertas y señales de riesgo, la trazabilidad de eventos y la respuesta rápida ante campañas fraudulentas. Entidades del orden nacional (CRC, Colcert, Fiscalía, Policía Nacional, entre otras) recibirán directamente de la plataforma centralizada, reportes de tráfico sospechoso con los recursos de identificación involucrados (numeración E.164). Los operadores deberán reportar en esta plataforma única y exclusivamente la información que determinará la CRC de manera precisa y en ningún caso los operadores reportarán, ni tendrán acceso, a información comercialmente sensible de sus competidores. El administrador de la plataforma no compartirá ni otorgará acceso a bases de datos ni a información personal, salvo por orden judicial.
Alternativa 3: Creación de un mecanismo formal de articulación y coordinación	Esta alternativa busca establecer la creación de mecanismos formales (por ejemplo, un comité interinstitucional) entre los PRST y la CRC, así como la participación voluntaria de otras entidades del orden nacional (Colcert, Fiscalía, Policía Nacional, entre otras) que permita a los operadores reportarle a la CRC información relevante como alertas periódicas de tráfico sospechoso con los recursos de identificación involucrados (numeración E.164). Las reglas que la CRC defina sobre este comité interinstitucional precisarán de manera clara la información que los operadores deberán reportar y en ningún caso los operadores reportarán, ni tendrán acceso, en esta instancia, a información comercialmente sensible de sus competidores, ni se compartirá información relacionada con datos personales. La CRC, en las referidas reglas, determinará los escenarios en los que será necesario invitar a otras entidades del orden nacional para contribuir en los objetivos del mecanismo. Si bien esta alternativa se plantea para servicios de voz, en caso que una alternativa similar sea seleccionada para servicios de SMS, se unificaría el mecanismo formal para voz y SMS
Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional	Requiere que todas las llamadas estén firmadas digitalmente mediante STIR/SHAKEN, incorporando *Rich Call Data* (RCD) para autenticidad y visualización de información del originador, bloqueando o marcando llamadas no verificadas.

9.2.2.3.1 Alternativa 1: Statu quo

Cada PRST aplica controles internos y establece coordinaciones con otros operadores para el tráfico de voz, cuando lo considere necesario en forma bilateral o mediante esquemas ya existentes. No se da una plataforma nacional de intercambio de alertas ni se crean mecanismos formales de articulación y coordinación.

9.2.2.3.2 Alternativa 2: Creación de una plataforma nacional de intercambio de alertas

Esta alternativa propone la creación de una plataforma nacional centralizada, administrada por la CRC o por un tercero con base en lineamiento regulatorios que expida la CRC. El propósito de la plataforma es permitir a los operadores reportar y visualizar en tiempo real patrones sospechosos, incidentes de fraude y llamadas con posible enmascaramiento de la identidad de línea llamante (CLI).

La plataforma funcionaría como un HUB de intercambio de alertas y señales de riesgo, con funciones de procesamiento y correlación de alertas, facilitando la coordinación entre operadores, la trazabilidad de eventos y la respuesta rápida ante campañas fraudulentas. El objetivo es fortalecer la capacidad de detección temprana y de reacción coordinada frente a amenazas, mejorando la protección del usuario y la eficacia de las investigaciones.

Los PRST deberían integrar sus sistemas de monitoreo y detección de fraude con la plataforma, enviando reportes automáticos de llamadas sospechosas, patrones anómalos y eventos de enmascaramiento de abonados. También deberían obtener información relevante de la plataforma como insumo para las decisiones que la regulación que finalmente se defina les permita tomar con respecto al tráfico, por ejemplo, bloqueo o etiquetado de llamadas a usuarios de telefonía móvil. La interoperabilidad del sistema se haría a través de una API segura para el intercambio de datos, permitiendo la interconexión con sistemas antifraude internacionales (por ejemplo, GSMA Fraud Intelligence).

Los operadores deberán reportar en esta plataforma única y exclusivamente la información que determinará la CRC de manera precisa y en ningún caso los operadores reportarán, ni tendrán acceso, a información comercialmente sensible de sus competidores.

Entidades del orden nacional (CRC, Colcert, Fiscalía, Policía Nacional, entre otras) recibirán directamente de la plataforma centralizada, reportes periódicos de tráfico sospechoso con los recursos de identificación involucrados (numeración E.164). El administrador de la plataforma no compartirá ni otorgará acceso a bases de datos ni a información personal, salvo por orden judicial.

Como la plataforma recibiría, procesaría y correlacionaría las alertas, resultaría de utilidad toda vez que se pueden generar notificaciones en tiempo real para todos los PRST. Esto permitiría reaccionar de manera más rápida y coordinada ante los intentos de fraude para responder a las alertas recibidas, bloqueando o etiquetando llamadas según los protocolos definidos.

Adicionalmente permitiría que las Entidades del orden nacional recibieran información relevante para el desarrollo de sus funciones y competencias específicas. De esta forma, la coordinación en tiempo real permite que todos los interesados puedan obtener las alertas y generar respuestas rápidas y coordinadas ante los intentos de fraude, consolidando una fuente de información única para que las Entidades del orden nacional (CRC, Colcert, Fiscalía, Policía Nacional, entre otras) reciban datos relevantes para sus funciones que contribuyan a la protección de los usuarios de los servicios de voz móvil y a la investigación y judicialización de los delitos de fraude como spoofing y vishing, y por tanto ser un aporte significativo a la construcción de una estrategia nacional integral contra el fraude cibernético.

9.2.2.3.3 Alternativa 3: Creación de un mecanismo formal de articulación y coordinación

Consiste en la creación de un Comité que sirva como mecanismo formal de articulación y coordinación a nivel nacional. El Comité será liderado y convocado por la CRC, quien definirá sus reglas y administración, incluyendo mecanismos de convocatoria periódica y de activación excepcional. Tendrá la participación obligatoria de los PRSTM y de asignatarios de recursos de identificación y, de ser el

caso, se invitará a otras entidades del Estado a colaborar (COLCERT, Fiscalía, Policía Nacional, entre otras) de acuerdo con los temas específicos que se estén tratando, pero no de manera vinculante.

En el Comité no se compartirá información comercialmente sensible entre competidores, ni tampoco información relacionada con datos personales.

La CRC definirá el tipo de información que deberá ser presentada por los operadores en forma estandarizada, incluyendo alertas de tráfico sospechoso asociado a numeración E.164. Entre la información a intercambiar se incluirán campos como fecha y hora del inicio de la detección, PRST emisor (Nacional o Carrier Internacional), numeración involucrada (número completo de origen de acuerdo con el número nacional significativo o el estándar E.164), la duración de la ventana de observación, la cantidad de eventos en la ventana de observación, el tipo de anomalía, las métricas de medición utilizadas y las acciones tomadas (bloqueo o etiquetado).

También se podrá pedir por parte de la CRC a los PRST que realicen la presentación al Comité Intersectorial de estadísticas consolidadas por ejemplo por tipo de anomalía, tipo de métrica o PRST emisor. Este mecanismo resulta útil porque permite superar la fragmentación actual de la información debido a una articulación inefectiva en la estrategia nacional de prevención del fraude y contribuye a mejorar la insuficiencia de las medidas de gestión y control de los PRST que fue otra de las causas identificada en el árbol del problema.

Al generar una visión nacional unificada de patrones de fraude se facilita la detección y la respuesta coordinada sin imponer cargas desproporcionadas ni generar riesgos competitivos. Además, genera información agregada a nivel nacional que permite entender de manera más comprensiva los patrones de tráfico y de fraude, tanto para los PRST y la CRC como eventualmente para otras Entidades del Estado.

Aunque no se trata de un sistema en tiempo real, contribuye a mitigar el contacto fraudulento a los usuarios mediante servicios de voz móvil al lograr una compartición de información entre los diferentes PRSTM que permita respuestas coordinadas frente al fraude e identificación de patrones. Además de ser un aporte significativo a la construcción de una estrategia nacional integral contra el fraude cibernético, dentro de las competencias de la CRC y con bajo impacto económico para los operadores.

En el marco de este comité, la CRC hará uso de su competencia de requerir información amplia, exacta, veraz y oportuna a los agentes que están obligados a participar y, en los términos del numeral 19 del artículo 22 de la Ley 1341 de 2009, la CRC podrá imponer las multas a las que haya lugar en caso de incumplimiento de los requerimientos realizados.

De acuerdo con las alternativas regulatorias que finalmente sean seleccionadas, el Comité Interinstitucional podría funcionar para atender tanto las temáticas vinculadas a fraude en voz móvil como de SMS que lo requieran, así como para la actualización de manera dinámica de las medidas técnicas que se establezcan para cada una de las alternativas que resulten finalmente seleccionadas.

9.2.2.3.4 Evaluación de alternativas

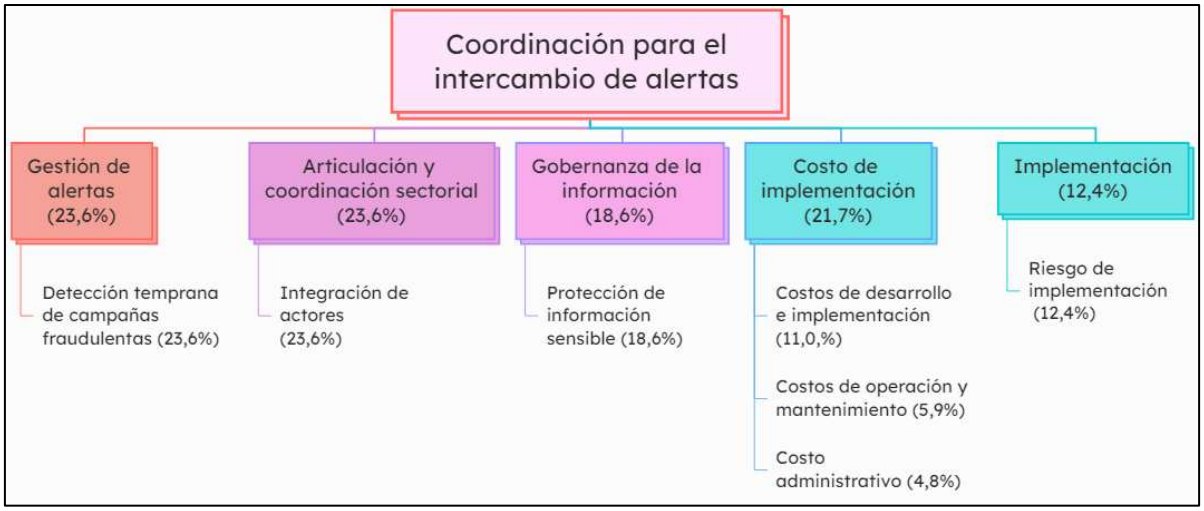
La evaluación de alternativas regulatorias para la temática «Falta de una instancia de coordinación para la articulación y el intercambio de alertas» se desarrolló mediante la metodología de Análisis de Decisión Multicriterio (ADMC), conforme a los lineamientos metodológicos definidos en la sección 9.1.1 del presente documento.

Este enfoque resulta pertinente dada la necesidad de evaluar simultáneamente múltiples dimensiones asociadas al diseño de mecanismos de coordinación e intercambio de información para la mitigación del fraude en servicios de voz móvil, incluyendo aspectos relacionados con la detección temprana de campañas fraudulentas, la integración de actores, la protección de información sensible, los riesgos de implementación y los costos asociados al despliegue y supervisión de las medidas propuestas.

En este contexto, la metodología permitió comparar de manera estructurada el desempeño relativo de las alternativas regulatorias frente a criterios técnicos, operativos y de gobernanza, considerando tanto los beneficios esperados en términos de articulación institucional y fortalecimiento de las capacidades de respuesta frente al fraude, como los costos, riesgos y requerimientos de coordinación asociados a su implementación. Particularmente, el análisis buscó identificar qué alternativa ofrece el mejor balance entre efectividad para la detección y gestión coordinada de eventos fraudulentos, viabilidad de implementación y sostenibilidad operativa.

Para el ejercicio de evaluación desarrollado se consideraron cinco criterios y siete subcriterios que cumplen con los principios fundamentales de exhaustividad, independencia y relevancia para el problema regulatorio analizado. Los criterios considerados se presentan en la Ilustración 24. La matriz de comparación, junto con el resultado de la prueba de consistencia y los ponderadores obtenidos para cada subcriterio, se presentan en la sección de Anexos.

Ilustración 24. Árbol jerárquico de la temática: Falta de una instancia de coordinación para la articulación y el intercambio de alertas



Fuente: Elaboración CRC

Criterios y Subcriterios

A continuación, se presentan las definiciones de los subcriterios establecidos para la evaluación de las diferentes alternativas regulatorias:

Gestión de alertas

- Detección temprana de campañas fraudulentas: Medida en que la alternativa facilita la identificación anticipada de patrones o campañas de fraude mediante el intercambio sistemático de información entre actores, facilitando la atención oportuna y preventiva de los eventos irregulares identificados.

Integración de actores

- Integración de actores: Nivel en que la alternativa facilita la articulación y participación coordinada de los distintos actores involucrados en la prevención y gestión del fraude, incluyendo PRST, CRC y otras entidades del orden nacional.

Gobernanza de la información

- Protección de información sensible: Grado en que la alternativa garantiza la confidencialidad de la información comercial y de los datos personales.

Implementación

- Riesgo de implementación: Nivel de complejidad técnica, operativa y de coordinación requerido para la puesta en marcha y funcionamiento efectivo de la alternativa.

Costos de implementación

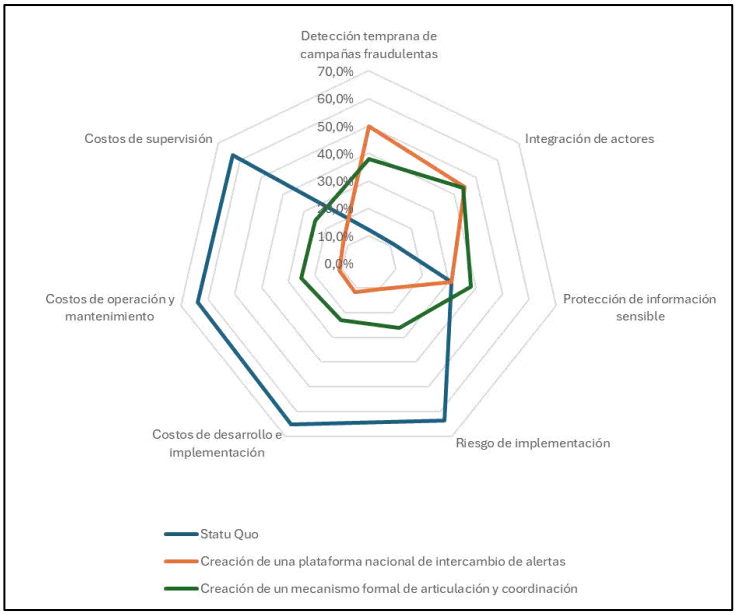
- Costos de desarrollo e implementación: Costos asociados al diseño, desarrollo y puesta en marcha de la solución.

- Costos de operación y mantenimiento: Recursos requeridos para la operación continua, soporte técnico y sostenibilidad del esquema implementado.

- Costos de supervisión: Recursos que la autoridad regulatoria debe destinar para monitorear y garantizar el funcionamiento adecuado del esquema.

Los resultados que se exponen en la Ilustración 25 correspondiente al desempeño relativo presentan el porcentaje de desempeño alcanzado por cada alternativa en cada subcriterio, ponderado según su importancia relativa dentro del modelo multicriterio. Por su parte, la Ilustración 26 de desempeño global presenta el puntaje agregado obtenido por cada alternativa evaluada. De esta manera, la evaluación permite identificar la alternativa que ofrece el mejor balance integral entre efectividad para atender el problema identificado, viabilidad de implementación y costos asociados.

Ilustración 25. Desempeño relativo de las alternativas de la temática: Falta de una instancia de coordinación para la articulación y el intercambio de alertas



Fuente: Elaboración CRC

A continuación, se presenta la descripción del desempeño de las alternativas regulatorias evaluadas para la temática «Falta de una instancia de coordinación para la articulación y el intercambio de alertas», frente a cada uno de los criterios considerados en el análisis multicriterio.

a. En cuanto al criterio de detección temprana de campañas fraudulentas, este evalúa la capacidad de las alternativas para facilitar la identificación anticipada de patrones sospechosos y eventos de fraude mediante mecanismos de intercambio sistemático de información. La alternativa de «Statu Quo» presenta el menor desempeño relativo (12,2%), dado que mantiene esquemas de coordinación unilaterales, es decir cada operador articula la gestión de alertas de forma independiente, y no incorpora mecanismos estructurados de compartición.

   La alternativa de «Creación de un mecanismo formal de articulación y coordinación» presenta un desempeño intermedio (37,9%), debido a que permite generar espacios formales de intercambio de información y coordinación sectorial, facilitando la identificación de patrones de fraude mediante reportes periódicos y análisis agregados.

   Por su parte, la alternativa de «Creación de una plataforma nacional de intercambio de alertas» presenta el mejor desempeño relativo (49,9%), en la medida en que incorpora capacidades centralizadas de recepción, procesamiento y correlación de alertas en tiempo real, facilitando respuestas más rápidas y coordinadas frente a campañas fraudulentas.

b. Respecto del criterio de integración de actores, este evalúa el nivel en que las alternativas facilitan la articulación y participación coordinada de los distintos actores relevantes para la gestión del

fraude. La alternativa de «Statu Quo» presenta el menor desempeño (11,3%), debido a que mantiene esquemas fragmentados y voluntarios de coordinación entre operadores.

La alternativa de «Creación de un mecanismo formal de articulación y coordinación» obtiene un desempeño relativo de 44,0%, siendo el segundo mejor resultado en este criterio, dado que establece una instancia formal liderada por la CRC que permite integrar de manera estructurada a los PRST y eventualmente a otras entidades del Estado como COLCERT, Fiscalía y Policía Nacional.

La alternativa de «Creación de una plataforma nacional de intercambio de alertas» presenta un desempeño ligeramente superior (44,7%), considerando que, aunque permite un intercambio automatizado de información entre múltiples actores, la articulación institucional depende en mayor medida de procesos operativos asociados al funcionamiento de la plataforma.

c. En relación con el criterio de protección de información sensible, este evalúa el grado en que las alternativas garantizan la confidencialidad de la información comercial y de los datos personales. La alternativa de «Statu Quo» presenta un desempeño intermedio (31,0%), dado que mantiene esquemas limitados de intercambio de información y, por tanto, menores riesgos asociados al tratamiento centralizado de datos.

   La alternativa de «Creación de un mecanismo formal de articulación y coordinación» presenta el mejor desempeño relativo (38,2%), debido a que define reglas explícitas sobre la información a reportar, evitando el intercambio de información comercialmente sensible y de datos personales, bajo un esquema de gobernanza coordinado por la CRC.

   Por su parte, la alternativa de «Creación de una plataforma nacional de intercambio de alertas» obtiene un desempeño de 30,8%, considerando que, aunque contempla restricciones regulatorias sobre el acceso y uso de la información, la centralización y procesamiento automatizado de alertas genera mayores retos de seguridad y gobernanza de la información.

d. Respecto del criterio de riesgo de implementación, este evalúa el nivel de complejidad técnica, operativa y de coordinación requerido para implementar cada alternativa. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (63,5%), dado que no requiere nuevas capacidades técnicas ni procesos de coordinación adicionales.

   La alternativa de «Creación de un mecanismo formal de articulación y coordinación» obtiene un desempeño intermedio (26,0%), debido a que requiere la estructuración de procesos formales de reporte, estandarización de información y coordinación sectorial, aunque sin demandar el despliegue de infraestructura tecnológica centralizada compleja.

   La alternativa de «Creación de una plataforma nacional de intercambio de alertas» presenta el menor desempeño relativo (10,5%), considerando la necesidad de desarrollar una infraestructura tecnológica interoperable, establecer APIs seguras, implementar mecanismos de correlación de alertas y coordinar integraciones técnicas entre múltiples actores nacionales e internacionales.

e. En cuanto al criterio de costos de desarrollo e implementación, este evalúa los costos asociados al diseño, desarrollo y puesta en marcha de cada alternativa. La alternativa de «Statu Quo»

presenta el mejor desempeño relativo (65,3%), dado que no requiere inversiones adicionales en infraestructura, sistemas o procesos regulatorios.

La alternativa de «Creación de un mecanismo formal de articulación y coordinación» presenta un desempeño intermedio (23,0%), debido a que sus requerimientos de implementación se concentran principalmente en actividades de coordinación institucional y estandarización de reportes.

Por su parte, la alternativa de «Creación de una plataforma nacional de intercambio de alertas» presenta el menor desempeño relativo (11,7%), considerando los costos asociados al desarrollo, administración y operación de una plataforma tecnológica centralizada con capacidades de interoperabilidad y procesamiento de alertas.

f. En relación con el criterio de costos de operación y mantenimiento, se observa un comportamiento similar. La alternativa de «Statu Quo» presenta el mayor desempeño relativo (63,9%), dado que conserva los esquemas actuales sin generar nuevos costos recurrentes de operación.

   La alternativa de «Creación de un mecanismo formal de articulación y coordinación» obtiene un desempeño de 25,0%, asociado principalmente a costos administrativos y de gestión periódica del comité interinstitucional.

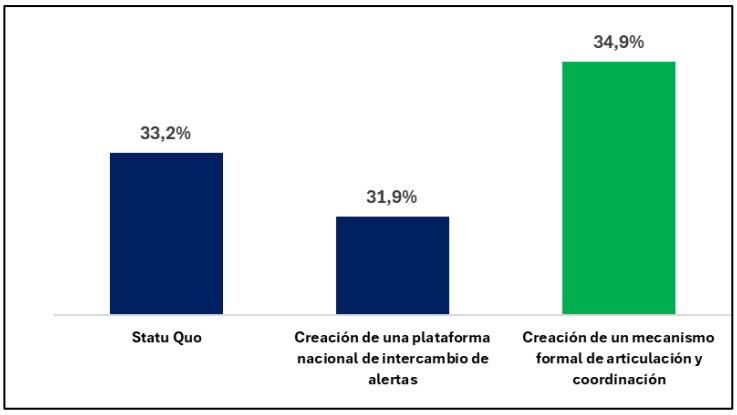
   La alternativa de «Creación de una plataforma nacional de intercambio de alertas» presenta el menor desempeño relativo (11,1%), debido a los costos continuos asociados al soporte técnico, mantenimiento de infraestructura, actualización de sistemas y monitoreo permanente de la plataforma.

g. Finalmente, respecto del criterio de costos de supervisión, este evalúa los recursos requeridos por la autoridad regulatoria para monitorear y garantizar el funcionamiento adecuado de cada alternativa. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (63,2%), dado que no introduce nuevas cargas regulatorias ni esquemas adicionales de supervisión.

   La alternativa de «Creación de un mecanismo formal de articulación y coordinación» presenta un desempeño de 24,8%, mientras que la alternativa de «Creación de una plataforma nacional de intercambio de alertas» obtiene el menor desempeño relativo (12,0%), debido a la necesidad de supervisar el funcionamiento técnico, la seguridad de la información y el cumplimiento de las obligaciones asociadas a la plataforma centralizada.

En síntesis, el análisis multicriterio evidencia que la alternativa «Creación de un mecanismo formal de articulación y coordinación» presenta el mejor desempeño global entre las alternativas evaluadas, alcanzando un puntaje agregado de 34,9%, frente a 33,2% de la alternativa de «Statu Quo» y 31,9% de la alternativa de «Creación de una plataforma nacional de intercambio de alertas». Esta alternativa sobresale especialmente en los criterios asociados a integración de actores y protección de información sensible, al tiempo que mantiene niveles de costos y riesgos de implementación significativamente inferiores frente a una solución tecnológica centralizada.

Ilustración 26. Puntaje agregado de cada alternativa de la temática: Falta de una instancia de coordinación para la articulación y el intercambio de alertas



Fuente: Elaboración CRC

Si bien la alternativa de «Creación de una plataforma nacional de intercambio de alertas» presenta ventajas importantes en términos de detección temprana y capacidades de respuesta en tiempo real, sus elevados requerimientos técnicos, costos de implementación y riesgos operativos reducen su desempeño global. Por su parte, la alternativa de «Statu Quo» presenta ventajas en términos de simplicidad y menores costos, aunque mantiene las limitaciones actualmente identificadas en materia de coordinación sectorial y articulación de esfuerzos para la prevención del fraude.

Conclusión

En consideración de los resultados, el análisis multicriterio evidencia que la alternativa de «Creación de un mecanismo formal de articulación y coordinación» presenta el mejor desempeño global, al alcanzar un puntaje agregado de 34,9%, frente a 33,2% de la alternativa de «Statu Quo» y 31,9% de la alternativa de «Creación de una plataforma nacional de intercambio de alertas».

Este resultado obedece a que la alternativa ganadora logra un balance más favorable entre los criterios asociados a la efectividad de la medida y aquellos relacionados con su viabilidad operativa e institucional. En particular, presenta desempeños destacados en los criterios de integración de actores y protección de información sensible, aspectos que resultan fundamentales para fortalecer la coordinación sectorial y garantizar el intercambio seguro de información entre los distintos actores involucrados en la prevención y gestión del fraude.

Por su parte, la alternativa de «Creación de una plataforma nacional de intercambio de alertas» obtiene el mejor desempeño en el criterio de detección temprana de campañas fraudulentas, reflejando las ventajas inherentes a una solución tecnológica centralizada para la recepción, procesamiento y correlación de alertas. Sin embargo, dichas ventajas se ven compensadas por mayores requerimientos de inversión, costos de operación, complejidades de gobernanza de la información y riesgos de implementación, factores que reducen su desempeño global dentro de la evaluación.

A su vez, la alternativa de «Statu Quo» presenta los mejores resultados en los criterios asociados a costos de implementación, costos de operación, costos de supervisión y riesgo de implementación, debido a que no incorpora nuevas obligaciones regulatorias ni requiere el despliegue de capacidades

adicionales. No obstante, esta situación responde principalmente a la ausencia de intervención regulatoria y, por tanto, no permite atender de manera efectiva las limitaciones actualmente identificadas en materia de coordinación sectorial e intercambio estructurado de alertas.

En este contexto, la evaluación evidencia que la creación de un mecanismo formal de articulación y coordinación constituye una solución proporcional y escalable para abordar la problemática identificada, en la medida en que fortalece la articulación entre operadores y autoridades competentes, promueve el intercambio sistemático de información relevante para la detección de eventos fraudulentos y establece reglas de gobernanza que permiten proteger adecuadamente la información sensible. Todo ello se logra sin incurrir en los elevados costos, complejidades técnicas y riesgos operativos asociados a la implementación de una plataforma tecnológica centralizada.

En consecuencia, se concluye que la alternativa de «Creación de un mecanismo formal de articulación y coordinación» ofrece la mejor relación entre efectividad regulatoria, viabilidad de implementación y sostenibilidad institucional, razón por la cual se identifica como la alternativa más adecuada para atender la problemática relacionada con la falta de una instancia de coordinación para la articulación y el intercambio de alertas.

9.2.2.3.5 Propuesta regulatoria «Falta de una instancia de coordinación para la articulación y el intercambio de alertas»

En el marco de las modificaciones que se han venido explicado, y que se concretarán en el ajuste del artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, se creará el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles, como instancia permanente de coordinación para el intercambio de alertas, la identificación de patrones de fraude y la construcción de una respuesta nacional coordinada frente al fraude cibernético a través de los servicios de voz móvil y mensajes cortos de texto (SMS). El CTLFSM será liderado y convocado por la CRC, con base en las reglas de funcionamiento y administración que se definen en la siguiente propuesta regulatoria:

Seguidamente se incorpora la propuesta regulatoria:

Modificar el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, el cual quedará así:

«**ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES.** Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude:

2.1.10.7.1. Obligaciones generales:

2.1.10.7.1.1. Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y debe hacer controles periódicos respecto a la efectividad de estos mecanismos.

2.1.10.7.1.2. Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) que pueda tener relación con un presunto fraude, el operador debe investigar sus causas; y en caso de que determine la no existencia de un fraude, le debe demostrar al usuario las razones por las cuales no procede su PQR (petición, queja/ reclamo o recurso). Sin embargo, si se demuestra

que el usuario actuó diligentemente en el uso del servicio contratado, no habrá lugar al cobro de los consumos objeto de reclamación.

2.1.10.7.2. Obligaciones particulares:

2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.

(…)

2.1.10.7.2.2. Obligaciones particulares en materia de prevención del fraude en los servicios tradicionales de voz. Los Proveedores de Redes y Servicios de Telecomunicaciones deberán implementar las siguientes medidas orientadas a prevenir el contacto fraudulento a usuarios a través de llamadas de voz:

(…)

2.1.10.7.3. Creación del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles. Créase el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles, en adelante CTLFSM, como instancia de intercambio de alertas, identificación de patrones de fraude y espacio de revisión técnica de medidas frente al fraude cibernético a través de los servicios de voz móvil y mensajes cortos de texto (SMS). El CTLFSM será liderado y convocado por la CRC, con base en las reglas de funcionamiento y administración que se definen más adelante.

2.1.10.7.3.1. Conformación. El CTLFSM estará conformado por los siguientes participantes obligatorios:

- Por representantes de los PRST para las temáticas relacionadas con el fraude en los servicios tradicionales de voz y SMS, ya sea en el ecosistema P2P o A2P.

- Por los asignatarios de recursos de identificación denominado código corto A2P para las temáticas relacionadas con el fraude en el ecosistema A2P.

- La CRC, quién presidirá el Comité y ejercerá su secretaría técnica.

Podrán ser invitadas a participar en sesiones específicas, cuando los temas a tratar así lo requieran, entidades del orden nacional o territorial con competencias relacionadas con la prevención del fraude cibernético en servicios móviles, incluyendo el COLCERT, la Fiscalía General de la Nación, la Policía Nacional, la Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia, o cualquier otra entidad estatal o privada según las necesidades de los temas a discutir. La participación de estas entidades como invitadas no tendrá carácter vinculante para ellas.

2.1.10.7.3.2. Periodicidad y convocatoria. El CTLFSM sesionará ordinariamente con una intensidad no inferior a cuatro sesiones al año. Las sesiones podrán ser presenciales o virtuales, según como lo determine la CRC en la respectiva convocatoria. La CRC podrá convocarlo de manera extraordinaria cuando se presenten incidentes de fraude en servicios móviles que

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

requieran atención urgente o cuando las circunstancias del ecosistema así lo demanden. Los participantes obligatorios podrán igualmente solicitar a la CRC la convocatoria a sesión extraordinaria cuando lo consideren necesario, pero será potestativo de la CRC acceder a la referida convocatoria.

2.1.10.7.3.3. Información a intercambiar. En el marco del CTLFSM, los PRST y los asignatarios de código corto A2P, según corresponda, presentarán la información estandarizada que la CRC defina mediante requerimiento de información (en la convocatoria a la sesión), en los formatos y con la periodicidad que esta establezca.

La CRC podrá requerir adicionalmente la presentación de estadísticas consolidadas, por ejemplo, discriminadas por tipo de anomalía, tipo de métrica o PRST emisor, con el propósito de construir una visión nacional agregada de los patrones de fraude.

En ningún caso se compartirá, en el marco del CTLFSM, información comercialmente sensible entre competidores, ni información que contenga datos personales de usuarios.

2.1.10.7.3.4. Vinculatoriedad. En el marco del CTLFSM los participantes podrán proponer y acordar mejoras en la implementación de las medidas mínimas establecidas en el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, cuando la evolución de las modalidades de fraude así lo requieran. En caso de que no haya propuestas o acuerdos de mejoras, aplicarán los estándares mínimos establecidos en el mencionado artículo. Las decisiones del CTLFSM sobre tales parámetros serán de cumplimiento obligatorio para los PRST en los términos y plazos establecidos en la respectiva acta de sesión y, de identificarse necesario, en la resolución por medio de la cual se incorporen actualizaciones a la regulación general, la cual será expedida por el Director Ejecutivo de la Comisión de Regulación de Comunicaciones, previa aprobación del Comité de Comisionados de Comunicaciones de la CRC. La vinculatoriedad de estas decisiones deriva de la obligación regulatoria de participar en el CTLFSM. Las decisiones del CTLFSM no podrán, en ningún caso, desmejorar, degradar, modificar o derogar los parámetros técnicos mínimos establecidos en el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016.

2.1.10.7.3.5. Requerimiento de información y sanciones. En el marco del CTLFSM, la CRC hará uso de su facultad de requerir a los agentes obligados información amplia, exacta, veraz y oportuna sobre los temas objeto del Comité. En caso de incumplimiento de los requerimientos realizados, la CRC podrá imponer las multas a que haya lugar conforme al numeral 19 del artículo 22 de la Ley 1341 de 2009.

2.1.10.7.3.6. Adaptación regulatoria. Los resultados y actas del CTLFSM servirán a la CRC como insumo técnico para la actualización de cualquier medida contenida en la Resolución CRC 5050 de 2016 que tenga como finalidad la lucha o prevención contra el fraude en materia de servicios tradicionales de voz o SMS. Los resultados y actas del CTLFSM no son vinculantes para la CRC, pero sí para sus miembros en los términos definidos en el artículo 2.1.10.7.3.4. de esta resolución.

2.1.10.7.3.7. Presidencia. La Presidencia del CTLFSM será ejercida por el Comisionado de la Sesión de Comunicaciones de la CRC que tiene la calidad de ingeniero, en los términos del numeral 20.2 del artículo 20 de la Ley 1341 de 2009, o por quien este designe.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.1.10.7.3.8. Secretaría. La Secretaría del CTLFSM será ejercida por el funcionario de la Comisión de Regulación de Comunicaciones que haga las veces de Coordinador del Grupo Interno de Trabajo de Relaciones con Grupos de Valor o por el servidor en quien se delegue esta función por parte del Comité de Comunicaciones de la CRC, y tendrá a su cargo la convocatoria a las sesiones, la remisión de la documentación pertinente, el levantamiento de actas, el registro y control de la documentación generada y la información de contacto de los miembros.

2.1.10.7.3.9. Representación. Cada miembro obligado participará en el CTLFSM a través de un representante con facultades suficientes para asumir en su nombre las obligaciones derivadas de las determinaciones técnicas adoptadas en el Comité. Cada miembro designará un representante principal y un suplente, e informará a la Secretaría cualquier cambio en dicha designación dentro de los cinco (5) días hábiles siguientes a que se produzca.

2.1.10.7.3.10. Convocatoria. La Secretaría convocará las sesiones ordinarias y extraordinarias mediante comunicación escrita o correo electrónico dirigida a los representantes de los miembros obligados y, cuando sea el caso, a los invitados, con antelación mínima de cinco (5) días hábiles para las sesiones ordinarias y de dos (2) días hábiles para las sesiones extraordinarias. La convocatoria incluirá el orden del día, el requerimiento de la información que cada participante deberá presentar ante la CRC y la documentación que será analizada en la sesión.

2.1.10.7.3.11. Quórum y votación. Las sesiones del CTLFSM se realizarán válidamente con la asistencia de la mayoría simple de los miembros obligados. La Secretaría del CTLFSM identificará e informará la cantidad y calidad de los miembros obligados a participar en el CTLFSM. Cada miembro obligado tendrá derecho a un voto, con independencia de su tamaño o participación de mercado. Las determinaciones técnicas y operativas se adoptarán por mayoría simple de los miembros presentes. En caso de empate, la CRC tendrá voto dirimente. Los votos de abstención se contabilizarán únicamente para registro.

2.1.10.7.3.12. Actas. De cada sesión se levantará un acta en la que constarán como mínimo la fecha, hora y lugar, los asistentes, el orden del día, los temas tratados, las determinaciones adoptadas con indicación del resultado de la votación cuando corresponda, y los compromisos asumidos por cada miembro con sus respectivos plazos. Las actas serán publicadas en la página web de la CRC dentro de los diez (10) días hábiles siguientes a la sesión, salvo la información que tenga carácter confidencial o reservado, la cual se mantendrá en archivo independiente. Las actas serán firmadas por el Presidente y el Secretario del CTLFSM. Las decisiones del CTLFSM no serán vinculantes para la CRC ni afectarán sus competencias en materia de regulación. Por el contrario, estas decisiones serán un insumo técnico, no vinculante, que la CRC tendrá en cuenta para efectos de modificar su regulación en caso de que haya lugar y previo al respectivo Análisis de Impacto Normativo (AIN).

2.1.10.7.3.13. Mesas de trabajo. La Presidencia podrá proponer al CTLFSM la conformación de mesas de trabajo técnico o jurídico para el análisis de temas específicos. Las mesas de trabajo tendrán carácter temporal, estarán integradas por los representantes técnicos que cada miembro designe para el efecto, y presentarán sus conclusiones al pleno del CTLFSM en la sesión que la Presidencia determine. Las conclusiones de las mesas de trabajo tendrán carácter de propuesta y no serán vinculantes.

2.1.10.7.3.14. Confidencialidad. La información presentada por los miembros en el marco del CTLFSM tendrá carácter reservado frente a terceros no participantes, salvo que la CRC determine su publicación por razones de transparencia regulatoria. Los participantes no podrán utilizar la información conocida en el marco del CTLFSM para fines distintos a los del Comité ni divulgarla a terceros sin autorización expresa de la CRC.

2.1.10.7.3.15. Ingreso de nuevos miembros. Cuando un nuevo agente adquiera la calidad de PRST o de asignatario de código corto A2P con posterioridad a la constitución del CTLFSM, al mismo tiempo adquirirá la obligación de ser parte del CTLFSM. Por lo tanto, dicho agente deberá designar su representante y suplente dentro de los treinta (30) días hábiles siguientes al día en el que adquirió esa calidad.

2.1.10.7.3.16. Vigencia del CTLFSM. El CTLFSM estará constituido de manera permanente. La CRC podrá, mediante acto administrativo, ampliar, restringir o modificar sus funciones, composición o reglas de funcionamiento cuando las circunstancias regulatorias así lo requieran.

PARÁGRAFO. Cualquier incumplimiento a las disposiciones establecidas en el artículo 2.1.10.7. dará lugar a que la CRC realice el respectivo traslado a la SIC o al MinTIC para el ejercicio de sus funciones de vigilancia y control de conformidad con sus respectivas competencias».

Adicionar el numeral 11.1.1.2.6. al artículo 11.1.1.2. del Capítulo 1 del Título XI de la Resolución CRC 5050 de 2016, el cual quedará así:

«ARTÍCULO 11.1.1.2. CASOS DE PROYECTOS DE REGULACIÓN QUE NO SON SUJETOS DE PUBLICACIÓN. No se dará aplicación a lo previsto en el artículo 2.2.13.3.2 del Decreto 1078 de 2015 en los siguientes casos:

(…)

11.1.1.2.6. En la expedición de las resoluciones de las que trata el artículo 2.1.10.7.3.4. relacionadas con las decisiones que adopte el CTLFSM en los términos allí contenidos».

9.2.2.4 Subemática 3: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas

Situación identificada:	En Colombia no existen mecanismos a través de los cuales los usuarios de los servicios de telecomunicaciones obtengan la información sobre el origen de las llamadas y/o su intensión, lo anterior en la medida que tampoco existen lineamientos específicos y uniformes que le permitan a los operadores aplicar métodos preventivos de etiquetado de tráfico de voz, lo que dificulta la detección temprana de patrones anómalos asociados a fraude (*vishing*, llamadas masivas ilegítimas, *spoofing*). Esta situación genera vulnerabilidades, impide presentar información preventiva para los usuarios limitando la capacidad de toma de decisiones informadas (contesta o rechaza) ante el origen de las llamadas en su dispositivo.

Causa relacionada:	Causa 1: Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes.
Alternativa 1: Statu quo	Cada operador aplica controles internos sin lineamientos regulatorios comunes. No se realiza el etiquetado de las llamadas para proporcionar alertas a los usuarios finales en el tráfico de voz.
Alternativa 2: Lineamientos regulatorios integrales para el monitoreo y etiquetado del tráfico de voz, con enfoque general y segmentación empresarial	Esta alternativa propone un marco regulatorio único que combina la supervisión proactiva de todo el tráfico de voz con un esquema de verificación reforzada para llamadas de origen empresarial. El objetivo es detectar y prevenir la suplantación y otras actividades fraudulentas en llamadas, mejorando la información que se le proporciona a los usuarios al momento de recibir la llamada, y con ello mejorando la confianza de los usuarios en la identificación de quien les llama.
Alternativa 3: Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias	Esta alternativa plantea la creación de rangos específicos de numeración E.164, reservados exclusivamente para la originación de llamadas comerciales y publicitarias. El objetivo es establecer una diferenciación clara y visible entre las llamadas de carácter personal y aquellas con fines comerciales, facilitando la identificación por parte del usuario mediante el indicativo nacional de destino NDC, y habilitando controles regulatorios y operativos más precisos sobre el tráfico comercial.
Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional	Requiere que todas las llamadas estén firmadas digitalmente mediante STIR/SHAKEN, incorporando *Rich Call Data* (RCD) para autenticidad y visualización de información del originador, bloqueando o marcando llamadas no verificadas.

9.2.2.4.1 Alternativa 1: Statu quo

Cada operador aplica controles internos sin lineamientos regulatorios comunes. No se realiza el etiquetado de las llamadas para proporcionar alertas a los usuarios finales en el tráfico de voz.

9.2.2.4.2 Alternativa 2: Lineamientos regulatorios integrales para el monitoreo y etiquetado del tráfico de voz, con enfoque general y segmentación empresarial

Esta alternativa propone un marco regulatorio que combina la supervisión proactiva de todo el tráfico de voz con un esquema de verificación para llamadas de origen empresarial con contenido publicitario. El objetivo es detectar y prevenir la suplantación y otras actividades fraudulentas en llamadas, mejorando la confianza de los usuarios en la identificación de quien les llama.

La solución se aborda en los siguientes dos subcomponentes complementarios:

A) Monitoreo y etiquetado del tráfico de voz: Se establecen lineamientos obligatorios para que todos los PRSTM implementen mecanismos de monitoreo en tiempo real del tráfico que cursa en sus redes de voz. Estas herramientas deberán analizar en vivo el tráfico de llamadas en busca de patrones sospechosos o comportamientos anómalos que puedan indicar suplantación de identidad o fraude (por ejemplo, detección de volumen inusual de llamadas por relación origen/destino, identificación de patrones repetitivos (llamadas cortas, secuenciales, típicas de robocall), correlación automática con listas negras y reportes de fraude, etc.).

Cuando los sistemas de monitoreo identifiquen llamadas potencialmente fraudulentas, los operadores deberán etiquetarlas informativamente en el dispositivo del usuario receptor con un aviso claro, como «Llamada sospechosa», antes de que el usuario responda. Este etiquetado de alerta no bloquea la comunicación, pero advierte de un posible riesgo de suplantación o estafa, permitiendo al usuario tomar precauciones adicionales.

Los lineamientos técnicos serán flexibles y neutrales en términos tecnológicos, de modo que cada operador pueda emplear soluciones adaptadas a su plataforma (por ejemplo, análisis de señalización de llamadas, algoritmos de detección de anormalidades o bases de datos colaborativas de números reportados), sin imponer un estándar único de autenticación. En síntesis, todas las llamadas de voz cursadas por las redes públicas de telecomunicaciones estarán sujetas a un monitoreo preventivo que, ante indicios objetivos de fraude, generará alertas visibles en el terminal del usuario receptor, reforzando así su capacidad para identificar y evitar llamadas engañosas.

B) Verificación del tráfico de voz de origen empresarial (lista blanca): Como complemento al monitoreo general, la alternativa instaura un esquema específico dirigido al segmento corporativo y de servicios masivos, que son particularmente susceptibles a la suplantación de numeración. Se creará un mecanismo de registro previo de empresas y sus rangos de numeración autorizada por los PRSTM en una plataforma centralizada de confianza (lista blanca) de cada uno de los PRSTM.

Bajo este modelo, las organizaciones (p. ej., entidades financieras, servicios públicos, call centers legítimos) deberán inscribir los números de teléfono o identidades de llamada que utilizan para comunicarse con los usuarios. Los operadores, al cursar las llamadas de voz, validarán en tiempo real si el número originador figura en esa lista blanca. En caso afirmativo, la llamada podrá ser etiquetada en el dispositivo del usuario con un indicador de confiabilidad (por ejemplo, un texto o símbolo que la identifique como «llamada con fines publicitarios»), lo cual incrementa la confianza del destinatario en la legitimidad de esa comunicación.

Este subcomponente pretende crear un entorno de comunicaciones fiable para las llamadas empresariales, dificultando la suplantación de grandes marcas o instituciones. Sólo las empresas debidamente registradas podrán gozar del estatus de llamadas verificadas, mientras que las llamadas comerciales no registradas no dispondrán de dicho aval y serán objeto de mayor vigilancia.

Es importante destacar que este esquema de lista blanca se diseña de forma voluntaria pero incentivada: no impone obligaciones sobre la generalidad del tráfico de voz (evitando así cargas innecesarias al público en general), sino que se centra en aquellos actores empresariales que deseen asegurar la identidad de sus comunicaciones hacia los usuarios.

La implementación de este subcomponente se realizará de manera neutral tecnológicamente, permitiendo la utilización de distintas soluciones (p. ej., bases de datos centralizadas, protocolos de autenticación, u otras herramientas de mercado) que logren el objetivo de validar la procedencia de las llamadas corporativas sin exigir un estándar técnico específico. De este modo, los operadores podrán adoptar las soluciones más acordes con sus capacidades, siempre que cumplan con los mínimos de verificación enunciados.

El monitoreo general en tiempo real (subcomponente A) servirá para reducir el impacto de llamadas fraudulentas en todos los usuarios, ya que posibilita alertarles en el acto sobre posibles engaños telefónicos (por ejemplo, llamadas internacionales con identidades nacionales falsas o fraudes tipo

vishing), disuadiendo así a los delincuentes y empoderando a los ciudadanos para que actúen con cautela. Este monitoreo global mejora la capacidad preventiva del sistema de comunicaciones sin interrumpir la continuidad del servicio.

Por su parte, el subcomponente B generará un «ecosistema de confianza» específico para comunicaciones empresariales, elevando la seguridad en un segmento de alto valor y riesgo. Las llamadas comerciales genuinas de instituciones registradas ganarán en credibilidad ante los usuarios (lo que beneficia tanto a usuarios como a empresas legítimas, al aumentar las tasas de contacto efectivo), mientras que se aíslan y señalan las llamadas de posibles suplantadores o telemercaderes no identificados. La conjunción de ambos enfoques brinda un equilibrio entre protección amplia (todo el tráfico supervisado) y medidas diferenciadas donde más se requieren (verificación intensiva de llamadas corporativas), sin imponer sobrecargas injustificadas a las comunicaciones personales ordinarias.

Los lineamientos resultantes de esta alternativa se plasmarían de forma neutral tecnológicamente, de modo que los operadores y otros agentes puedan implementar las soluciones adaptadas a su entorno de red (pueden plantearse estándares comunes de referencia, sin exclusividad de ninguno). La puesta en marcha prevé un periodo de ajuste escalonado donde los operadores desplegarán gradualmente sus sistemas de monitoreo y etiquetado, y las empresas interesadas en el registro de numeración incursionarán voluntariamente en la plataforma de lista blanca antes de considerar cualquier obligatoriedad sectorial.

La CRC coordinará mesas técnicas con la industria para definir criterios de etiquetado unificados (por ejemplo, textos o iconos estándar para «llamada verificada» y «llamada sospechosa»), de manera que la experiencia de usuario sea consistente en todas las redes. Se preverán también mecanismos de salvaguarda: por ejemplo, procesos claros para que empresas no registradas puedan verificar su identidad tras ser etiquetadas como «no verificadas», o para que los usuarios reporten tanto llamadas fraudulentas no detectadas como eventuales «falsos positivos».

En general, la alternativa promueve un entorno regulatorio flexible y evolutivo. Los lineamientos obligatorios se centrarán en los objetivos funcionales (monitoreo y etiquetado del tráfico, verificación de remitentes empresariales), dejando abierta la posibilidad de que distintas tecnologías (desde análisis de señalización y plataformas de reputación hasta futuros avances en identificación de llamadas) sean empleadas para cumplirlos. Esto garantiza que la regulación pueda adaptarse con el tiempo a la evolución tecnológica, a la vez que logra la reducción de la suplantación de llamadas y el fraude telefónico a través de una acción combinada e inteligente que abarca desde la totalidad de la red hasta las comunicaciones empresariales específicas.

9.2.2.4.3 Alternativa 3: Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias

Esta alternativa plantea la creación de rangos específicos de numeración E.164, reservados exclusivamente para la originación de llamadas comerciales y publicitarias. El objetivo es establecer una diferenciación clara y visible entre las llamadas de carácter personal y aquellas con fines comerciales, facilitando la identificación por parte del usuario mediante el indicativo nacional de destino NDC, y habilitando controles regulatorios y operativos más precisos sobre el tráfico comercial.

De esta manera, en el evento en que el usuario reciba una llamada comercial desde un número que no corresponda al NDC establecido para estos fines, podría terminar la llamada por sospecha de fraude y proceder con la denuncia del número a las autoridades competentes. La asignación de estos rangos permitiría implementar políticas de trazabilidad, monitoreo y bloqueo selectivo, contribuyendo a la mitigación de riesgos de suplantación y fraude.

La CRC definiría y publicaría los bloques de numeración no geográfica destinados exclusivamente a comunicaciones comerciales y publicitarias, integrando esta información en el Sistema de Información y Gestión de Recursos de Identificación (SIGRI). Los operadores tendrían la obligación de adjudicar y enrutar el tráfico comercial únicamente a través de estos rangos. Las empresas y marcas que realicen campañas comerciales deberían solicitar a sus PRST numeración dentro de los rangos exclusivos, y utilizarla únicamente para los fines autorizados.

Para llevar a cabo esta alternativa, se establecería un calendario de migración para la transición de numeración comercial existente hacia los nuevos rangos, acompañado de campañas de información y pedagogía para los usuarios.

9.2.2.4.4 Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional

Ver explicación completa de la alternativa en el numeral 9.2.2.1.

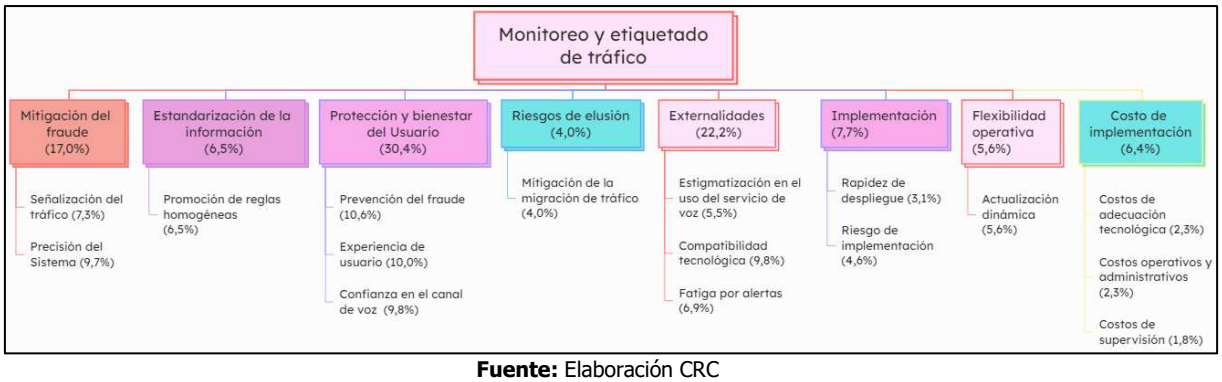
9.2.2.4.5 Evaluación de alternativas

La evaluación de alternativas regulatorias para la temática «Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas» se desarrolló mediante la metodología de Análisis de Decisión Multicriterio (ADMC). Este enfoque resulta pertinente dada la necesidad de evaluar simultáneamente múltiples dimensiones asociadas a la implementación de mecanismos de monitoreo, clasificación y etiquetado del tráfico de voz, incluyendo aspectos relacionados con la mitigación del fraude, la experiencia del usuario, la confianza en el canal de voz, la compatibilidad tecnológica, los riesgos de implementación y los costos asociados al despliegue de las medidas propuestas.

En este contexto, la metodología permitió comparar de manera estructurada el desempeño relativo de las alternativas regulatorias frente a criterios técnicos, operativos y de protección al usuario, considerando tanto los beneficios esperados en términos de fortalecimiento de la capacidad preventiva frente a fraudes tipo vishing y spoofing, como los riesgos, costos y efectos potenciales sobre la experiencia de los usuarios y la operación de los servicios de voz móvil.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 27. Árbol jerárquico de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas



Fuente: Elaboración CRC

Para el ejercicio de evaluación desarrollado se consideraron siete criterios y dieciséis subcriterios que cumplen con los principios fundamentales para la construcción de modelos multicriterio, (ver Ilustración 27). Los criterios considerados fueron: i) mitigación del fraude, ii) estandarización de la información, iii) protección y bienestar del usuario, iv) riesgos de elusión, v) externalidades, vi) implementación, vii) flexibilidad operativa y viii) costos de implementación. La matriz de comparación, junto con el resultado de la prueba de consistencia y la tabulación de los ponderadores de los subcriterios, se presentan en la sección de ANEXOS.

Criterios y Subcriterios

A continuación, se presentan las definiciones de los subcriterios establecidos para la evaluación de las diferentes alternativas regulatorias:

Mitigación del fraude

- Señalización del tráfico: Grado en que la alternativa permite identificar, categorizar y diferenciar tipos de tráfico legítimo, sospechoso o fraudulento mediante reglas o etiquetas estandarizadas.

- Precisión del sistema: Grado en que la alternativa identifica correctamente llamadas legítimas y fraudulentas.

Estandarización de la información

- Promoción de reglas homogéneas: Grado en que la alternativa establece criterios homogéneos para la clasificación del tráfico para todos los actores del sector.

Protección y bienestar del usuario

- Prevención del fraude: Grado en que el etiquetado contribuye a disminuir la probabilidad de que los usuarios sean afectados por fraudes.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Experiencia de usuario: Grado en que la alternativa fortalece la capacidad del usuario para identificar y facilitar la comprensión y gestión de llamadas entrantes.

- Confianza en el canal voz: Grado en que la alternativa incrementa la percepción de seguridad del usuario frente a las llamadas entrantes.

Riesgos de elusión

- Mitigación de la migración de tráfico: Medida en que la alternativa puede mitigar el desplazamiento de tráfico hacia canales no monitoreados o no regulados.

Externalidades

- Estigmatización en el uso del servicio de voz: Grado en que la alternativa evita generar impactos negativos sobre el uso legítimo del servicio, ya sea por rechazo de llamadas o por mal etiquetado de la línea.

- Compatibilidad tecnológica: Grado en que la alternativa puede implementarse y visualizarse correctamente en los dispositivos y redes existentes.

- Fatiga por alertas: Grado en que la alternativa evita la saturación de alertas o pérdida de efectividad de las señales.

Implementación

- Rapidez de despliegue: Tiempo requerido para implementar la alternativa desde su adopción hasta su operación efectiva.

- Riesgo de implementación: Grado en que la alternativa presenta incertidumbres técnicas, operativas y de interacción con el usuario que puedan afectar la implementación efectiva de mecanismos de información, alerta o etiquetado de llamadas.

Flexibilidad operativa

- Actualización dinámica: Grado en que la alternativa permite ajustar de manera dinámica y rápida las metodologías de monitoreo y seguimiento del tráfico de voz.

Costos de implementación

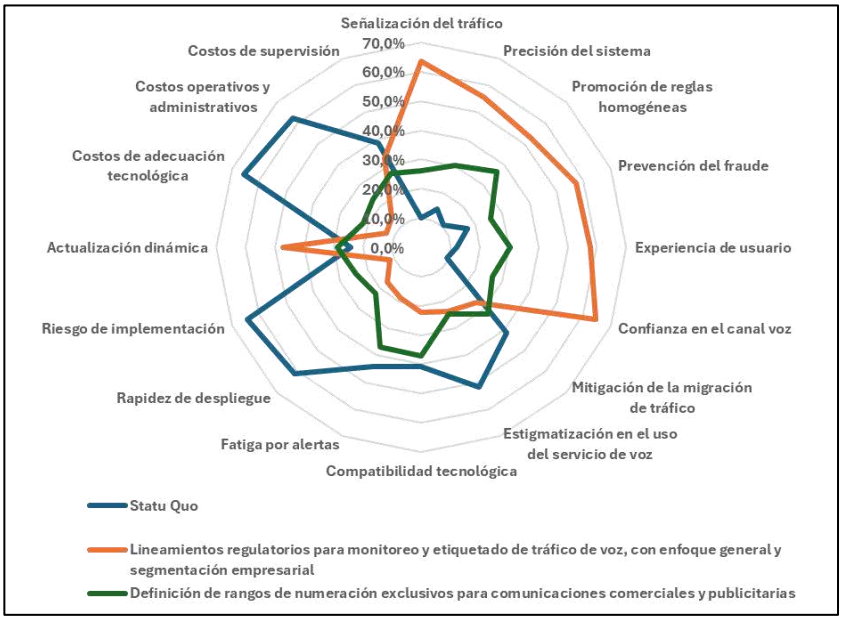
- Costos de adecuación tecnológica: Costos asociados a la implementación de sistemas de monitoreo, analítica y etiquetado del tráfico.

- Costos operativos y administrativos: Costos recurrentes derivados de la operación, mantenimiento y gestión de los procesos de monitoreo y reporte.

- Costos de supervisión: Recursos requeridos por la autoridad regulatoria para verificar el cumplimiento de las obligaciones.

Los resultados que se exponen en la Ilustración 28 de desempeño relativo corresponden al porcentaje de desempeño alcanzado por cada alternativa en cada subcriterio, ponderado según su importancia relativa dentro del modelo multicriterio. Por su parte, la Ilustración 29 de desempeño global presenta el puntaje agregado obtenido por cada alternativa evaluada. De esta manera, la evaluación permite identificar la alternativa que ofrece el mejor balance integral entre capacidad de mitigación del fraude, fortalecimiento de la información al usuario, viabilidad operativa y costos asociados a la implementación de las medidas.

Ilustración 28. Desempeño relativo de las alternativas de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas



Fuente: Elaboración CRC

A continuación, se presenta la descripción del desempeño de las alternativas regulatorias evaluadas para la temática «Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas», frente a cada uno de los criterios considerados en el análisis multicriterio.

a. En cuanto al criterio de señalización del tráfico, este evalúa la capacidad de las alternativas para identificar, categorizar y diferenciar tipos de tráfico legítimo, sospechoso o fraudulento mediante reglas o etiquetas estandarizadas. La alternativa de «Statu Quo» presenta el menor desempeño relativo (10,0%), dado que no incorpora mecanismos regulatorios de etiquetado o clasificación uniforme del tráfico de voz.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta un desempeño intermedio (26,3%), debido a que permite diferenciar visualmente las llamadas comerciales mediante bloques específicos de numeración, aunque sin incorporar capacidades dinámicas de monitoreo o clasificación de riesgo.

Por su parte, la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño relativo (63,7%), considerando que incorpora mecanismos de monitoreo en tiempo real y etiquetado preventivo de llamadas sospechosas o verificadas.

b. Respecto del criterio de precisión del sistema, este evalúa el grado en que las alternativas permiten identificar correctamente llamadas legítimas y fraudulentas. La alternativa de «Statu Quo» presenta nuevamente el menor desempeño (14,2%), dado que no incorpora herramientas regulatorias de análisis o clasificación del tráfico.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» alcanza un desempeño intermedio (30,2%), ya que facilita identificar llamadas comerciales legítimas mediante numeración diferenciada, aunque no permite detectar dinámicamente escenarios de spoofing o fraude sofisticado.

   La alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño relativo (55,6%), debido a que incorpora capacidades de monitoreo, correlación de patrones sospechosos y validación de llamadas empresariales mediante mecanismos de lista blanca.

c. En relación con el criterio de promoción de reglas homogéneas, este evalúa el nivel en que las alternativas establecen criterios comunes para la clasificación y tratamiento del tráfico de voz. La alternativa de «Statu Quo» presenta el menor desempeño (10,8%), dado que mantiene esquemas heterogéneos y discrecionales entre operadores.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta un desempeño intermedio (36,4%), considerando que introduce reglas homogéneas para el uso de rangos específicos de numeración comercial.

   Por su parte, la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» obtiene el mayor desempeño relativo (52,8%), debido a que establece criterios regulatorios comunes para el monitoreo, clasificación y etiquetado del tráfico de voz.

d. Respecto del criterio de prevención del fraude, este evalúa el grado en que las alternativas contribuyen a reducir la probabilidad de afectación de los usuarios por fraudes telefónicos. La alternativa de «Statu Quo» presenta el menor desempeño relativo (17,1%), dado que no incorpora mecanismos preventivos adicionales para alertar o informar al usuario.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta un desempeño intermedio (25,7%), debido a que facilita al usuario identificar llamadas comerciales legítimas o sospechosas según el rango de numeración utilizado.

   La alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño relativo (57,2%), considerando que incorpora alertas preventivas y mecanismos de verificación que fortalecen la capacidad de decisión del usuario frente a posibles escenarios de fraude.

e. En cuanto al criterio de experiencia de usuario, este evalúa el grado en que las alternativas facilitan la comprensión y gestión de llamadas entrantes. La alternativa de «Statu Quo» presenta el menor desempeño relativo (12,0%), debido a la ausencia de mecanismos informativos adicionales sobre el origen o naturaleza de las llamadas.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» obtiene un desempeño intermedio (30,3%), dado que facilita la identificación básica del tipo de llamada mediante numeración diferenciada.

   La alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mayor desempeño relativo (57,7%), en la medida en que incorpora etiquetas visibles de llamadas verificadas o sospechosas, fortaleciendo la capacidad del usuario para tomar decisiones informadas.

f. Respecto del criterio de confianza en el canal voz, este evalúa el grado en que las alternativas incrementan la percepción de seguridad del usuario frente a las llamadas entrantes. La alternativa de «Statu Quo» presenta el menor desempeño (9,3%), dado que mantiene las condiciones actuales sin mecanismos de verificación o etiquetado visible.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta un desempeño intermedio (26,1%), considerando que la diferenciación numérica contribuye parcialmente a la identificación del tráfico comercial.

   Por su parte, la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» obtiene el mayor desempeño relativo (64,6%), debido a que introduce mecanismos preventivos y señales visibles de autenticidad o riesgo para el usuario.

g. En relación con el criterio de mitigación de la migración de tráfico, este evalúa la capacidad de las alternativas para evitar el desplazamiento del tráfico hacia canales no monitoreados o no regulados. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (41,2%), dado que no introduce nuevas cargas regulatorias que puedan incentivar la migración hacia canales alternativos.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta un desempeño intermedio (32,3%), mientras que la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» obtiene el menor desempeño relativo (26,5%), considerando que la introducción de mecanismos de monitoreo y etiquetado podría generar incentivos parciales de desplazamiento hacia otras plataformas de comunicación.

h. En cuanto al criterio de estigmatización en el uso del servicio de voz, este evalúa el grado en que las alternativas evitan afectar negativamente el uso legítimo del servicio por errores de clasificación o etiquetado. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (51,7%), debido a que no incorpora mecanismos de etiquetado que puedan generar falsos positivos.

Las alternativas regulatorias presentan desempeños inferiores. La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» obtiene un desempeño de 24,7% dado el riesgo de generación de rechazos anticipados por parte de los usuarios de las comunicaciones legitimas, mientras que la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» alcanza un desempeño de 23,6%, reflejando el riesgo potencial de clasificación incorrecta o rechazo de llamadas legítimas.

i. Respecto del criterio de compatibilidad tecnológica, este evalúa la capacidad de implementación y visualización adecuada en redes y dispositivos existentes. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (40,7%), dado que no requiere adecuaciones adicionales.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» obtiene un desempeño intermedio (37,1%), debido a que la diferenciación mediante numeración E.164 resulta ampliamente compatible con las redes actuales.

   Por su parte, la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta un desempeño inferior (22,2%), considerando la necesidad de implementar capacidades de monitoreo, etiquetado y visualización en múltiples entornos tecnológicos.

j. En relación con el criterio de fatiga por alertas, este evalúa la capacidad de las alternativas para evitar saturación de señales o pérdida de efectividad de las alertas. La alternativa de «Statu Quo» presenta el mejor desempeño relativo (44,4%), dado que no incorpora mecanismos de alertamiento continuo.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta un desempeño intermedio (37,0%), mientras que la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» obtiene el menor desempeño relativo (18,8%), debido al riesgo de sobreexposición del usuario a alertas frecuentes.

k. Respecto del criterio de rapidez de despliegue, la alternativa de «Statu Quo» presenta el mejor desempeño relativo (61,2%), seguida de la alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» (22,2%).

   La alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» obtiene el menor desempeño (16,6%), debido a la complejidad asociada al despliegue de capacidades de monitoreo y etiquetado en tiempo real.

l. En cuanto al criterio de riesgo de implementación, la alternativa de «Statu Quo» presenta el mejor desempeño relativo (64,3%), dado que no incorpora cambios regulatorios o tecnológicos relevantes.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» obtiene un desempeño intermedio (24,2%), mientras que la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con

enfoque general y segmentación empresarial» presenta el menor desempeño relativo (11,5%), considerando la complejidad técnica y operativa asociada al monitoreo, clasificación y etiquetado dinámico de llamadas.

m. En relación con el criterio de actualización dinámica, este evalúa la capacidad de adaptación frente a nuevas tipologías de fraude. La alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño relativo (47,2%), debido a que permite ajustar dinámicamente las metodologías de análisis y clasificación del tráfico.

   La alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta un desempeño intermedio (28,7%), mientras que la alternativa de «Statu Quo» obtiene el menor desempeño relativo (24,1%).

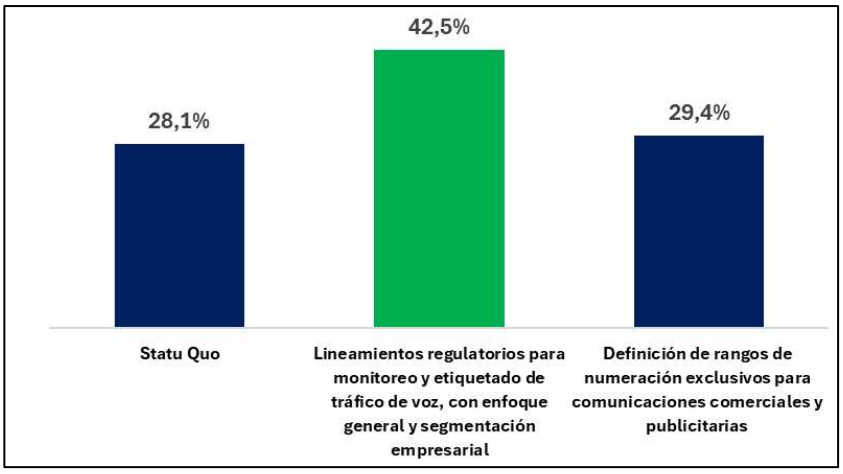
n. Finalmente, respecto de los criterios asociados a costos de implementación, la alternativa de «Statu Quo» presenta consistentemente los mejores desempeños relativos en costos de adecuación tecnológica (65,6%), costos operativos y administrativos (62,3%) y costos de supervisión (38,6%), debido a que no requiere nuevas inversiones regulatorias o tecnológicas.

o. De forma genera, la alternativa de «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» presenta desempeños intermedios en estos criterios, mientras que la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta los menores desempeños relativos, considerando los costos asociados al despliegue de herramientas de monitoreo, sistemas de clasificación, mecanismos de etiquetado y procesos de supervisión continua.

En síntesis, el análisis multicriterio evidencia que la alternativa «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño global entre las alternativas evaluadas, alcanzando un puntaje agregado de 42,5%, frente a 29,4% de la alternativa «Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias» y 28,1% del «Statu Quo» (ver Ilustración 29).

Esta alternativa sobresale especialmente en los criterios asociados a mitigación del fraude, experiencia de usuario, confianza en el canal de voz y capacidad de actualización dinámica, debido a que incorpora mecanismos integrales de monitoreo preventivo, etiquetado de llamadas sospechosas y validación de llamadas empresariales.

Ilustración 29. Puntaje agregado de cada alternativa de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas



Fuente: Elaboración CRC

No obstante, esta alternativa también presenta mayores desafíos en términos de costos, riesgos de implementación y complejidad operativa frente a las demás alternativas evaluadas. Por su parte, la alternativa basada en rangos exclusivos de numeración presenta ventajas importantes en términos de simplicidad regulatoria y compatibilidad tecnológica, aunque con capacidades más limitadas para la detección dinámica de fraude. Finalmente, el «Statu Quo» presenta ventajas en costos y facilidad de implementación, aunque mantiene las limitaciones actualmente identificadas en materia de información preventiva y protección del usuario frente a llamadas fraudulentas.

Conclusión

En consideración de los resultados obtenidos en el análisis multicriterio, la alternativa «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño global frente a los objetivos perseguidos en la temática relacionada con la falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas.

Lo anterior, debido a que incorpora mecanismos integrales de monitoreo preventivo, clasificación y etiquetado del tráfico de voz que fortalecen significativamente la capacidad de detección de patrones asociados a fraude, mejoran la información disponible para el usuario al momento de recibir la llamada y contribuyen a incrementar la confianza en el canal de voz.

Si bien esta alternativa implica mayores requerimientos de adecuación tecnológica, mayores costos operativos y una mayor complejidad de implementación frente a las demás opciones evaluadas, dichos esfuerzos se encuentran asociados al despliegue de capacidades avanzadas de monitoreo y gestión dinámica del tráfico de voz. En este sentido, la alternativa permite avanzar hacia un entorno más homogéneo y robusto de información preventiva para los usuarios, fortaleciendo la capacidad del ecosistema para mitigar riesgos asociados a vishing, spoofing y otras modalidades de fraude telefónico, sin depender exclusivamente de mecanismos estáticos de diferenciación de numeración.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9.2.2.4.6 Propuesta regulatoria «Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas»

La propuesta regulatoria para la alternativa ganadora se basa en modificar el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016, que actualmente regula la obligación general de los operadores de hacer uso de herramientas tecnólogas para prevenir la comisión de fraude, con la finalidad de incluir obligaciones particulares en materia de prevención del fraude en servicios tradicionales de voz.

Concretamente, esto se realiza mediante la adición de un numeral en ese artículo que obligará a los PRST a implementar sistemas de monitoreo en tiempo real del tráfico de voz con capacidad de detectar, como mínimo, unos patrones indicativos de actividad sospechosa que están descritos en la propuesta regulatoria, así como etiquetado de tráfico relacionada con fines publicitarios.

Seguidamente se incorpora la propuesta regulatoria:

Modificar el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, el cual quedará así:

«**ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES.** Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude:

2.1.10.7.1. Obligaciones generales:

2.1.10.7.1.1. Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y debe hacer controles periódicos respecto a la efectividad de estos mecanismos.

2.1.10.7.1.2. Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) que pueda tener relación con un presunto fraude, el operador debe investigar sus causas; y en caso de que determine la no existencia de un fraude, le debe demostrar al usuario las razones por las cuales no procede su PQR (petición, queja/ reclamo o recurso). Sin embargo, si se demuestra que el usuario actuó diligentemente en el uso del servicio contratado, no habrá lugar al cobro de los consumos objeto de reclamación.

2.1.10.7.2. Obligaciones particulares:

2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.

(…)

2.1.10.7.2.2. Obligaciones particulares en materia de prevención del fraude en los servicios tradicionales de voz. Los Proveedores de Redes y Servicios de Telecomunicaciones deberán implementar las siguientes medidas orientadas a prevenir el contacto fraudulento a usuarios a través de llamadas de voz:

(…)

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.1.10.7.2.2.2. Los PRST deberán implementar sistemas de monitoreo en tiempo real del tráfico de voz con capacidad de detectar, como mínimo, los siguientes patrones indicativos de actividad potencialmente sospechosa, las cuales pueden ser actualizadas o mejoradas en el marco del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles que se crea en virtud del artículo 2.1.10.7.3 de la presente resolución:

- Volumen inusual de llamadas por relación origen/destino, conforme a los umbrales que el PRST defina en su metodología interna, los cuales podrán ser dinámicos mediante técnicas de aprendizaje de máquina.

- Patrones repetitivos de llamadas cortas y secuenciales típicos de robocall, evaluados a través de indicadores como la duración promedio de llamada (ACD) y la tasa de respuesta (ASR).

- Correlación con listas de numeración asociadas a actividad fraudulenta, nacionales o internacionales, incluyendo las disponibles a través de mecanismos de intercambio legítimo de información.

- Eventos de enmascaramiento de numeración nacional.

Cuando el sistema de monitoreo detecte alguno de estos patrones, el PRST deberá etiquetar las llamadas originadas desde el número o rango de numeración involucrado con la indicación «Alerta de llamada sospechosa», visible en el dispositivo del usuario receptor. El etiquetado tendrá carácter temporal y se mantendrá mientras persista el patrón detectado. En ningún caso podrá extenderse por más de un mes contado desde la fecha en que cese el patrón que lo motivó.

2.1.10.7.2.2.2.1. Etiquetado de llamadas con fines publicitarios. Los PRSTM deberán crear un mecanismo que le permita a sus clientes corporativos, que utilicen los servicios tradicionales de voz para contactar a usuarios con fines publicitarios, inscribir de manera previa los rangos de numeración, números de teléfono o identidades de llamada utilizados con esa finalidad. Los referidos clientes corporativos tendrán la obligación de inscribirse en el registro creado por el PRSTM, previo a utilizar la numeración asignada que usarán con fines publicitarios. De esta manera, los PRSTM administrarán esa lista propia centralizada y dinámica de llamadas con la finalidad de etiquetar las llamadas que cumplan con esas características, originadas desde las líneas de dichos clientes, con la indicación «Llamada con fines publicitarios», visible en el dispositivo del usuario receptor. Para este efecto, los PRSTM mantendrán actualizado el registro de los clientes sujetos a este etiquetado en una lista propia administrada por el PRSTM que puede ser modificada de manera dinámica, ya sea porque sus clientes lo soliciten o porque los PRSTM así lo deciden. Aquellos PRSTM que identifiquen, en el marco del cumplimiento de las obligaciones derivadas del RNE, que sus clientes corporativos están realizando llamadas publicitarias a personas inscritas en el mencionado RNE, procederán a bloquear las llamadas en lugar de etiquetarlas.

Cada seis (6) meses, los PRST consolidarán una base de datos de todos los clientes u originadores inscritos en sus listas propias a las que hace referencia este artículo y de todas las llamadas etiquetadas como «Llamada con fines publicitarios» durante el período correspondiente y remitirán dicha información a la Superintendencia de Industria y Comercio (SIC), con copia a la CRC, dentro de los treinta (30) días hábiles siguientes al vencimiento de cada período semestral. La SIC utilizará esta información como insumo en el ejercicio de sus competencias de vigilancia y

control en materia de cumplimiento del Registro de Números Excluidos (RNE), de conformidad con el artículo 9 de la Ley 2300 de 2023.

2.1.10.7.2.2.2.2. Procedimiento de revisión del etiquetado de llamada sospechosa. El usuario titular de una línea de numeración nacional que sea objeto del etiquetado previsto en el presente artículo podrá solicitar al PRST la revisión de la medida dentro de los diez (10) días hábiles siguientes a la notificación del etiquetado, acreditando que su comportamiento de uso responde a una causa legítima. El PRST resolverá la solicitud conforme al siguiente procedimiento:

2.1.10.7.2.2.2.2.1. Una vez recibida la solicitud, el PRST analizará la información aportada por el titular y podrá requerir información adicional dentro de los tres (3) días hábiles siguientes. El plazo total para resolver no podrá exceder de diez (10) días hábiles contados desde la recepción de la solicitud completa.

2.1.10.7.2.2.2.2.2. Si el PRST determina que el comportamiento detectado corresponde al uso del servicio para fines publicitarios o comerciales, comunicará esta conclusión al titular de la línea y procederá a sustituir la etiqueta «Alerta de llamada sospechosa» por la etiqueta «Llamada con fines publicitarios» conforme al numeral 2.1.10.7.2.2.2.1. del presente artículo.

2.1.10.7.2.2.2.2.3. Si el titular de la línea no presenta la solicitud de revisión dentro del plazo establecido, o si habiéndola presentado no logra acreditar una causa legítima que explique el comportamiento detectado, el PRST podrá, previa comunicación escrita al titular con antelación mínima de cinco (5) días hábiles, dar por terminado el contrato de prestación del servicio de voz con el usuario titular de la línea, de conformidad con las condiciones contractuales aplicables y con las disposiciones del régimen de protección de usuarios de servicios de comunicaciones. La terminación del contrato no impedirá que el PRST reporte el caso al CTLFSM previsto en el artículo 2.1.10.7.3. de la presente resolución cuando el patrón detectado sea indicativo de actividad sospechosa a gran escala.

2.1.10.7.2.2.2.2.4. La aplicación del procedimiento previsto en el presente numeral no suspende el etiquetado de la llamada durante su tramitación. El etiquetado se mantendrá activo hasta que el PRST comunique al titular la conclusión del procedimiento o hasta que el patrón que lo motivó cese, lo que ocurra primero.

(…)».

9.2.2.5 Subtemática 4: Falta de estandarización en la aplicación de listas de no originación (DNO)

Situación identificada:	En el contexto colombiano, la ausencia de criterios uniformes y mecanismos coordinados para la aplicación de listas de no originación (DNO por sus siglas en inglés Do Not Originate) entre los operadores ha generado fragmentación y brechas en la protección contra el spoofing y la suplantación de identidad en el canal de voz. Cada operador gestiona sus propias listas razonables de números que no deben ser utilizados para originar llamadas, lo que dificulta la trazabilidad, permite la persistencia de prácticas fraudulentas y limita la eficacia de las medidas preventivas. La falta de estandarización impide que los usuarios y las

	autoridades cuenten con una protección homogénea y robusta frente a la suplantación de números, afectando la confianza en el servicio y la capacidad de respuesta ante incidentes.
Causa relacionada:	Causa 1: Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso. Causa 2: Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes.
Alternativa 1: Statu quo.	Consiste en mantener el esquema actual de gestión de listas de no originación (DNO) en el canal de voz, en el cual cada operador administra de manera independiente sus propias listas de números que no deben ser utilizados para originar llamadas. Bajo este enfoque, no existe un marco regulatorio uniforme ni una coordinación estandarizada para la definición, actualización o consulta de las listas DNO.
Alternativa 2: Estándar Mínimo Obligatorio de DNO con «listas propias» por PRST	Esta alternativa plantea que cada PRST mantenga su propia lista de no originación (DNO), pero bajo la obligación de cumplir con un estándar mínimo uniforme definido por la CRC. El estándar establecería categorías obligatorias de números a incluir como, por ejemplo, números no atribuidos, no asignados, no adjudicados, números comerciales o institucionales de solo recibo de llamadas, etc.
Alternativa 3: DNO definida dinámicamente por los PRST de manera colaborativa	Cosiste en que los PRST definan, implementen y administren de manera autónoma sus listas de números de no originación (DNO) estableciendo internamente los criterios técnicos y operativos para la inclusión, actualización y gestión de dichos números, con base en sus capacidades de detección de fraude, análisis de tráfico y gestión del riesgo pudiendo además aplicar tratamientos diferenciados para tráfico nacional e internacional entrante. En este escenario, la CRC asumiría un rol de acompañamiento y seguimiento con cierta periodicidad orientado a promover buenas prácticas, facilitar espacios de coordinación entre agentes del sector y realizar monitoreo general de la efectividad de las medidas adoptadas, sin imponer obligaciones específicas sobre la estructura o contenido de las listas DNO administradas por cada PRST.
Alternativa 4: Sustitución funcional de DNO por autenticación del CLI y reglas anti-spoofing internacional STIR/SHAKEN/RCD	Esta alternativa propone sustituir el paradigma de listas DNO por la exigencia de autenticación técnica del identificador de la línea llamante CLI) mediante protocolos como STIR/SHAKEN/RCD y la aplicación de reglas anti-spoofing internacional. Bajo este enfoque, la CRC exigiría la firma y verificación digital del CLI para llamadas IP, así como políticas uniformes de bloqueo o supresión del CLI nacional en llamadas internacionales entrantes con indicios de suplantación.

9.2.2.5.1 Alternativa 1: Statu quo

La alternativa statu quo consiste en mantener el esquema actual de gestión de listas de no originación (DNO) en el canal de voz, en el cual cada operador define y administra de manera independiente sus propias listas de números que no deben ser utilizados para originar llamadas. Bajo este enfoque, no existe un marco regulatorio uniforme ni una coordinación estandarizada para la definición, actualización o consulta de las listas DNO.

Los criterios de inclusión, los formatos de reporte y los procedimientos de bloqueo varían entre operadores, cuando ellos existen, lo que genera fragmentación y posibles inconsistencias en la protección contra el *spoofing* y la suplantación de identidad.

9.2.2.5.2 Alternativa 2: Estándar Mínimo Obligatorio de DNO con «listas propias» por PRST

Esta alternativa plantea que cada PRST mantenga su propia lista de no originación (DNO), pero bajo la obligación de cumplir con un estándar mínimo uniforme definido por la CRC. El estándar establecería categorías obligatorias de números a incluir como, por ejemplo, números no atribuidos, no asignados, no adjudicados, números comerciales o institucionales de solo recibo de llamadas y otras categorías que la CRC determine necesarias para cerrar brechas de suplantación y spoofing.

El objetivo es preservar la autonomía operativa de los PRST, pero garantizar que todos apliquen un piso común de protección y trazabilidad frente a la suplantación y el uso indebido de numeración.

Cada PRST tendría la responsabilidad de mantener su lista conforme al estándar, reportar periódicamente a la CRC si así se define, y someterse a auditorías de cumplimiento por parte de las autoridades competentes.

En consecuencia, los PRST implementarían mecanismos internos para bloquear llamadas originadas desde números incluidos en su lista DNO, y para responder a solicitudes de actualización o inclusión de nuevos números. Por su parte, las autoridades competentes supervisarían la correcta aplicación del estándar, gestionarían las correspondientes inspecciones, y podrían imponer sanciones en caso de incumplimiento.

Esta alternativa regulatoria es útil porque logra un equilibrio y preserva la autonomía operativa y la flexibilidad técnica de cada PRST, evitando la imposición de un sistema centralizado único que podría generar altos costos de implementación o demoras operativas, pero al mismo tiempo elimina la fragmentación actual en la que cada operador decide de forma discrecional qué números bloquear en su DNO, lo que genera inconsistencias porque pueden presentarse brechas de protección en las cuales algunas redes tengan un estándar menos exigente que otras.

Al imponer un piso común obligatorio de protección, se garantiza que todos los PRST apliquen criterios homogéneos contra el spoofing y la suplantación de identidad en el canal de voz, generando mecanismos efectivos de mitigación en el contacto a los usuarios con fines fraudulentos mediante los servicios de voz móvil.

El uso de un mismo estándar técnico para la definición del DNO genera un efecto asociado a la protección homogénea y robusta contra el contacto fraudulento vía servicios de voz móvil en todo el territorio nacional, reduciendo significativamente la posibilidad de que números no autorizados para originar llamadas sean usados por delincuentes para suplantar entidades financieras, gobierno u otras instituciones.

De esa manera los usuarios tienen menor exposición a llamadas de spoofing y vishing con lo cual se genera mayor confianza al recibir llamadas de voz móvil que provienen desde numeración nacional legítima.

En cuanto a los PRST se genera una obligación clara y uniforme de bloquear llamadas desde números DNO, con mecanismos de control y reporte. Además, se cierran brechas que hoy en día pueden aprovechar actores irregulares con lo cual la alternativa regulatoria presenta una contribución concreta a la estrategia nacional integral de prevención del fraude cibernético.

9.2.2.5.3 Alternativa 3. DNO definida dinámicamente por los PRST de manera colaborativa

Esta alternativa propone un esquema de gestión colaborativa y dinámica de listas de números de no originación (DNO) por parte de los proveedores de redes y servicios de telecomunicaciones (PRST). Bajo este enfoque, cada operador define, implementa y administra internamente sus listas DNO, con base en lo que acuerden con los demás proveedores de manera colaborativa, estableciendo los criterios técnicos y operativos para la inclusión, actualización y depuración de la numeración, con base en sus herramientas de detección de fraude, análisis de tráfico y mecanismos de gestión de riesgos asociados al uso indebido de numeración.

En este escenario, no se establecen por vía normativa estándares mínimos regulatorios para la conformación o gestión de dichas listas, lo que permite que los PRST ajusten sus mecanismos de control de manera flexible y adaptativa conforme a las condiciones operativas de sus redes, a los requerimientos del control del fraude, y a la evolución de los patrones de tráfico.

Bajo este enfoque, los PRST pueden aplicar criterios diferenciados según el tipo de tráfico cursado en sus redes, particularmente distinguiendo entre tráfico nacional y tráfico internacional entrante, atendiendo a las diferencias técnicas y operativas asociadas a cada uno de estos segmentos. Por su parte, la CRC asumiría un rol de acompañamiento y seguimiento periódico con el fin de promover buenas prácticas sectoriales y monitorear la efectividad de las medidas implementadas.

Esta alternativa se considera útil en la medida que aprovecha las capacidades técnicas y operativas de los PRST para gestionar de manera dinámica los riesgos asociados al uso indebido de numeración en el servicio de voz. Lo anterior, debido a que los operadores cuentan con herramientas de monitoreo de red, analítica de tráfico y sistemas de detección de fraude que permiten identificar patrones irregulares y ajustar rápidamente las medidas de control, incluyendo la actualización de sus listas DNO por efecto de sus propios análisis o por el reporte de terceros.

Asimismo, la posibilidad de discriminar controles según el tipo de tráfico (nacional o internacional entrante) permite aplicar medidas más proporcionales y efectivas, dado que estos segmentos presentan niveles de riesgo distintos, especialmente en relación con fenómenos como la suplantación del identificador de llamada y/o el uso indebido de numeración.

La implementación de esta alternativa permitiría que los PRST adopten mecanismos de control más flexibles y adaptativos para la gestión de numeración utilizada como identificador de llamadas, ajustando dinámicamente las listas DNO conforme evolucionen los patrones de tráfico o los riesgos asociados al fraude.

En términos regulatorios, esta aproximación reduce la necesidad de imponer estándares regulatorios prescriptivos, al tiempo que promueve la adopción de técnicas prácticas orientadas a mitigar el uso indebido de numeración. Adicionalmente, el acompañamiento y monitoreo por parte de la Comisión permitiría hacer seguimiento a la efectividad, así como fomentar la coordinación sectorial, manteniendo un balance entre autonomía operativa de los PRST y supervisión regulatoria.

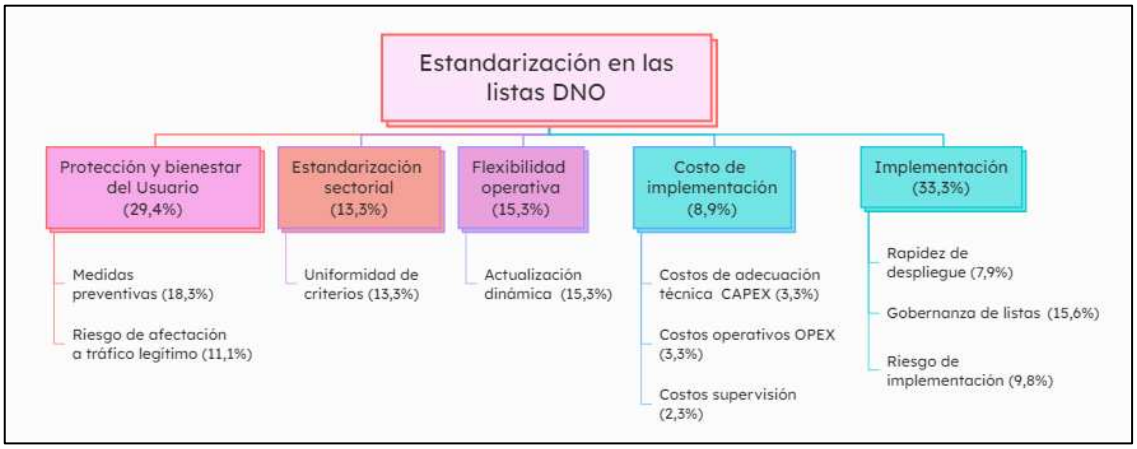
9.2.2.5.4 Alternativa 4: Sustitución funcional de DNO por STIR/SHAKEN/RCD

Ver explicación completa de la alternativa en el numeral 9.2.2.1.

9.2.2.5.5 Evaluación de alternativas

Esta sección detalla los resultados del Análisis de Decisión Multicriterio aplicado para evaluar las alternativas de gestión de listas de no originación (DNO) y autenticación de identidad, orientadas a mitigar la suplantación en redes de voz. El análisis se fundamenta en un árbol jerárquico que vincula la problemática de seguridad con sus causas técnicas y regulatorias, evaluando diversas opciones que van desde el mantenimiento del esquema actual y estándares mínimos de listas propias establecidas por la CRC, hasta modelos de gestión colaborativa y protocolos avanzados de autenticación con el acompañamiento de la CRC.

Ilustración 30. Árbol jerárquico de decisión para el análisis de las alternativas regulatorias propuestas -listas de no orignación (DNO)



Fuente: Elaboración CRC

Para el ejercicio de evaluación, se consideraron seis criterios y diez subcriterios, presentados en la Ilustración 30, los cuales cumplen con los principios fundamentales para la construcción de indicadores de impacto y viabilidad técnica.

Estos abarcan dimensiones críticas como la protección y bienestar del usuario (enfocada en la eficacia de las medidas preventivas y la mitigación del riesgo de afectación al tráfico legítimo), la estandarización sectorial mediante la uniformidad de criterios, la flexibilidad operativa para la actualización dinámica de listas, y la estructura de implementación que integra la gobernanza, la

rapidez del despliegue y los costos asociados (CAPEX, OPEX y supervisión). La matriz de comparación junto con el resultado de la prueba de consistencia, así como la tabulación de los ponderadores de los subcriterios, se encuentran en la sección de ANEXOS.

Criterios y Subcriterios

A continuación, se presentan las definiciones de los subcriterios que se establecieron para la evaluación de las diferentes alternativas:

Protección y bienestar del usuario

- Medidas preventivas: Grado en que la alternativa permite establecer parámetros amplios y objetivos para identificar y bloquear llamadas originadas desde numeración no autorizada.

- Riesgo de afectación a tráfico legítimo: Nivel en que la alternativa puede mitigar el riesgo de bloqueos indebidos de comunicaciones legítimas (falsos positivos).

Estandarización sectorial

- Uniformidad de criterios: Grado en que la alternativa establece criterios homogéneos entre todos los PRST para la inclusión de números en listas DNO.

Flexibilidad operativa

- Actualización dinámica: Grado en que la alternativa permite ajustar de manera dinámica y rápida las listas DNO y los filtros de llamadas, a fin de prevenir de manera oportuna el fraude.

Implementación

- Rapidez de despliegue: Tiempo requerido para implementar la alternativa desde su adopción hasta su operación efectiva.

- Gobernanza de listas: Grado en que la alternativa establece reglas claras, verificables y consistentes para la definición, actualización, validación, auditoría y control de los mecanismos, incluyendo la asignación de responsabilidades.

- Riesgo de implementación: Grado en que la alternativa presenta incertidumbres técnicas, operativas, de coordinación y de transición regulatoria que puedan afectar su adopción efectiva.

Costos de implementación

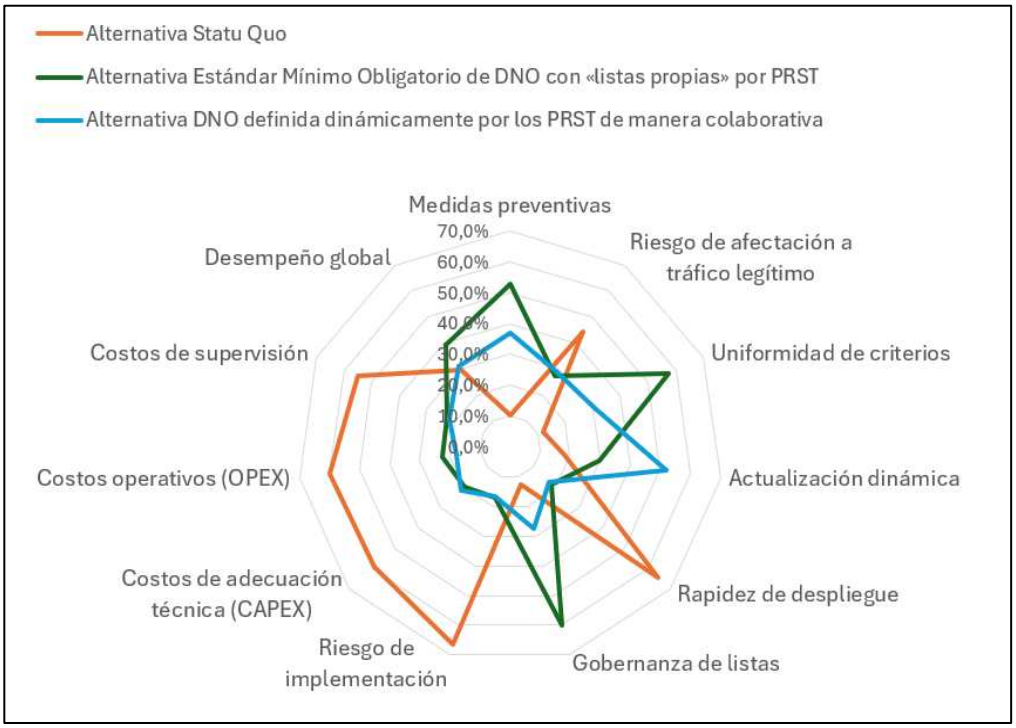
- Costos de adecuación técnica - CAPEX: Costos asociados a la implementación o ajuste de sistemas para gestionar listas DNO bajo la alternativa propuesta.

- Costos operativos - OPEX: Costos recurrentes relacionados con la administración, actualización y gestión de las listas DNO.

- Costos de supervisión: Recursos requeridos por la CRC para monitorear el cumplimiento de la alternativa.

Los resultados que se exponen en la Ilustración 31 corresponden al porcentaje de desempeño relativo alcanzado por cada alternativa en cada subcriterio, multiplicado por su respectivo ponderador, mientras que el puntaje agregado de desempeño global se presenta en la Ilustración 32. De esta manera, la evaluación permite identificar la alternativa que, en términos integrales, ofrece el mejor balance entre capacidad de respuesta al problema identificado, alineación con los objetivos del proyecto y costos de implementación.

Ilustración 31. Desempeño relativo de las alternativas regulatorias en cada criterio regulatorias propuestas -listas de no orignación (DNO)



Fuente: Elaboración CRC

A continuación, se presenta la descripción del desempeño de las alternativas frente a cada uno de los subcriterios definidos en el ejercicio de evaluación:

a. El subcriterio de Medidas preventivas evalúa el grado en que la alternativa permite establecer parámetros amplios y objetivos para identificar y bloquear llamadas originadas desde

numeración no autorizada. En este aspecto, la alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» presenta el mejor desempeño con un 52,6%, debido a que incorpora categorías homogéneas y obligatorias de numeración que deben ser incluidas en las listas DNO, fortaleciendo de manera consistente las capacidades preventivas de los operadores.

La alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» alcanza un 36,9%, mientras que el «Statu Quo» registra un 10,5%, reflejando una capacidad limitada para responder de forma uniforme frente a nuevas modalidades de fraude.

b. El subcriteiro denominado riesgo de afectación a tráfico legítimo analiza la capacidad de las alternativas para evitar bloqueos indebidos de comunicaciones legítimas o falsos positivos. El «Statu Quo» presenta el mejor desempeño relativo con un 44,2%, dado que no introduce nuevas reglas de bloqueo sobre el tráfico de voz.
Entre las alternativas regulatorias, la alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» obtiene un desempeño ligeramente superior (28,6%) frente a la alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» (27,2%), debido a que la gestión dinámica y colaborativa de listas permite realizar ajustes más rápidos y específicos sobre los criterios de inclusión y exclusión de numeración.

c. La Uniformidad de criterios evalúa el grado en que la alternativa establece reglas homogéneas entre todos los PRST para la inclusión de números en listas DNO. La alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» alcanza el mayor desempeño con un 57,2%, evidenciando que la definición de parámetros mínimos regulatorios contribuye significativamente a la estandarización sectorial y a reducir disparidades operativas entre operadores.

   Por su parte, la alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» obtiene un 30,8%, mientras que el «Statu Quo» presenta un 12,0%.

d. El subcriterio Actualización dinámica mide la capacidad de las alternativas para ajustar de manera rápida y flexible las listas DNO y los filtros de llamadas frente a nuevas modalidades de fraude. En este aspecto, la alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» presenta el mejor desempeño con un 52,1%, debido a que permite incorporar cambios ágiles y coordinados entre operadores conforme evolucionan los patrones de fraude y spoofing.

   La alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» alcanza un 29,9%, mientras que el «Statu Quo» registra un 18,0%.

e. En relación con le subcriterio Rapidez de despliegue, que evalúa la existencia de reglas claras, verificables y consistentes para la definición, actualización, validación, auditoría y control de los mecanismos DNO, «Statu Quo» presenta el mayor desempeño con un 64,6%, debido a que no requiere adecuaciones técnicas ni regulatorias adicionales. Las alternativas «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» y «DNO definida dinámicamente por los PRST de manera colaborativa» alcanzan desempeños similares de 18,2% y 17,1%, respectivamente, reflejando la necesidad de ajustes operativos y procesos de coordinación sectorial para su implementación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

f. El subcriterio de Gobernanza de listas evalúa la existencia de reglas claras, verificables y consistentes para la definición, actualización, validación, auditoría y control de los mecanismos DNO. La alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» obtiene el mejor desempeño con un 60,1%, debido a que establece obligaciones regulatorias homogéneas y mecanismos más robustos de supervisión y trazabilidad sobre la administración de las listas.

   La alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» alcanza un 27,3%, mientras que el «Statu Quo» registra un 12,6%.

g. El subcriterio riesgo de implementación analiza las incertidumbres técnicas, operativas, de coordinación y transición regulatoria que pueden afectar la adopción efectiva de las alternativas. El «Statu Quo» presenta el mejor desempeño relativo con un 66,3%, dado que no requiere procesos de transición ni adecuaciones relevantes sobre las redes y sistemas existentes.

   Las alternativas «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» y «DNO definida dinámicamente por los PRST de manera colaborativa» presentan desempeños similares de 16,9% y 16,8%, respectivamente, asociados a los desafíos de implementación y coordinación que implican ambos esquemas regulatorios.

h. El subcriterio Costos de adecuación técnica (CAPEX) evalúa las inversiones requeridas para implementar o ajustar sistemas de gestión de listas DNO bajo cada alternativa. El «Statu Quo» presenta el mejor desempeño con un 59,3%, debido a que no requiere inversiones adicionales.

   La alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» alcanza un 21,2%, mientras que la alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» obtiene un 19,5%, reflejando mayores requerimientos de adecuación tecnológica.

i. El subcriterio Costos operativos (OPEX) analiza los costos recurrentes relacionados con la administración, actualización y gestión de las listas DNO. El «Statu Quo» presenta nuevamente el mejor desempeño con un 59,9%, seguido por la alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» con un 22,4% y la alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» con un 17,7%, evidenciando mayores necesidades operativas derivadas de la gestión continua de listas y reglas de bloqueo.

j. El subcriterio Costos de supervisión evalúa los recursos requeridos por la CRC para monitorear y verificar el cumplimiento de las obligaciones regulatorias asociadas a cada alternativa. El «Statu Quo» presenta el mayor desempeño con un 55,2%, debido a que mantiene el esquema actual de supervisión.

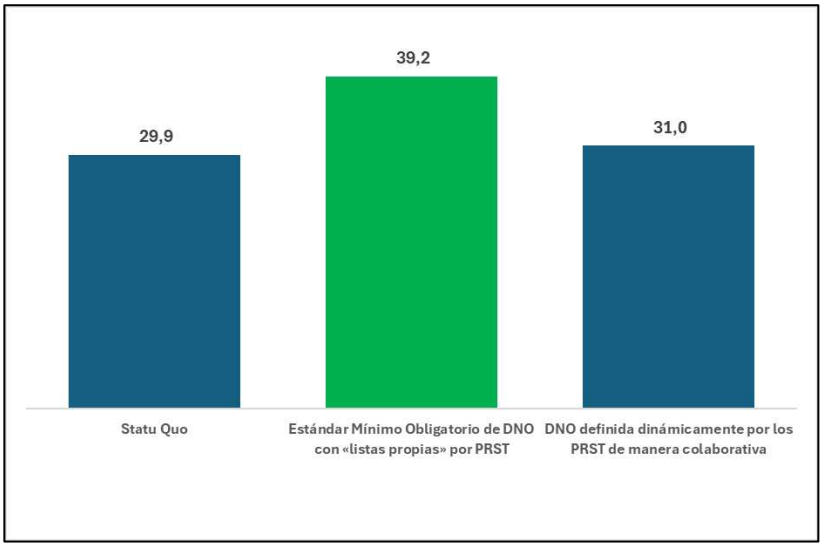
   La alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» obtiene un 22,8%, mientras que la alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» alcanza un 22,0%, reflejando mayores requerimientos de monitoreo institucional.

En términos agregados, la alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» presenta el mejor desempeño global con un 39,2%, superando tanto a la alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» con un 31,0%, como al «Statu Quo» con un 29,9%. Su principal fortaleza radica en el equilibrio alcanzado entre capacidades preventivas, estandarización sectorial y gobernanza de listas, elementos fundamentales para fortalecer la protección frente al spoofing y reducir las brechas operativas existentes entre operadores.

Aunque la alternativa «DNO definida dinámicamente por los PRST de manera colaborativa» presenta ventajas importantes en materia de actualización dinámica y flexibilidad operativa, sus mayores retos de coordinación y gobernanza limitan su desempeño global relativo.

Por su parte, el «Statu Quo» mantiene ventajas asociadas a menores costos y facilidad de implementación, pero presenta limitaciones relevantes frente a la capacidad preventiva y la uniformidad regulatoria requerida para enfrentar de manera más robusta el fraude mediante suplantación de identidad en el servicio de voz móvil.

Ilustración 32. Puntaje agregado del desempeño relativo de cada alternativa regulatoria - listas de no orignación (DNO)



Fuente: Elaboración CRC

Conclusión

La alternativa «Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST» presenta el mejor desempeño global frente a los objetivos perseguidos en materia de fortalecimiento de los mecanismos de prevención y mitigación del fraude mediante servicios de voz móvil. Lo anterior, debido a que permite establecer un esquema homogéneo, verificable y trazable para la administración de listas de no originación (DNO), fortaleciendo significativamente las capacidades preventivas frente al spoofing y la suplantación de identidad. Asimismo, la alternativa sobresale en aspectos estratégicos como las medidas preventivas, la uniformidad de criterios y la gobernanza de listas, evidenciando una elevada

capacidad para incrementar la integridad y seguridad de las comunicaciones, así como para reducir las brechas de protección existentes entre operadores.

La alternativa se fundamenta en un modelo en el cual cada PRST conserva la administración de su propia lista DNO, pero bajo la obligación de cumplir un estándar mínimo uniforme definido por la CRC. Dicho estándar incluiría categorías obligatorias de numeración que deben ser bloqueadas para originar llamadas, tales como números no atribuidos, no asignados, no adjudicados y numeración destinada únicamente a recepción de llamadas, entre otras categorías que determine la Comisión. Este enfoque permite preservar la autonomía operativa y la flexibilidad técnica de los proveedores, evitando la imposición de un sistema centralizado único que podría generar mayores costos y complejidades operativas, pero garantizando al mismo tiempo que todos los PRST apliquen criterios homogéneos y consistentes de protección frente al fraude.

9.2.2.5.6 Propuesta regulatoria «Falta de estandarización en la aplicación de listas de no originación (DNO)»

La propuesta regulatoria para la alternativa ganadora se basa en modificar el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016, que actualmente regula la obligación general de los operadores de hacer uso de herramientas tecnólogas para prevenir la comisión de fraude, con la finalidad de incluir obligaciones particulares en materia de prevención del fraude en servicios tradicionales de voz.

Concretamente, mediante la adición de un numeral en ese artículo se obligará a los PRST para que mantengan e implementen en sus redes una lista de No Originación (DNO) que contenga, como mínimo, la numeración nacional que no debe ser utilizada como identificador de línea llamante (CLI) por corresponder a numeración no atribuida, no asignada, no adjudicada por la CRC, o reservada exclusivamente para la recepción de llamadas. Los PRST deberán bloquear las llamadas que presenten numeración incluida en la lista DNO.

Respecto de las alternativas seleccionadas en las temáticas de voz, los PRST deberán implementar las medidas previstas en los nuevos numerales dentro de los tres (3) meses siguientes a la publicación en el Diario Oficial de la respectiva resolución, y acreditarán su puesta en operación ante la CRC mediante informe técnico que describa los sistemas implementados, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas.

Seguidamente se incorpora la propuesta regulatoria:

Modificar el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, el cual quedará así:

«**ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES.** Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude:

2.1.10.7.1. Obligaciones generales:

2.1.10.7.1.1. Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y debe hacer controles periódicos respecto a la efectividad de estos mecanismos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.1.10.7.1.2. Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) que pueda tener relación con un presunto fraude, el operador debe investigar sus causas; y en caso de que determine la no existencia de un fraude, le debe demostrar al usuario las razones por las cuales no procede su PQR (petición, queja/ reclamo o recurso). Sin embargo, si se demuestra que el usuario actuó diligentemente en el uso del servicio contratado, no habrá lugar al cobro de los consumos objeto de reclamación.

2.1.10.7.2. Obligaciones particulares:

2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.

(…)

2.1.10.7.2.2. Obligaciones particulares en materia de prevención del fraude en los servicios tradicionales de voz. Los Proveedores de Redes y Servicios de Telecomunicaciones deberán implementar las siguientes medidas orientadas a prevenir el contacto fraudulento a usuarios a través de llamadas de voz:

(…)

2.1.10.7.2.2.3. Los PRST deberán mantener e implementar en sus redes una lista de No Originación (DNO) que contenga, como mínimo, la numeración nacional que no debe ser utilizada como identificador de línea llamante (CLI) por corresponder a numeración no atribuida, no asignada, no adjudicada por la CRC, o reservada exclusivamente para la recepción de llamadas. Los PRST deberán bloquear las llamadas que presenten numeración incluida en la lista DNO.

El Administrador de los Recursos de Identificación publicará y mantendrá actualizada en el SIGRI la relación de numeración que debe ser incluida obligatoriamente en la lista DNO de todos los PRST. Los PRST podrán añadir a su lista DNO numeración adicional que identifiquen en el ejercicio de sus funciones de monitoreo, e informarán de dichas adiciones a la CRC dentro de los cinco (5) días hábiles siguientes a la modificación de su lista DNO.

2.1.10.7.2.2.4. Plazo de implementación y reporte. Los PRST deberán implementar las medidas previstas en los numerales 2.1.10.7.2.2.1., 2.1.10.7.2.2.2. y 2.1.10.7.2.2.3 del presente artículo dentro de los tres (3) meses siguientes a la publicación en el Diario Oficial de la resolución que las adoptó, y acreditarán su puesta en operación ante la CRC mediante informe técnico que describa los sistemas implementados, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas, los cuales serán presentados a más tardar dentro del mes siguiente al vencimiento del plazo otorgado para su implementación. Los PRST deberán reportar, previo requerimiento de la CRC, los eventos de detección, las medidas de etiquetado aplicadas, las revisiones solicitadas por usuarios y las actualizaciones realizadas a sus listas DNO, conforme al requerimiento que expida la Comisión.

(…)».

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9.2.2.6 Enfoque de evaluación de las alternativas de mejor desempeño frente a STIR/SHAKEN.

Como se indicó en las secciones anteriores, las temáticas asociadas al servicio de voz móvil fueron evaluadas inicialmente mediante las metodologías que resultaban más adecuadas según la naturaleza de cada problema regulatorio. En particular, la temática relacionada con las «Limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)» fue evaluada mediante Análisis Costo-Beneficio, mientras que las temáticas asociadas a la coordinación e intercambio de alertas, la información proporcionada al usuario sobre las llamadas recibidas y la estandarización de listas de no originación (DNO) fueron evaluadas mediante Análisis de Decisión Multicriterio (ADMC).

No obstante, la alternativa «Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional» presenta una particularidad metodológica: constituye una solución transversal que podría atender simultáneamente varias de las problemáticas identificadas en las temáticas de voz móvil.

En efecto, esta alternativa permite autenticar técnicamente el identificador de línea llamante (CLI), fortalecer la trazabilidad de las llamadas, enriquecer la información presentada al usuario mediante Rich Call Data (RCD), apoyar esquemas de etiquetado y reducir riesgos asociados a spoofing y vishing. Por esta razón, su evaluación no se realiza de forma independiente dentro de cada temática, dado que ello podría generar una sobreestimación de sus costos al contabilizar repetidamente inversiones comunes en infraestructura, certificados, interoperabilidad, monitoreo, integración y administración tecnológica.

En consecuencia, la evaluación de STIR/SHAKEN/RCD se realiza mediante un enfoque de Costos Administrativos, comparando el costo regulatorio agregado de esta solución transversal frente al costo total del paquete conformado por las medidas que obtuvieron el mejor desempeño en las cuatro temáticas de voz móvil. Este enfoque permite identificar cuál alternativa minimiza los costos administrativos, tecnológicos y operativos de implementación, considerando las economías de escala, las sinergias funcionales y los posibles solapamientos entre medidas. El modelo de costeo regulatorio utilizado para este análisis diferencia costos de inversión inicial (CAPEX), costos operativos recurrentes (OPEX), distribución de costos entre actores y sinergias potenciales entre alternativas, de acuerdo con la documentación técnica del modelo de costeo regulatorio del proyecto.

Así, el análisis compara dos opciones: i) implementar el conjunto de medidas ganadoras para cada temática de voz móvil, y ii) adoptar una solución transversal de STIR/SHAKEN/RCD que sustituya o absorba funcionalmente parte de dichas medidas. Bajo esta lógica, la decisión no se basa únicamente en la robustez tecnológica de la medida, sino en su capacidad para generar beneficios regulatorios equivalentes o superiores con menores costos administrativos y de implementación.

9.2.2.6.1 Alternativas objeto de comparación

En la Tabla 9 se presenta el paquete de medidas ganadoras, el cual está conformado por las alternativas que obtuvieron el mejor resultado en las evaluaciones previas de cada temática:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 9. Paquete de medidas ganadoras de las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

Temática	Medida ganadora	Enfoque de evaluación previo
Temática 1. Limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)	«Prohibición total del enmascaramiento de la identidad de línea llamante (CLI)»	Análisis Costo-Beneficio
Temática 2. Falta de una instancia de coordinación para la articulación y el intercambio de alertas	«Creación de un mecanismo formal de articulación y coordinación»	ADMC
Temática 3. Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas	«Lineamientos regulatorios integrales para el monitoreo y etiquetado del tráfico de voz, con enfoque general y segmentación empresarial»	ADMC
Temática 4. Falta de estandarización en la aplicación de listas de no originación (DNO)	«Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST»	ADMC

Frente a este paquete se compara la alternativa transversal «STIR/SHAKEN/RCD», la cual incorpora mecanismos de autenticación criptográfica del CLI, verificación de llamadas, administración de certificados, integración con redes IMS/SIP y visualización enriquecida de información del originador mediante Rich Call Data.

9.2.2.6.2 Resultados de la evaluación bajo el enfoque de costos administrativos

En la Tabla 10 se presentan los costos estimados para el paquete de medidas ganadoras y para la alternativa transversal STIR/SHAKEN/RCD, diferenciando entre CAPEX, OPEX anual y costo total bajo un horizonte de evaluación de tres años.

Tabla 10. Costos Administrativos de las alternativas regulatorias de mejor desempeño del segmento de voz móvil frente a STIR/SHAKEN.

Descripción corta	CAPEX (COP)	OPEX/año (COP)	Total 3 años (COP)
«Prohibición total del enmascaramiento de la identidad de línea llamante (CLI)»	4.052,7	1.533,3	8.652,7
«Creación de un mecanismo formal de articulación y coordinación»	1.337,4	670,6	3.349,4

Descripción corta	CAPEX (COP)	OPEX/año (COP)	Total 3 años (COP)
«Lineamientos regulatorios integrales para el monitoreo y etiquetado del tráfico de voz, con enfoque general y segmentación empresarial»	11.023,8	3.374,2	21.146,4
«Estándar Mínimo Obligatorio de DNO con "listas propias" por PRST»	2.588,5	856,0	5.156,5
TOTAL, PAQUETE DE MEDIDAS	19.002,6	6.434,1	38.305,0
STIR/SHAKEN/RCD (cobertura por raíz común) + (etiquetado por firma criptográfica)+ (cobertura indirecta)	104.766,4	17.845,0	158.301,4

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

Los resultados evidencian que la implementación de STIR/SHAKEN/RCD implica un costo agregado aproximadamente 4,1 veces superior al paquete de medidas regulatorias seleccionadas. La diferencia se explica principalmente por la necesidad de desplegar infraestructura especializada de autenticación SIP, servidores dedicados STI-AS/STI-VS, actualización del core IMS/SBC de los operadores, plataformas de certificación digital, mecanismos de gobernanza PKI y módulos de Rich Call Data (RCD).

Por el contrario, el paquete de medidas regulatorias aprovecha en gran medida capacidades ya existentes en los PRST, particularmente sistemas de monitoreo de tráfico, motores de reglas, mecanismos de listas internas DNO y esquemas de coordinación operativa. Esto permite reducir significativamente la necesidad de inversiones intensivas en infraestructura core de red y disminuir la complejidad técnica de integración.

9.2.2.6.3 Análisis de criterios adicionales de evaluación.

Complejidad de la implementación

Un elemento diferenciador entre ambas aproximaciones corresponde al nivel de complejidad tecnológica requerido para su despliegue. El paquete de medidas regulatorias se fundamenta principalmente en mecanismos operativos y analíticos que pueden ser implementados mediante adecuaciones incrementales sobre plataformas existentes de monitoreo, analítica de tráfico y gestión antifraude. En consecuencia, sus principales componentes corresponden a:

- motores de monitoreo y clasificación de tráfico;
- reglas anti-spoofing;
- sistemas de etiquetado;
- listas DNO;
- mecanismos de coordinación sectorial;

- plataformas livianas de intercambio de alertas.

Este enfoque reduce las dependencias tecnológicas críticas y facilita una implementación gradual y modular. En contraste, STIR/SHAKEN/RCD requiere una transformación estructural de la arquitectura de las redes para tener llamadas de voz full IP, incluyendo:

- despliegue de infraestructura PKI nacional;
- interoperabilidad SIP extremo a extremo;
- actualización de SBC/IMS;
- integración de certificados digitales;
- validación criptográfica en tiempo real;
- interoperabilidad internacional;
- soporte de Rich Call Data (RCD).

Adicionalmente, su efectividad depende de manera importante del grado de migración de las redes móviles hacia arquitecturas full IP e IMS. En escenarios donde persisten interconexiones TDM o coexistencia híbrida entre tecnologías legacy e IP, la autenticación extremo a extremo puede degradarse significativamente, limitando el alcance operativo del modelo STIR/SHAKEN. Este aspecto ha sido identificado también por la FCC y la CRTC como uno de los principales retos para la implementación plena del esquema.

Así mismo, la alternativa STIR/SHAKEN/RCD incorpora una mayor dependencia de coordinación internacional, debido a que la autenticación del CLI requiere reconocimiento mutuo de certificados y políticas de confianza entre carriers internacionales, gateways y autoridades de certificación. En ausencia de acuerdos multilaterales robustos, parte importante del tráfico internacional podría ingresar únicamente con niveles parciales de atestación (Gateway Attestation), reduciendo la efectividad del modelo frente al spoofing internacional.

Sinergias y economías de escala

A pesar de sus elevados costos iniciales, STIR/SHAKEN/RCD presenta importantes economías de escala derivadas de su naturaleza transversal. Una vez desplegada la infraestructura base, sus funcionalidades pueden utilizarse simultáneamente para:

- autenticación de CLI;
- etiquetado de llamadas;
- provisión de identidad verificada;
- mitigación de spoofing;
- trazabilidad de tráfico;
- fortalecimiento de listas DNO;
- intercambio de reputación y señales antifraude.

Esto implica que una parte significativa del CAPEX se comparte entre múltiples funcionalidades regulatorias. El modelo de costeo identificó particularmente las siguientes sinergias:

- reutilización del SOC 24/7;
- reutilización de motores de monitoreo;
- integración compartida con plataformas FMS;

- reutilización de infraestructura SBC/IMS;
- consolidación de módulos de reportería y monitoreo.

No obstante, aun considerando dichas sinergias, el costo agregado continúa siendo sustancialmente superior al paquete de medidas regulatorias seleccionadas.

Efectividad observada internacionalmente

La experiencia internacional muestra que STIR/SHAKEN ha logrado resultados positivos en la mitigación de llamadas fraudulentas, particularmente en Estados Unidos y Canadá. La FCC reportó reducciones relevantes en llamadas robocall con CLI spoofed tras la entrada en vigor de los mandatos de autenticación obligatoria en 2021. Asimismo, distintos estudios sectoriales señalan mejoras importantes en la capacidad de trazabilidad y bloqueo de tráfico fraudulento.

Por su parte, las medidas regulatorias seleccionadas en el paquete presentan una efectividad más focalizada y heterogénea. En particular, los mecanismos de monitoreo y etiquetado basados en FMS y ML permiten actualizar reglas dinámicamente conforme evolucionan los patrones de fraude, mientras que los esquemas de coordinación sectorial facilitan el intercambio operativo de alertas sin requerir transformaciones estructurales del core de red.

Conclusión

En consideración de los resultados obtenidos, se evidencia que el paquete de medidas regulatorias conformado por las alternativas ganadoras de cada temática presenta una relación más favorable entre costos de implementación, complejidad operativa y capacidad de despliegue progresivo frente a la alternativa integral basada en STIR/SHAKEN/RCD.

Si bien STIR/SHAKEN/RCD constituye una solución estructural robusta que incorpora mecanismos de autenticación criptográfica del identificador de línea llamante, fortalecimiento de la trazabilidad de las comunicaciones y provisión de información enriquecida al usuario, su implementación en el contexto actual implica costos significativamente superiores a los del paquete de medidas regulatorias seleccionado. Esta situación se explica principalmente por la necesidad de realizar adecuaciones sobre elementos críticos de la red, la implementación de infraestructura especializada de certificación y autenticación, así como por la coexistencia de arquitecturas tecnológicas heterogéneas y distintos niveles de migración hacia redes IP en el mercado colombiano.

En contraste, el paquete de medidas regulatorias permite abordar de manera incremental y complementaria las problemáticas identificadas, aprovechando capacidades ya existentes en los PRST, reduciendo la carga administrativa y financiera asociada a su implementación y facilitando una adopción gradual en el corto y mediano plazo. En este sentido, desde el enfoque de costos administrativos, la CRC identifica que el paquete de medidas regulatorias seleccionadas constituye actualmente la alternativa más eficiente y proporcional para atender las problemáticas analizadas.

En este sentido, desde el enfoque de costos administrativos, la CRC identifica que el paquete de medidas regulatorias seleccionadas constituye la alternativa más eficiente y proporcional para atender las problemáticas identificadas en el corto y mediano plazo, sin perjuicio de que futuras condiciones de madurez tecnológica, migración a redes full IP y evolución de estándares internacionales permitan reevaluar posteriormente la implementación de esquemas integrales de autenticación como

STIR/SHAKEN/RCD. En otras palabras, a medida que avance la modernización de las redes de telecomunicaciones, se consoliden arquitecturas full IP, aumente la interoperabilidad nacional e internacional y se reduzcan los costos asociados a la infraestructura de autenticación y certificación, la relación entre costos y beneficios de esta tecnología podría modificarse sustancialmente, por lo cual la CRC realizará seguimiento a la implementación de estas metodologías.

9.2.3 Temáticas enfocadas en la educación de la ciudadanía

9.2.3.1 Temática 1: Acciones educativas y de interacción con la ciudadanía que aumenten el conocimiento de los usuarios

Situación identificada:	Desconocimiento de los usuarios sobre privacidad de la información, modalidades de fraude, técnicas de ingeniería social, acciones de prevención y de mitigación, lo cual facilita la obtención de datos personales con fines fraudulentos por parte de personas inescrupulosas y la comisión de fraudes a través de mensajes de texto y llamadas de voz.
Causa relacionada:	Desconocimiento de los usuarios sobre privacidad de la información, modalidades de fraude, técnicas de ingeniería social, acciones de prevención y de mitigación, facilita la obtención de datos personales con fines fraudulentos.
Alternativa 1: Statu quo.	Mantener la provisión de redes y servicios de telecomunicaciones y de contenidos y aplicaciones y la integración tecnológica sin obligaciones de socialización o educación a los usuarios finales. En el mismo sentido, mantener sin obligaciones de socialización o educación al regulador único de telecomunicaciones en Colombia.
Alternativa 2: Acciones de pedagogía, transparencia e interacción	Incluir una serie de medidas que se materializan en obligaciones a nivel pedagógico y de prevención en beneficio de los usuarios de servicios móviles, las cuales estarán en cabeza de los PRST, PCA, IT, pero también a cargo de la CRC. Estas medidas tienen como base la coordinación y liderazgo entre los distintos agentes involucrados y el sector, de manera que se definen con claridad las responsabilidades específicas asociadas a las acciones de educación y prevención. Además, las medidas están divididas entre aquellas que son comunes para servicios SMS y voz, y otras independientes para SMS y voz respectivamente.
Alternativa 3: Sistema de trazabilidad de PQR relacionadas con fraude a través de mensajes de texto o llamadas de voz	Crear e implementar un sistema de trazabilidad de las temáticas objeto de PQR presentadas por parte de los usuarios a la CRC o a los PRST, PCA e IT, relacionadas con fraudes a través de mensajes de texto o llamadas telefónicas. Este sistema sería administrado por la CRC y alimentado con las PQR presentadas por los usuarios y la información periódica que reporten los PRST, PCA e IT.

9.2.3.1.1 Alternativa 1: Statu quo

Esta alternativa implica mantener las condiciones regulatorias vigentes, esto es, la no existencia en cabeza de los proveedores de redes y servicios de telecomunicaciones, de los proveedores de contenidos de aplicaciones y de los integradores tecnológicos, de obligaciones de divulgación y socialización acerca de los derechos que le asisten a sus usuarios frente a sus datos personales, así

como tampoco respecto de las modalidades de fraude existentes a través de mensajes de texto y llamadas de voz; y de las acciones que estos pueden tomar para prevenir o mitigar ser víctimas de las mismas.

A su vez esta alternativa también implica que las autoridades competentes en materia de protección de datos personales y de protección de los derechos de los usuarios de servicios de comunicaciones, no deben adelantar estrategias de divulgación o campañas educativas para que dichos usuarios puedan apropiarse de la información relativa a la privacidad de la información que suministran para la prestación de estos servicios, así como tampoco de las modalidades de fraude que se han evidenciado a través de SMS y llamadas de voz, y las medidas que pueden adoptar para prevenir o mitigar las mismas.

9.2.3.1.2 Alternativa 2: Acciones de pedagogía, transparencia e interacción

De acuerdo con los comentarios recibidos por los agentes interesados frente al Documento de Alternativas Regulatorias, así como de la respuesta a las preguntas formuladas en la respectiva consulta pública en relación con las temáticas a abordar en las alternativas del presente proyecto regulatorio, esta Comisión evidencia la pertinencia de formular como alternativa una serie de medidas que tengan como base la coordinación y liderazgo entre los distintos agentes involucrados y el sector, de manera que se definan con claridad las responsabilidades específicas asociadas a las acciones de educación, prevención, así como en desarrollo y formación de fuerza laboral en ciberseguridad de manera permanente al interior de los equipos de los PRST, PCA e IT.

Al respecto, se propone la adición de un capítulo al Título VI de la Resolución CRC 5050 de 2016 llamado MEDIDAS EDUCATIVAS, PEDAGÓGICAS Y DE INTERACCIÓN CON USUARIOS EN MATERIA DE PREVENCIÓN DEL FRAUDE EN EL MARCO DEL RÉGIMEN DE ADMINISTRACIÓN DE RECURSOS DE IDENTIFICACIÓN.

Por lo tanto, en ese nuevo capítulo del mencionado Título se incluirían las siguientes medidas que son comunes para servicios SMS y voz, y otras independientes para SMS y voz respectivamente, así:

1. **Medidas educativas, pedagógicas y de interacción con usuarios que son comunes para SMS y voz:**

    a. La CRC elaborará un documento o contenido en general que contenga tips, recomendaciones, guías o consejos para que los ciudadanos lo puedan consultar en un micrositio que se creará en la página web de la Comisión y que será difundido por los distintos canales de comunicación que usa la Comisión, con la finalidad de poner en conocimiento o educar al público en general acerca de la identificación de SMS o llamadas de voz con fines presuntamente fraudulentos.

    Con un objetivo similar, pero dirigido a entidades públicas, se elaborará un documento o contenido en general de consulta para esas entidades estatales que será compartido en un canal creado para esos efectos.

    Este contenido serán actualizado de manera periódica y recurrente por parte de la Comisión, en función de avances tecnológicos, nuevas modalidades de fraude y, en

general, identificación de criterios que tengan como consecuencia la necesidad de ajustar o actualizar estas guías.

Para efectos de la elaboración del contenido que contenga tips, recomendaciones, guías o consejos, la Comisión tendrá en cuenta que los destinatarios pueden tener múltiples características que ameritan un contenido diferencial, ya sea por su edad, condiciones socioeconómicas, región, entre otros.

Con ocasión de la publicación de los documentos, entregables o contenido a los cuales hace referencia esta medida, la Comisión también podrá organizar, a su elección, talleres prácticos e institucionales, los cuales serán principalmente virtuales, con la finalidad de poner en conocimiento o educar al público en general acerca de la identificación de SMS o llamadas de voz con fines presuntamente fraudulentos. Las condiciones de tiempo, modo y lugar en los cuales se realizarán esos espacios serán publicadas en el micrositio al cual hace referencia esta medida.

b. De manera correlativa, se establecería la obligación a cargo de los asignatarios y operadores de difundir el mencionado micrositio de la CRC en sus respectivas páginas web para masificar la consulta por parte de los ciudadanos. Para estos efectos, estos agentes económicos deberán adecuar su página web con una pestaña particular en la cual sus usuarios, clientes y público en general serán redirigidos al micrositio de la Comisión.

c. Los asignatarios y los operadores tendrán la obligación de desarrollar campañas pedagógicas para la prevención de fraude, en la periodicidad y los términos que la Comisión definiría en la regulación (cuatro campañas al año). De manera concreta, la Comisión definirá un hashtag para hacerle seguimiento a esas campañas pedagógicas.

   Concretamente, los asignatarios de recursos de identificación del ecosistema de mensajería A2P del TÍTULO VI de la Resolución CRC 5050 de 2016 y los PRST deberán desarrollar al menos cuatro (4) campañas pedagógicas de prevención de fraude al año, una por cada trimestre calendario (enero a marzo, abril a junio, julio a septiembre, octubre a diciembre), difundidas en todas sus redes sociales y páginas web. Las campañas deberán ser masivas, sostenidas y utilizar múltiples canales de comunicación.

   El contenido de las campañas deberá incluir, sin limitarse a ello, información sobre los derechos de los usuarios respecto de sus datos personales, las modalidades de fraude existentes a través de mensajes de texto y llamadas de voz, las técnicas de ingeniería social utilizadas por los ciberdelincuentes para obtener información confidencial, y las acciones que los usuarios pueden tomar para prevenirlas o mitigarlas. Las campañas tendrán un enfoque diferencial para usuarios en condición de vulnerabilidad, incluyendo adultos mayores, usuarios con bajos niveles de alfabetización digital y usuarios en zonas con menor acceso a servicios digitales.

   La CRC definirá mediante una circular un hashtag oficial para el seguimiento de estas campañas, así como los criterios mínimos de contenido, alcance y medios que deberán cumplir.

Dentro de los quince (15) días hábiles siguientes a la finalización de cada trimestre, el agente obligado remitirá a la CRC los comprobantes que acrediten su cumplimiento. El incumplimiento de esta obligación constituirá infracción a la regulación en los términos de la Ley 1341 de 2009 y sus modificaciones.

Además de lo anterior, estos agentes tendrán la obligación de capacitar de manera periódica a sus grupos internos de trabajo en las mismas temáticas descritas y con la misma intensidad y periodicidad.

d. La CRC promoverá espacios interinstitucionales con todas las entidades involucradas e interesadas en la prevención del fraude para crear sinergias y aunar esfuerzos en materia pedagógica y educativa. Además, se evaluará la participación de organizaciones internacionales con esos mismos propósitos y efectos.

Para el anterior efecto, al menos dos veces al año (una vez por semestre) la Comisión organizará los referidos espacios, en los que invitará a la Superintendencia de Industria y Comercio, a la Superintendencia Financiera, al MinTIC, al COLCERT, a la Fiscalía General de la Nación y a organizaciones internacionales de importante reputación en materia de lucha contra el fraude, con la finalidad de compartir experiencias en materia educativa, de transparencia e interacción con los usuarios y unir esfuerzos en la realización de campañas pedagógicas.

2. Medidas educativas o pedagógicas para los servicios de SMS:

a. La Comisión promoverá la difusión pública de sus actuaciones administrativas de recuperación, de modo que se facilite la participación de cualquier tercero interesado, en los términos de los artículos 37 y 38 de la Ley 1437 de 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Esto ayudaría a que cualquier interesado se vincule a los trámites administrativos de recuperación de recursos de identificación para los fines que correspondan, entre otros, aportar y solicitar pruebas. Lo anterior garantizaría un mayor nivel de transparencia, conocimiento, pedagogía, educación y, además, facilitaría a la Comisión contar con elementos de juicio adicionales para adoptar sus decisiones.

Esta difusión se realizaría en un micrositio específico de la página web de la Comisión que se crearía para estos efectos, en el cual la ciudadanía en general podría conocer el inicio y resultado de las actuaciones administrativas descritas.

b. La Comisión incluirá en la regulación una exigencia para los asignatarios de códigos cortos para SMS y USSD, según la cual deberán incluir en sus contratos con clientes del sector financiero la carga contractual de que los referidos clientes inscriban, en el portal web que la CRC crearía para estos efectos, los códigos cortos que usan para soportar sus servicios de mensajería, información que podrá ser consultada por el público en general en el micrositio específico creado para estos efectos.

La Comisión tendrá un plazo determinado, a partir de la publicación del acto administrativo correspondiente, para elaborar el micrositio y la herramienta en la cual será publicada la información a la cual hace referencia esta medida.

Los asignatarios tendrán un plazo de tres (3) meses para ajustar sus contratos con los clientes señalados en esta medida, contados a partir vencimiento del plazo anterior. Una vez vencido este plazo, los asignatarios deberán informar a la Comisión sobre el cumplimiento de esta obligación.

3. Medidas educativas o pedagógicas para los servicios de voz:

a. La Comisión incluirá en la regulación una exigencia para los PRST, según la cual deberán incorporar en sus contratos con clientes del sector financiero la carga contractual de que los referidos clientes inscriban, en la plataforma web que la CRC creará para estos efectos, aquella numeración E.164 geográfica o no geográfica que usan para soportar sus servicios de llamadas de voz, información que podrá ser consultada por el público en general en el micrositio específico creado para estos efectos.

La Comisión tendrá un plazo determinado, a partir de la publicación del acto administrativo correspondiente, para elaborar el micrositio y la herramienta en la cual será publicada la información a la cual hace referencia esta medida.

Los PRST tendrán un plazo de tres (3) meses para ajustar sus contratos con los clientes señalados en esta medida, contados a partir vencimiento del plazo anterior. Una vez vencido este plazo, los PRST deberán informar a la Comisión sobre el cumplimiento de esta obligación.

4. Medidas de formación interna en materia de prevención del fraude.

a. La Comisión incluirá en la regulación una exigencia para los PRST, PCA e IT según la cual deberán implementar programas de formación interna en materia de prevención del fraude cibernético dirigidos a sus equipos de trabajo, cubriendo los siguientes contenidos mínimos.

i. Las modalidades de fraude cibernético más frecuentes en el sector de las telecomunicaciones, incluyendo mecanismos tales como smishing, vishing y spoofing, así como las técnicas de ingeniería social utilizadas por los defraudadores para explotar los canales de voz y mensajería de texto.

ii. El marco regulatorio vigente en materia de prevención del fraude, incluyendo las obligaciones establecidas en la presente resolución y las consecuencias regulatorias y contractuales derivadas de su incumplimiento.

iii. Los procedimientos internos del agente para la detección, reporte y gestión de incidentes de fraude, incluyendo los canales de escalamiento hacia el validador centralizado, el Administrador de los Recursos de Identificación y el CTLFSMSM, según corresponda.

iv. Los protocolos de atención al usuario en situaciones relacionadas con el fraude, con énfasis en el trato adecuado a usuarios en condición de vulnerabilidad, incluyendo adultos mayores y usuarios con bajos niveles de alfabetización digital.

v. Las buenas prácticas en materia de protección de datos personales en el contexto de la prestación de servicios de telecomunicaciones y mensajería A2P.

9.2.3.1.3 Alternativa 3: Sistema de trazabilidad de PQR relacionadas con fraude a través de mensajes de texto o llamadas de voz

Esta alternativa propone la creación de un sistema de trazabilidad de las temáticas objeto de PQR presentadas por parte de los usuarios a la CRC o a los PRST, PCA e IT relacionadas con presuntos fraudes a través de mensajes de texto o llamadas telefónicas. Esta alternativa contribuiría a ejecutar una respuesta rápida y coordinada ante incidentes, facilitando la identificación de patrones de fraude y apoyando investigaciones judiciales.

Ahora bien, es importante aclarar que la implementación del sistema de trazabilidad propuesto en esta alternativa de ninguna manera conlleva a la publicación de los datos personales asociados a las PQR presentadas. Por el contrario, la información a publicar correspondería únicamente a las temáticas relacionadas con la presunta comisión de fraudes a través de llamadas de voz y mensajes de texto, lo cual le permitirá conocer a todos los agentes interesados las modalidades comúnmente empleadas por los delincuentes. En otras palabras, esta medida está pensada para ser una herramienta de divulgación y, por esa vía, prevención y mitigación de las modalidades de conductas fraudulentas más usuales.

Con esta alternativa se establecería la obligación en cabeza de los PRST, PCA e IT de reportar periódicamente a la CRC esta información, de tal forma que la Comisión pueda recopilar las temáticas de las PQR que le han presentado directamente, junto con la de los agentes que estarían obligados a este reporte.

En concreto, los PRST, PCA e IT deberán reportar a la CRC trimestralmente, en el formato que se creará para esos efectos, la siguiente información:

- Fecha de los hechos
- Causa de la PQR, que podrá ser fraude por vía de SMS o voz.
- Tipo de fraude reportado, ya sea smishing, phishing, vishing, entre otros.
- Persona natural o jurídica que es denunciada.

Aunado a lo anterior, esta alternativa conllevaría a que se defina una estrategia educativa y de prevención de manera conjunta entre los agentes regulados y la CRC, la cual puede servirse de los canales dispuestos por estos agentes y por la CRC para comunicarse con los ciudadanos. Para este

efecto, una vez la Comisión reciba y procese la información reportada por los agentes en la forma indicada, la CRC citará mesas de trabajo con los diferentes agentes, en las fechas y forma que la CRC decida, con la finalidad de definir las estrategias educativas y de prevención correspondientes, las cuales serán de obligatorio cumplimiento para los operadores y asignatarios.

Esta estrategia abarcaría temáticas como las modalidades de fraude existentes a través de mensajes de texto y llamadas de voz, las técnicas de ingeniería social que los ciberdelincuentes utilizan para engañar a los usuarios y así obtener su información confidencial y; las acciones que pueden tomar para prevenir o mitigar ser víctimas de estas.

9.2.3.1.4 Evaluación de alternativas

En esta sección se presentan los resultados de la evaluación de las alternativas regulatorias asociadas a las temáticas enfocadas en la educación de la ciudadanía, frente al desconocimiento de los usuarios sobre privacidad de la información, modalidades de fraude y acciones de prevención relacionadas con mensajes de texto y llamadas de voz, a partir de la aplicación del ejercicio de Análisis de Decisión Multicriterio.

En primer lugar, se presenta el árbol jerárquico de decisión, que incluye la problemática identificada, las causas relacionadas y los criterios y subcriterios definidos para el análisis. Posteriormente, se exponen los resultados de la valoración del desempeño de las alternativas regulatorias frente a cada criterio y su desempeño global ponderado.

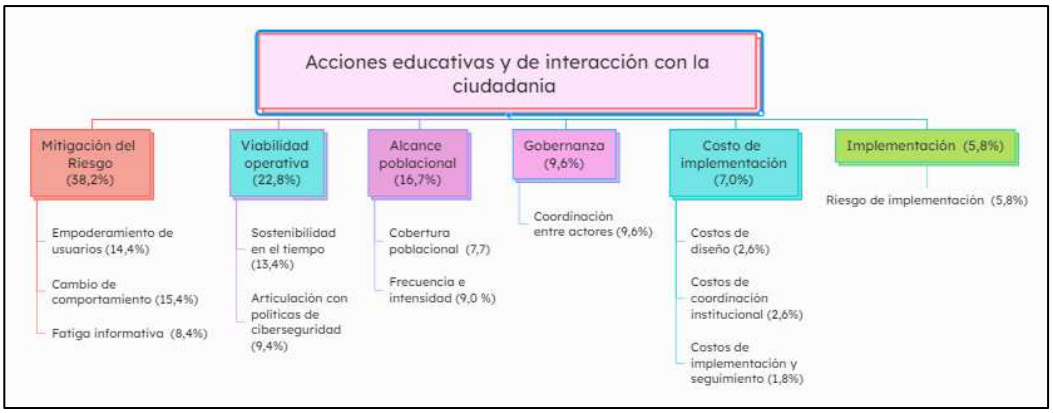
Finalmente, se presenta el análisis de cada alternativa evaluada y se identifica la medida regulatoria que resulta más conveniente, junto con la propuesta regulatoria correspondiente.

Criterios y Subcriterios

Para el ejercicio de evaluación desarrollado, se consideraron seis criterios y doce subcriterios, los cuales cumplen con los principios fundamentales para la construcción de indicadores de impacto y viabilidad. Estos abarcan dimensiones críticas como la mitigación del riesgo (enfocada en el empoderamiento, cambio de comportamiento y control de la fatiga informativa), el alcance poblacional (cobertura diferencial y frecuencia de las acciones), la gobernanza mediante la coordinación de actores, la viabilidad operativa y técnica de la implementación, y la estructura de costos asociados al diseño y seguimiento.

El árbol jerárquico de decisión que ilustra la temática sujeta de evaluación, integrando variables que van desde la sostenibilidad temporal hasta la articulación con la Estrategia Nacional de Seguridad Digital 2025-2027, se presenta en la Ilustración 33. La matriz de comparación junto con el resultado de la prueba de consistencia, así como la tabulación de los ponderadores de los subcriterios, se encuentran en la sección de Anexos.

Ilustración 33. Árbol jerárquico de decisión para el análisis de las alternativas regulatorias propuestas – Educación a la ciudadanía



Fuente: Elaboración CRC.

A continuación, se presentan las definiciones de los subcriterios que se establecieron para la evaluación de las diferentes alternativas:

Mitigación del Riesgo

- Empoderamiento de usuarios: Grado en que la alternativa proporciona herramientas, información y mecanismos que permiten a los usuarios identificar riesgos de fraude, tomar decisiones informadas y adoptar comportamientos preventivos.
- Cambio de comportamiento: Grado en que la alternativa logra generar modificaciones sostenidas en el comportamiento de los usuarios frente a riesgos de fraude cibernético.
- Fatiga Informativa: Grado en que la alternativa evita saturar al usuario con mensajes repetitivos o irrelevantes.

Alcance Poblacional

- Cobertura poblacional: Grado en que la alternativa logra integrar enfoques diferenciales sobre los usuarios, con el fin de incluir grupos poblacionales específicos como personas de tercera edad, menor nivel de formación, niños y jóvenes.
- Frecuencia e Intensidad: Grado en que la alternativa establece acciones educativas que se implementan de manera periódica, continua y con un nivel de intensidad suficiente para generar recordación y apropiación del conocimiento.

Gobernanza

- Coordinación entre actores: Grado en que la alternativa promueve acciones coordinadas entre PRST, CRC, entidades públicas y otros actores relevantes.

Implementación

- Riesgo de implementación: Grado en que la alternativa presenta incertidumbres técnicas, operativas o institucionales para su implementación efectiva.

Viabilidad Operativa

- Sostenibilidad en el tiempo: Capacidad de la alternativa para mantenerse en el tiempo sin depender de esfuerzos puntuales o no recurrentes.
- Articulación con políticas de seguridad: Grado en que la alternativa se articula con la Política Nacional de Ciberseguridad de Colombia, la Estrategia Nacional de Seguridad Digital 2025-2027 y el CONPES 3995.

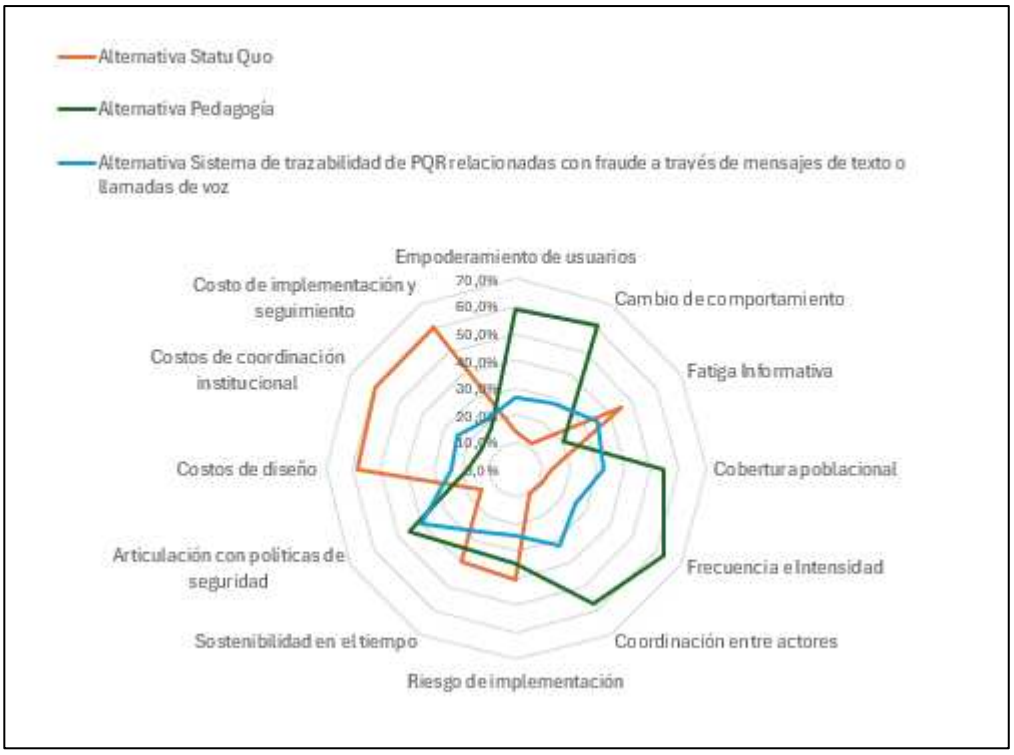
Costos de Implementación

- Costos de diseño: Costos asociados al diseño y desarrollo de las herramientas pedagógicas y de reporte de información.
- Costos de coordinación institucional: Costos derivados de la articulación entre múltiples actores para implementar las acciones.
- Costo de implementación y seguimiento: Nivel de recursos técnicos y administrativos requeridos por la autoridad regulatoria para monitorear y verificar las medidas.

Los resultados que se exponen en la Ilustración 34 corresponden al porcentaje de desempeño relativo alcanzado por cada alternativa en cada subcriterio, multiplicado por su respectivo ponderador, mientras que el puntaje agregado de desempeño global se presenta en la Ilustración 35. De esta manera, la evaluación permite identificar la alternativa que, en términos integrales, ofrece el mejor balance entre capacidad de respuesta al problema identificado, alineación con los objetivos de política pública y costos de implementación.

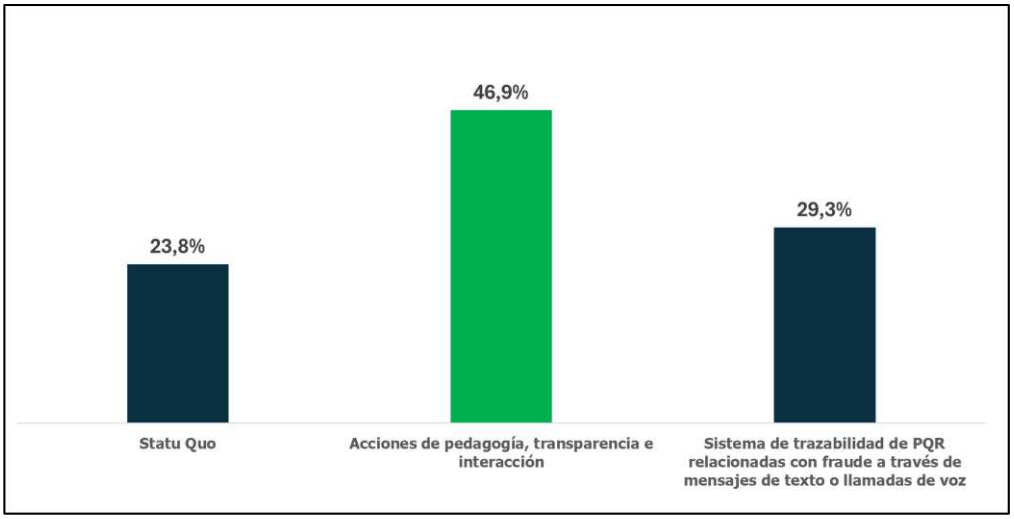
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 34. Desempeño relativo de las alternativas regulatorias en cada criterio. – Educación a la ciudadanía



Fuente: Elaboración CRC.

Ilustración 35. Puntaje agregado del desempeño relativo de cada alternativa regulatoria. - Educación a la ciudadanía



Fuente: Elaboración CRC.

A continuación, se presenta la descripción del desempeño de las alternativas frente a cada uno de los subcriterios definidos en el ejercicio de evaluación. Para efectos de claridad, se han asignado los siguientes nombres: Alternativa 1 (Statu Quo), Alternativa 2 (Pedagogía) y Alternativa 3 (Sistema de trazabilidad de PQR).

a. Mitigación del Riesgo. Este criterio evalúa la capacidad de las alternativas para reducir la vulnerabilidad de los usuarios frente al fraude mediante tres dimensiones principales. En el subcriterio de Empoderamiento de usuarios, la Alternativa 2 (Pedagogía) presenta el mejor desempeño con un 59,0%, al fortalecer las capacidades de los usuarios para identificar riesgos, reconocer modalidades de fraude y adoptar prácticas preventivas. La Alternativa 3 alcanza un 26,8%, mientras que el Statu Quo registra un 14,2%. En relación con el Cambio de comportamiento, la Alternativa 2 vuelve a sobresalir con un 60,8%, reflejando una mayor efectividad para generar transformaciones sostenidas en las conductas de prevención y autoprotección de los usuarios frente a fraudes asociados a mensajes de texto y llamadas de voz. La Alternativa 3 obtiene un 27,9%, mientras que el Statu Quo presenta el desempeño más bajo con un 11,2%. Finalmente, en el subcriterio de Fatiga Informativa, el Statu Quo alcanza el mayor desempeño relativo (45,3%), dado que no incorpora nuevas cargas informativas para los usuarios. Sin embargo, entre las alternativas regulatorias evaluadas, la Alternativa 3 presenta un mejor equilibrio (34,8%) frente a la Alternativa 2 (19,9%), lo que evidencia una mayor capacidad para evitar la saturación de mensajes y contenidos preventivos.

b. Alcance poblacional. Este componente mide la capacidad de las medidas para llegar efectivamente a distintos grupos de la población y mantener una interacción continua con los usuarios. En el subcriterio de Cobertura poblacional, la Alternativa 2 alcanza el mejor desempeño con un 54,3%, evidenciando una mayor capacidad para impactar diversos segmentos poblacionales mediante estrategias pedagógicas de amplio alcance. La Alternativa 3 obtiene un 32,6%, mientras que el Statu Quo registra un 13,2%. En cuanto a Frecuencia e Intensidad, la Alternativa 2 lidera significativamente con un 63,2%, reflejando la posibilidad de desarrollar campañas continuas, reiterativas y de alta intensidad que favorecen la recordación y apropiación de mensajes preventivos. La Alternativa 3 alcanza un 25,6%, mientras que el Statu Quo obtiene el menor desempeño con un 11,1%.

c. Gobernanza. En relación con la Coordinación entre actores, este criterio evalúa la capacidad de articulación entre los PRST, la CRC y demás entidades involucradas en la prevención del fraude. La Alternativa 2 presenta el mejor resultado con un 57,1%, lo que evidencia una estructura más sólida para coordinar acciones conjuntas, compartir información y desarrollar estrategias integradas de sensibilización y prevención. La Alternativa 3 obtiene un 32,2%, mientras que el Statu Quo alcanza únicamente un 10,7%, reflejando una limitada capacidad de articulación institucional bajo el modelo vigente.

d. Implementación. El subcriterio de Riesgo de implementación evalúa las incertidumbres técnicas, operativas y administrativas asociadas a la ejecución de cada alternativa. En este aspecto, el

Statu Quo presenta el mayor desempeño relativo (40,6%), dado que no requiere modificaciones sustanciales en procesos, infraestructura o esquemas de coordinación institucional. La Alternativa 2 obtiene un 34,6%, reflejando retos moderados asociados al diseño y despliegue de estrategias pedagógicas permanentes, mientras que la Alternativa 3 presenta el desempeño más bajo (24,7%), debido a las mayores exigencias técnicas y operativas derivadas de la implementación de sistemas de trazabilidad y gestión de información.

e. Viabilidad Operativa. Este criterio analiza la sostenibilidad de las alternativas en el tiempo y su alineación con las políticas públicas de seguridad digital. En el subcriterio de Sostenibilidad en el tiempo, el Statu Quo alcanza el mejor desempeño (39,6%), debido a que corresponde al esquema actualmente vigente y no requiere recursos adicionales permanentes. La Alternativa 2 registra un 34,2%, mostrando una capacidad importante de permanencia mediante estrategias pedagógicas mientras que la Alternativa 3 obtiene un 26,2%, asociada a mayores requerimientos técnicos y de mantenimiento operativo. Por otra parte, en Articulación con políticas de seguridad, la Alternativa 2 obtiene el mayor resultado con un 45,3%, al mostrar una mayor alineación con los objetivos nacionales de fortalecimiento de la cultura de ciberseguridad y protección de usuarios. La Alternativa 3 presenta un desempeño cercano (40,0%), mientras que el Statu Quo alcanza un 14,7%.

f. Costos de Implementación. Este bloque evalúa el impacto económico y administrativo de las medidas, donde un mayor porcentaje representa menores costos relativos o una mayor eficiencia operativa. En los subcriterios de Costos de diseño y Costos de coordinación institucional, el Statu Quo presenta los desempeños más altos (58,5% y 60,1%, respectivamente), dado que no requiere inversiones adicionales ni nuevos mecanismos institucionales. La Alternativa 3 obtiene resultados intermedios (23,6% y 24,9%), mientras que la Alternativa 2 presenta los desempeños más bajos (17,9% y 15,0%), reflejando mayores requerimientos de inversión y coordinación para el diseño, producción y ejecución de campañas pedagógicas. Asimismo, en el subcriterio de Costo de implementación y seguimiento, el Statu Quo lidera con un 60,3%, consolidándose como la alternativa de menor carga financiera y administrativa. La Alternativa 3 alcanza un 21,5%, mientras que la Alternativa 2 obtiene un 18,2%, indicando mayores necesidades de recursos para asegurar la continuidad y efectividad de las acciones implementadas.

En síntesis, el análisis multicriterio evidencia que la Alternativa 2 (Pedagogía) presenta el mejor desempeño global con un 46,9%, superando ampliamente al Sistema de trazabilidad de PQR relacionadas con fraude a través de mensajes de texto o llamadas de voz (29,3%) y al Statu Quo (23,8%). Su desempeño sobresale especialmente en los criterios de mayor peso dentro de la evaluación, como Cambio de comportamiento (60,8%), Empoderamiento de usuarios (59,0%), Frecuencia e Intensidad (63,2%), Coordinación entre actores (57,1%) y Cobertura poblacional (54,3%), lo que demuestra una elevada capacidad para fortalecer la prevención del fraude mediante estrategias de sensibilización y educación continua.

Asimismo, la alternativa muestra una importante articulación con las políticas de seguridad digital (45,3%), consolidando su coherencia con los objetivos regulatorios de protección a los usuarios. Por

su parte, el Statu Quo mantiene ventajas relativas en términos de menores costos de diseño, coordinación e implementación, así como en sostenibilidad operativa y bajo riesgo de implementación, debido a que corresponde al esquema vigente. Sin embargo, aunque la Alternativa 2 implica mayores requerimientos de inversión y coordinación institucional, los resultados evidencian que sus beneficios en mitigación del riesgo, transformación de comportamientos y fortalecimiento preventivo la posicionan como la alternativa más robusta, efectiva y alineada con los objetivos regulatorios orientados a combatir el fraude mediante mensajes de texto y llamadas de voz.

Conclusión

En consideración de los resultados obtenidos en el análisis multicriterio, la alternativa 2 «Acciones de pedagogía, transparencia e interacción» presenta el mejor desempeño global frente a los objetivos perseguidos en materia de prevención del fraude a través de mensajes de texto y llamadas de voz. Lo anterior, debido a que fortalece de manera significativa las capacidades de los usuarios para identificar riesgos, reconocer modalidades de fraude y adoptar medidas de autoprotección, contribuyendo así a la mitigación de escenarios de suplantación y engaño. Asimismo, la alternativa sobresale en criterios estratégicos como empoderamiento de usuarios, cambio de comportamiento, frecuencia e intensidad de las acciones y cobertura poblacional, lo que evidencia una alta capacidad para generar impactos sostenidos y masivos en la cultura de prevención del fraude.

La alternativa se fundamenta en un enfoque integral de educación, transparencia y coordinación institucional, mediante el cual la CRC asumiría un rol articulador en la elaboración y difusión de contenidos pedagógicos, recomendaciones y campañas preventivas dirigidas tanto a la ciudadanía como a entidades públicas. De manera complementaria, se prevé la obligación para asignatarios, operadores y PRST de desarrollar campañas pedagógicas periódicas, masivas y sostenidas en el tiempo, así como de difundir herramientas de consulta y micrositios administrados por la Comisión. Estas medidas se acompañan de espacios de articulación interinstitucional con entidades nacionales e internacionales relevantes en la lucha contra el fraude, con el propósito de fortalecer las sinergias institucionales y consolidar estrategias conjuntas de sensibilización, transparencia e interacción con los usuarios.

Adicionalmente, la alternativa incorpora medidas específicas para los servicios de SMS y voz orientadas a incrementar la transparencia y la capacidad de validación por parte de los usuarios. Entre estas se destacan la creación de micrositios para la divulgación de actuaciones administrativas de recuperación de recursos de identificación, así como mecanismos de consulta pública sobre códigos cortos y numeración utilizada por entidades del sector financiero para soportar sus servicios de mensajería y llamadas de voz. Si bien esta alternativa implica mayores requerimientos de implementación, coordinación y seguimiento frente al esquema actual, dichos esfuerzos se encuentran asociados a la adopción de un modelo preventivo y pedagógico de alcance transversal, alineado con los objetivos regulatorios de fortalecimiento de la seguridad digital, mitigación del fraude y protección efectiva de los usuarios en los servicios de comunicaciones.

9.2.3.1.5 Propuesta regulatoria «Acciones educativas y de interacción con la ciudadanía que aumenten el conocimiento de los usuarios»

La alternativa ganadora se concretará en la adición del Capítulo 14 al Título VI de la Resolución CRC 5050 de 2016, el cual contendrá las medidas educativas, pedagógicas, de interacción con usuarios en

materia de prevención del fraude en el marco del régimen de administración de recursos de identificación, así como lineamientos de desarrollo de fuerza laboral en ciberseguridad al interior de los PRST, PCA e IT.

Adiciónese el Capítulo 14 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, el cual quedará así:

«CAPÍTULO 14
MEDIDAS EDUCATIVAS, PEDAGÓGICAS Y DE INTERACCIÓN CON USUARIOS EN MATERIA DE PREVENCIÓN DEL FRAUDE EN EL MARCO DEL RÉGIMEN DE ADMINISTRACIÓN DE RECURSOS DE IDENTIFICACIÓN

SECCIÓN 1.
MEDIDAS COMUNES PARA SMS Y VOZ

ARTÍCULO 6.14.1.1. MICROSITIO DE LA CRC Y DOCUMENTOS DE CONSULTA PÚBLICA. La CRC elaborará y publicará en un micrositio específico de su página web contenido educativo y pedagógico dirigido al público en general que contenga consejos, recomendaciones y guías para la identificación de mensajes de texto y llamadas de voz con fines presuntamente fraudulentos. De manera complementaria, la CRC elaborará contenido dirigido exclusivamente a entidades públicas, el cual será compartido a través del mismo canal.

La CRC actualizará ese contenido de manera periódica en función de avances tecnológicos, nuevas modalidades de fraude o cualquier otro elemento que haga necesario su ajuste. Para la elaboración de ese contenido dirigido al público en general, la CRC tendrá en cuenta que sus destinatarios pueden tener características diversas que ameritan un tratamiento diferencial, incluyendo la edad, las condiciones socioeconómicas y la región de residencia, entre otras.

Con ocasión de la publicación de este contenido, la CRC organizará periódicamente talleres prácticos, principalmente virtuales, dirigidos al público en general y a entidades públicas. Las condiciones de tiempo, modo y lugar de estos espacios serán publicadas en el micrositio al que hace referencia el presente artículo.

La CRC tendrá un plazo de seis (6) meses contados a partir de la publicación en el Diario Oficial del acto administrativo que creó este micrositio para habilitar y/o ajustar el micrositio al que hace referencia el presente artículo, así como para publicar los contenidos a los que hace referencia esta disposición.

ARTÍCULO 6.14.1.2. OBLIGACIÓN DE DIFUSIÓN DEL MICROSITIO POR PARTE DE LOS ASIGNATARIOS Y OPERADORES. Los asignatarios de recursos de identificación que hagan parte del ecosistema A2P y los PRST deberán incluir en sus páginas web una pestaña específica a través de la cual sus usuarios, clientes y el público en general sean redirigidos al micrositio de la CRC al que hace referencia el artículo 6.14.1.1. Esta obligación deberá cumplirse dentro del mes siguiente a la publicación del micrositio por parte de la CRC.

ARTÍCULO 6.14.1.3. CAMPAÑAS PEDAGÓGICAS DE LOS ASIGNATARIOS Y OPERADORES. Los asignatarios de recursos de identificación que hagan parte del ecosistema A2P y los PRST deberán desarrollar al menos cuatro (4) campañas pedagógicas de prevención de

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

fraude al año, una por cada trimestre calendario (enero a marzo, abril a junio, julio a septiembre, octubre a diciembre), difundidas en todas sus redes sociales y páginas web. Las campañas deberán ser masivas, sostenidas y utilizar múltiples canales de comunicación.

El contenido de las campañas deberá incluir, sin limitarse a ello, información sobre los derechos de los usuarios respecto de sus datos personales, las modalidades de fraude existentes a través de mensajes de texto y llamadas de voz, las técnicas de ingeniería social utilizadas por los ciberdelincuentes para obtener información confidencial, y las acciones que los usuarios pueden tomar para prevenirlas o mitigarlas. Las campañas deben tener un enfoque diferencial para usuarios en condición de vulnerabilidad, incluyendo adultos mayores, usuarios con bajos niveles de alfabetización digital y usuarios en zonas con menor acceso a servicios digitales.

La CRC definirá mediante una circular un hashtag oficial para el seguimiento de estas campañas en cada trimestre, así como los criterios mínimos de contenido, alcance y medios que deberán cumplir.

Dentro de los quince (15) días hábiles siguientes a la finalización de cada trimestre, el agente obligado remitirá a la CRC los comprobantes que acrediten su cumplimiento.

ARTÍCULO 6.14.1.4. ESPACIOS INTERINSTITUCIONALES. La CRC promoverá espacios de coordinación interinstitucional orientados a crear sinergias y aunar esfuerzos en materia pedagógica y educativa para la prevención del fraude. Con este propósito, al menos dos veces al año, la CRC organizará espacios a los que invitará a la Superintendencia de Industria y Comercio, a la Superintendencia Financiera de Colombia, al Ministerio de Tecnologías de la Información y las Comunicaciones, al COLCERT, a la Fiscalía General de la Nación y a organizaciones nacionales e internacionales de reconocida trayectoria en materia de lucha contra el fraude cibernético, con la finalidad de compartir experiencias en materia educativa y de transparencia con los usuarios y articular esfuerzos en la realización de campañas pedagógicas conjuntas.

ARTÍCULO 6.14.1.5. FORMACIÓN INTERNA EN MATERIA DE PREVENCIÓN DEL FRAUDE. Los asignatarios de recursos de identificación que hagan parte del ecosistema A2P y los PRST deberán implementar programas de formación interna en materia de prevención del fraude cibernético dirigidos a sus equipos de trabajo, con una periodicidad mínima de cuatro (4) sesiones al año, una por cada trimestre calendario. Los programas de formación deberán cubrir, como mínimo, los siguientes contenidos:

6.14.1.5.1. Las modalidades de fraude cibernético más frecuentes en el sector de las telecomunicaciones, incluyendo mecanismos tales como smishing, vishing y spoofing, así como las técnicas de ingeniería social utilizadas por los defraudadores para explotar los canales de voz y mensajería de texto.

6.14.1.5.2. El marco regulatorio vigente en materia de prevención del fraude, incluyendo las obligaciones establecidas en la presente resolución y las consecuencias regulatorias y contractuales derivadas de su incumplimiento.

6.14.1.5.3. Los procedimientos internos del agente para la detección, reporte y gestión de incidentes de fraude, incluyendo los canales de escalamiento hacia el validador centralizado, el Administrador de los Recursos de Identificación y el CTLFSM, según corresponda.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.14.1.5.4. Los protocolos de atención al usuario en situaciones relacionadas con el fraude, con énfasis en el trato adecuado a usuarios en condición de vulnerabilidad, incluyendo adultos mayores y usuarios con bajos niveles de alfabetización digital.

6.14.1.5.5. Las buenas prácticas en materia de protección de datos personales en el contexto de la prestación de servicios de telecomunicaciones y mensajería A2P.

Los programas de formación deberán alcanzar, como mínimo, a los equipos de atención al usuario, gestión de clientes corporativos, operaciones de red, cumplimiento regulatorio y áreas comerciales. Los agentes obligados deberán garantizar que el personal que se incorpore con posterioridad al inicio de cada ciclo anual reciba la capacitación correspondiente dentro de los treinta (30) días hábiles siguientes a su vinculación.

Dentro de los quince (15) días hábiles siguientes a la finalización de cada trimestre, el agente obligado remitirá a la CRC un reporte que acredite el cumplimiento del programa de formación del período, con indicación del número de empleados capacitados, los contenidos cubiertos, la metodología utilizada y la cobertura por área funcional. Además, en las oportunidades que la CRC lo determine en el marco del CTLFSM, los agentes obligados presentarán los comprobantes, experiencias y resultados obtenidos producto de sus programas de formación de equipos internos.

SECCIÓN 2.
MEDIDAS PEDAGÓGICAS ESPECÍFICAS PARA SMS

ARTÍCULO 6.14.2.1. DIFUSIÓN PÚBLICA DE ACTUACIONES ADMINISTRATIVAS DE RECUPERACIÓN. La CRC promoverá la difusión pública de las actuaciones administrativas de recuperación de recursos de identificación, con el propósito de facilitar la participación de cualquier tercero interesado conforme a los artículos 37 y 38 de la Ley 1437 de 2011. Para tal efecto, la CRC habilitará en su página web un micrositio específico en el que se publicará el inicio y el resultado de las actuaciones administrativas de recuperación de recursos de identificación, de modo que cualquier ciudadano pueda conocerlos y, cuando lo considere pertinente, vincularse a los respectivos trámites para aportar, solicitar pruebas y, en general, ejercer derechos como tercero interesado. Para este efecto, la CRC utilizará el micrositio previsto en el numeral 6.1.1.8.1 del artículo 6.1.1.8 de la presente resolución.

ARTÍCULO 6.14.2.2. INSCRIPCIÓN DE CÓDIGOS CORTOS DEL SECTOR FINANCIERO. Los asignatarios de recursos de identificación utilizados para el envío de mensajes cortos de texto deberán incluir en sus contratos con clientes corporativos del sector financiero la obligación de que dichos clientes inscriban, en el portal que la CRC disponga para el efecto, los códigos cortos y los SENDER ID, según aplique, que utilicen para soportar sus servicios de mensajería. La información inscrita será de consulta pública a través del micrositio de la CRC.

La CRC tendrá un plazo de seis (6) meses contados a partir de la publicación en el Diario Oficial de la resolución que creó esta obligación para habilitar el portal y el micrositio a los que hace referencia el presente artículo. Los asignatarios tendrán un plazo de seis (6) meses contados a partir del vencimiento del plazo anterior para ajustar sus contratos e informar a la CRC sobre el cumplimiento de esta obligación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

SECCIÓN 3.
MEDIDAS PEDAGÓGICAS ESPECÍFICAS PARA VOZ

ARTÍCULO 6.14.3.1. INSCRIPCIÓN DE NUMERACIÓN DEL SECTOR FINANCIERO. Los PRST deberán incluir en sus contratos con clientes corporativos del sector financiero la obligación de que dichos clientes inscriban, en el portal que la CRC disponga para el efecto, la numeración E.164 geográfica o no geográfica que utilicen para soportar sus servicios de llamadas de voz. La información inscrita será de consulta pública a través del micrositio de la CRC, con el propósito de que los ciudadanos puedan verificar si un número que los ha contactado corresponde a una entidad financiera legítima.

La CRC tendrá un plazo de seis (6) meses contados a partir de la publicación en el Diario Oficial del acto administrativo que creó esta obligación para habilitar el portal y el micrositio a los que hace referencia el presente artículo. Los PRST tendrán un plazo de tres (3) meses contados a partir del vencimiento del plazo anterior para ajustar sus contratos e informar a la CRC sobre el cumplimiento de esta obligación».

9.2.4 Temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

De acuerdo con la «Política de Mejora Regulatoria» de la CRC, las dinámicas de los mercados que se regulan exigen que el ejercicio de simplificación sea constante e integral, por lo que la Comisión estableció el enfoque de simplificación como un pilar de la mejora regulatoria de aplicación constante, que tiene como finalidad contar con un marco regulatorio dinámico, sencillo, que goce de lenguaje claro y que reconozca que hace parte de un marco normativo sectorial, así como que, si bien la regulación genera costos y cargas administrativas, debe buscarse que estos no sean excesivos.

De esta manera, este enfoque de simplificación no se refiere únicamente a la reducción o eliminación de regulación, sino que es un concepto más amplio que incluye mejoras en los procesos de interacción con los sujetos de la regulación y de estos con sus usuarios, así como la optimización, digitalización y automatización de los trámites que se requieran con el fin de reducir los costos que estos puedan generar. Así las cosas, el pilar de simplificación regulatoria se materializa durante el diseño y desarrollo de la regulación de carácter general, mediante la revisión integral de las temáticas regulatorias que se revisan en los proyectos que se llevan a cabo en la CRC, con el fin de identificar si en al menos una de las medidas sujetas a revisión se cumple alguno de los siguientes criterios:

1. Evolución de mercado: Se presenta cuando las condiciones en el mercado que dieron origen a la regulación han dejado de existir, de tal manera que es inviable continuar con la aplicación de la norma existente.

2. Evolución tecnológica: Se materializa por la implementación de tecnologías que modifican ciertas características de la prestación de los servicios o transforman los modelos de negocio de los agentes involucrados, por lo que la norma correspondiente ya no es aplicable para los agentes del sector. Lo anterior se debe analizar de conformidad con las circunstancias particulares de cada caso según aplique.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

3. Duplicidad normativa: Se refiere a la existencia de artículos en dos o más normas que cumplen funciones iguales o similares.

4. Transitoriedad: Se presenta en aquellos artículos que eran aplicables durante un periodo de tiempo determinado, que ya finalizó.

Ahora bien, en el Documento de Formulación del proyecto «Simplificación Regulatoria 2024» la CRC desarrolló dos raceros adicionales a los anteriormente enumerados que entraron a formar parte de los criterios de identificación de las normas susceptibles de simplificación dentro de los cuales se destaca el de Posibilidad de optimización de la disposición regulatoria que «[s]e presenta cuando es posible mejorar la formulación, redacción, estructuración y organización interna de la proposición normativa, de manera que se fortalezca el propósito perseguido con la regla subyacente a la norma y, por lo tanto, no se afecte negativamente su finalidad original o se disminuya su eficacia». El segundo criterio se relaciona con la Posibilidad de reducción de costos de cumplimiento que se presenta cuando es posible modificar la norma de modo que se persigan los mismos objetivos y se logren los mismos resultados, pero con un menor costo de cumplimiento por parte de los agentes regulados

En este sentido, si se materializa al menos uno de los criterios antes descritos en los artículos y anexos de la Resolución CRC 5050 de 2016 que son sujetos de revisión en el marco de la presente iniciativa, estos serán candidatos para simplificar, siempre y cuando su derogación no colisione con mandatos constitucionales, legales, o lineamientos de política pública que se encuentren vigentes.

A continuación, se presentan los análisis y resultados obtenidos mediante la metodología de simplificación normativa.

9.2.4.1 Temática 1: Elementos para la mitigación del fraude por medio de la identificación de agentes reincidentes de acciones irregulares mediante el uso de códigos cortos

Situación identificada:	En el marco del proceso de recuperación de recursos de identificación, establecido en el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016, se ha identificado el uso indebido de códigos cortos de forma reincidente.
Causa relacionada:	Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso.
Alternativa 1: Statu quo.	Mantener el régimen actual de asignación y recuperación de códigos cortos, sin introducir medidas específicas frente a la reincidencia. Se seguiría aplicando la recuperación del recurso por el incumplimiento de las obligaciones generales de los asignatarios de los recursos de identificación establecidas en el artículo 6.1.1.6.2.; así como, las causales del artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, sin obligaciones adicionales para nuevos procesos de asignación.
Alternativa 2: Establecer obligaciones y consecuencias ante reincidencia que habilitan a operadores con ciertas prerrogativas contractuales	Incorporar nuevos requerimientos para la asignación y nuevas obligaciones para los asignatarios, así como ajustes en sede de recuperación. Además, se habilitará a los PRST para que puedan suspender la relación contractual con PCA/IT reincidentes por recuperación de códigos cortos y, además, para que en ciertos escenarios sea dable solicitar ante la CRC la terminación definitiva de

	la relación contractual. Por último, se dispondrá que la SIC podrá tener acceso a los expedientes de recuperación de los recursos de identificación para que tenga elementos de juicio adicionales en el marco de sus competencias relacionadas con el RNE.

9.2.4.1.1 Alternativa 1: Statu quo

Esta alternativa propone mantener el régimen vigente de administración de recursos de identificación, en el cual la reincidencia en el uso indebido de códigos cortos por parte del asignatario no genera consecuencias adicionales más allá de la recuperación del recurso y la no asignación de nuevos códigos cortos si en el año inmediatamente anterior a la solicitud de asignación la CRC recuperó uno o más códigos cortos asignados previamente a ese solicitante por alguna de las causales de recuperación dispuestas en los numerales 6.4.3.2.2., 6.4.3.2.8., 6.4.3.2.9. y 6.4.3.2.10. del artículo 6.4.3.2 de la resolución CRC 5050 de 2016.

Bajo este enfoque, los asignatarios que hayan sido objeto de recuperación de códigos cortos pueden volver a solicitar nuevos códigos cortos, pasado el tiempo al que hace referencia el artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, modificado por el artículo 101 de la Resolución CRC 7811 de 2025, y siempre que cumplan con los requisitos formales establecidos en la regulación.

9.2.4.1.2 Alternativa 2: Establecer obligaciones y consecuencias ante reincidencia que habilitan a operadores con ciertas prerrogativas contractuales

Esta alternativa contempla la posibilidad de que los PRST puedan suspender provisionalmente la relación de acceso con los PCA/IT en aquellos casos en que a estos agentes la CRC les haya recuperado por segunda vez un código corto por las causales de uso diferente al de la asignación y de remisión de contenidos en nombre de terceros sin su autorización.

En aquellos casos, los PRST podrán suspender temporalmente –por un mes– dicha relación de acceso en forma unilateral, para lo cual deberán informar tanto a la CRC como a la SIC sobre las medidas adoptadas para minimizar los efectos de tal suspensión en los usuarios. En la misma línea, se propone incluir la posibilidad de que los PRST puedan solicitar a la CRC autorización para la terminación definitiva cuando se recupere por tercera vez un código corto por las causales indicadas a un PCA/IT. Así, en estos casos, ante una nueva reincidencia –tercera recuperación de código corto por parte de la Comisión–, el PRST con quien dicho PCA/IT tiene una relación de acceso podría iniciar un trámite de desconexión definitiva ante la CRC con el fin de que esta Comisión autorice tal terminación.

La razonabilidad y proporcionalidad de esta medida se halla, en primer lugar, en que con ella se persigue un fin constitucional y regulatoriamente relevante, que no es otro más que garantizar la seguridad de los usuarios y preservar la confianza en los servicios de mensajes cortos de texto (SMS), en un contexto específico de incremento de la criminalidad materializada por medio de este servicio. En efecto, la medida se apoya en un criterio objetivo y verificable –la segunda y tercera recuperación de un código corto por causales asociadas a uso indebido– lo que evita que la actuación del PRST dependa de valoraciones subjetivas sobre el contenido del mensaje. En este sentido, la desconexión temporal y la terminación definitiva resultan adecuadas para interrumpir la continuidad del riesgo y prevenir que usuarios del PRST reciban contenidos fraudulentos desde agentes que ya han

demostrado, en más de una ocasión, incapacidad o falta de controles para asegurar el uso correcto de los códigos.

Aunado a lo anterior, la introducción de la posibilidad de suspensión por parte de los PRST y la posibilidad de autorizar la terminación de la relación de acceso en forma definitiva permitiría cerrar las brechas de eficacia que persisten si únicamente se mantiene como herramienta regulatoria la recuperación del código corto específico.

Ciertamente, la recuperación de un código corto puntual puede llegar a ser insuficiente para contener el fenómeno en cuestión cuando el PCA/IT puede continuar el envío de tráfico riesgoso a través de otros códigos cortos previamente asignados dentro de la misma relación de acceso. Así, en principio, el mes de desconexión provisional operaría como un mecanismo de contención eficaz y, al mismo tiempo, como un incentivo para que el PCA/IT adopte correctivos verificables en sus procesos internos de control, trazabilidad y autorización de campañas.

Finalmente, la posibilidad de dar por terminada la relación de acceso en forma definitiva, previa autorización de la CRC fortalecería aún más el propósito superior de garantizar la seguridad de los usuarios. Este enfoque contribuye a gestionar el riesgo sin trasladar a los PRST una carga imposible de asumir (como convertirse en árbitros del carácter fraudulento del contenido) y reduce, adicionalmente, la exposición del operador a controversias o acciones litigiosas derivadas de permitir el curso de tráfico evidentemente riesgoso.

De esta forma, la prerrogativa propuesta en cabeza de los PRST se considera proporcional porque, en todo caso, el impacto económico para el PCA/IT tiene un límite claro, como quiera que la suspensión es temporal, solo procede ante reincidencia (no ante hechos aislados) y la consecuencia más intensa, la terminación definitiva, no se activa automáticamente, sino que exige una tercera recuperación y, además, la autorización de la CRC, lo que introduce un control efectivo y, en consecuencia, evita el riesgo de arbitrariedad por parte de los PRST. Así las cosas, la ponderación entre las ventajas y desventajas que implica la medida resulta positiva, pues la posible afectación al negocio de los PCA/IT se justificaría por el propósito superior de prevenir daños a los usuarios y de reforzar la integridad del sistema.

Ahora bien, en línea con la medida planteada, también se propone la inclusión de dos nuevas causales de oposición a ser invocadas por los PRST ante una solicitud de acceso por parte de PCA/IT a quienes se les haya previamente terminado una relación de acceso con ocasión de la constatada reincidencia en materia de recuperación de códigos cortos. Así, en primer lugar, se incluirá la posibilidad de que todo aquel PRST, en virtud de cuya solicitud se haya autorizado la terminación de una relación de acceso por motivos de reincidencia en la recuperación de códigos cortos, pueda negarse a otorgar el nuevo acceso durante un (1) año a dicho PCA/IT contado a partir de la terminación definitiva autorizada por la CRC. Y, en segundo lugar, se incluirá como causal para oponerse al acceso que el PCA/IT cuya relación de acceso se terminó definitivamente no haya tomado medidas suficientes para prevenir el envío de mensajes de contenido fraudulento por medio de los códigos cortos a él asignados.

Las anteriores medidas se complementarán con la incorporación de nuevos requerimientos para la asignación y, además, de nuevas obligaciones para los asignatarios, así como ajustes en sede de recuperación, como se expone a continuación:

a. Nuevos requisitos de asignación:

- Según lo dispuesto en el numeral 6.4.2.1.3. del artículo 6.4.2.1 de la Resolución CRC 5050 de 2016 actualmente es requisito para la asignación la «descripción detallada del servicio que se prestará a través del código corto solicitado donde se especifique, como mínimo, lo siguiente: i) La indicación de si se trata de un contenido o aplicación; ii) La descripción del contenido o de aplicación a ofrecer al usuario; iii) El procedimiento de interacción con el usuario».

  En tal sentido, se modificará ese numeral para que sea requisito, además de lo anterior, que la descripción específica del contenido o funcionalidad ofrecida al usuario tenga en cuenta la categoría del contenido y las actividades operativas específicas asociadas a la prestación del servicio, lo que deberá incluir la identificación del origen del mensaje y los mecanismos que permiten su trazabilidad a lo largo del flujo de comunicación hasta la notificación al usuario final.

- El solicitante del recurso deberá informar en detalle las medidas de control y herramientas tecnológicas que serán empleadas por parte del PCA y su integrador tecnológico (según aplique) para prevenir fraudes o usos indebidos a través del envío de mensajes SMS o USSD mediante los códigos cortos solicitados, precisando su aplicación según la modalidad correspondiente.

- El solicitante deberá aportar certificado de existencia y representación legal vigente, expedido con no más de noventa (90) días, en el que conste que la matricula legal está vigente. Además, certificado de existencia y representación legal vigente del integrador tecnológico, en caso de aplicar.

b. Nuevas obligaciones:

Dentro del artículo 6.1.1.6. Resolución CRC 5050 de 2016, que consagra las obligaciones del administrador de recursos de identificación y de los asignatarios de esos recursos, se incluirán las siguientes obligaciones:

i) El asignatario de los recursos deberá contar con la autorización de terceros cuando tales recursos sean utilizados para enviar contenido en nombre de esos terceros.

ii) En el evento en que un PCA asignatario pretenda cambiar el integrador tecnológico contratado para el uso de un determinado código corto asignado, deberá informar previamente ante la CRC para efectos de modificar las condiciones iniciales de asignación.

iii) En Los asignatarios que estén obligados a contar con matrícula mercantil en los términos del Código de Comercio deberán mantenerla debidamente actualizada en los términos ordenados por el artículo 33 del Código de Comercio. De no estar actualizada la CRC puede recuperar los códigos cortos que tenga esa sociedad asignada.

Por último, se establecerá la posibilidad de que la SIC pueda acceder a los expedientes administrativos que se surten ante la CRC, relacionadas con la recuperación de recursos de identificación, para que la SIC tenga elementos de juicio adicionales en el marco de sus competencias relacionadas con el RNE.

Criterio de simplificación que cumple: Posibilidad de optimización de la disposición regulatoria.

Justificación: Es posible mejorar la formulación, redacción, estructuración y organización interna de ciertas proposiciones normativas relacionadas con la Administración de Recursos de Identificación para que la finalidad de la recuperación de los códigos cortos sea eficaz ante reincidentes. En otras palabras, por vía de este criterio se fortalecerá el propósito perseguido con la regla subyacente a la competencia que tiene la CRC en materia de recuperación de códigos cortos, para que sea eficaz en la lucha contra el fraude.

En concreto, se adicionará el Parágrafo 4 al artículo 6.1.1.8. de la Resolución CRC 5050 de 2016 con la posibilidad que tendrán los PRST, en el escenario allí descrito, para suspender provisionalmente la relación de acceso y, posteriormente, solicitar la desconexión definitiva ante un nuevo escenario de reincidencia. De manera correlativa, se adicionarán, con este mismo enfoque, los numerales 4.1.2.6.4 y 4.1.2.6.5 al artículo 4.1.2.6. del CAPÍTULO 2 del TÍTULO IV, en relación con las nuevas causales de oposición.

Además, se complementarán con esa misma finalidad las disposiciones relacionadas con obligaciones de los asignatarios y se precisarán ciertas reglas al momento de la asignación para que la finalidad y eficacia del régimen de administración de recursos de identificación se cumplan en relación con la mitigación y prevención del fraude. En concreto, se introducirán las nuevas obligaciones en el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la Resolución CRC 5050 de 2016. Además, se incluirán y precisarán nuevos requisitos para la asignación de códigos cortos por vía de modificar el artículo 6.4.2.1. de la resolución CRC 5050 de 2016. Finalmente, se incluirá una nueva causal de recuperación de códigos cortos en el artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, asociada a los escenarios de imposibilidad para continuar ejerciendo su objeto social.

Por último, se establecerá la posibilidad de que la SIC pueda acceder a los expedientes administrativos que se surten ante la CRC, relacionadas con la recuperación de recursos de identificación, para que la SIC tenga elementos de juicio adicionales en el marco de sus competencias relacionadas con el RNE. Con esto se busca optimizar las disposiciones relacionadas con la efectividad del RNE.

Propuesta regulatoria:

Modificar el parágrafo al artículo 2.1.18.1. de la Resolución CRC 5050 de 2016, el cual quedará así:

«ARTÍCULO 2.1.18.1. ACCESO AL REGISTRO DE NÚMEROS EXCLUIDOS. Toda persona que no desee ser contactada mediante mensajes publicitarios o comerciales enviados a través de SMS, aplicaciones o web o correo electrónico, ni mediante llamadas telefónicas de carácter comercial o publicitario, podrá inscribirse en el Registro de Números Excluidos (RNE), el cual es administrado por la CRC. Quienes se inscriban en el RNE podrán solicitar, en cualquier momento y de forma gratuita, que su inscripción sea eliminada del registro. La inscripción o eliminación al registro se hará efectiva a partir del día hábil siguiente.

La inscripción en el RNE no se referirá a los contactos que tengan como finalidad informar al consumidor sobre la confirmación oportuna de las operaciones monetarias realizadas, sobre ahorros voluntarios y cesantías, enviar información solicitada por el consumidor o generar alertas sobre transacciones fraudulentas, inusuales o sospechosas.

Los productores y proveedores de bienes y servicios podrán acceder al RNE para efectos de conocer si los consumidores o usuarios a quienes pretenden contactar para fines comerciales o publicitarios se encuentran inscritos en él o no.

Aquellos productores y proveedores de bienes y servicios que se encuentran inscritos en el RNE para conocer la información de los consumidores o usuarios que pretenden contactar podrán solicitar a la CRC que certifique la inscripción efectiva mediante una constancia escrita.

PARÁGRAFO. La Superintendencia de Industria y Comercio (SIC), en el marco de sus competencias y, en especial, en virtud de la facultad prevista en el artículo 9 de la Ley 2300 de 2023, podrá solicitar a la CRC cualquier tipo de información relacionada con los trámites administrativos de recuperación de recursos de identificación establecidos en el TÍTULO VI de la Resolución CRC 5050 de 2016, con la finalidad de que sirvan de insumo para las investigaciones que la SIC adelanta relacionadas con el RNE. La SIC podrá solicitar información al validador centralizado, una vez esté operativo el funcionamiento de este tercero, con la finalidad de recabar insumos y pruebas que sirvan para las investigaciones que la SIC adelanta relacionada con el RNE».

Adicionar los numerales 4.1.2.6.4 y 4.1.2.6.5 al artículo 4.1.2.6. del CAPÍTULO 2 del TÍTULO IV de la Resolución CRC 5050 de 2016, así:

«**ARTÍCULO 4.1.2.6. OPOSICIÓN A LA INTERCONEXIÓN**. Los proveedores de redes y servicios de telecomunicaciones sólo podrán negarse u oponerse a otorgar la interconexión solicitada cuando demuestren fundada y razonablemente ante la CRC, en un plazo no mayor de quince (15) días calendario, contados a partir de la respectiva solicitud, que la interconexión causaría alguno de las siguientes consecuencias:

(...)

4.1.2.6.4. Que el hecho de acceder a la solicitud implique otorgarle acceso a un asignatario de códigos cortos, ya sea PCA o IT, respecto del cual la CRC había autorizado la desconexión en el año inmediatamente anterior a la fecha de la solicitud de acceso, en los términos del parágrafo 4 del artículo 6.1.1.8 de la Resolución CRC 5050 de 2016. Si la solicitud de acceso es presentada una vez haya transcurrido más de un año, desde la fecha de ejecutoria del acto administrativo que autorizó la referida desconexión, esta causal de oposición no podrá alegarse.

4.1.2.6.5. Que el hecho de acceder a la solicitud implique otorgarle acceso a un asignatario de códigos cortos, ya sea PCA o IT, respecto del cual la CRC había autorizado la desconexión en los términos del parágrafo No. 4 del artículo 6.1.1.8 de la Resolución CRC 5050 de 2016, y que el referido asignatario no haya tomado las medidas suficientes para prevenir el envío de mensajes de contenido fraudulento por medio de los códigos cortos a él asignados y las medidas necesarias para demostrar que no volverá a incurrir

en las causales de recuperación de códigos cortos que motivaron la referida autorización de desconexión. En el evento en el que el PRST alegue esta causal, la Comisión le otorgará al PCA/IT asignatario la oportunidad para que, en el respectivo trámite administrativo, demuestre lo contrario.

El proveedor de redes y servicios de telecomunicaciones que se niegue a otorgar la interconexión está obligado a presentar, en su argumentación ante la CRC, las alternativas para evitar los daños alegados y los responsables sugeridos para adelantar tales acciones.

En caso de no llegarse a un acuerdo entre las partes afectadas, estas podrán acudir ante la CRC para iniciar un trámite administrativo de solución de controversias sobre los puntos en desacuerdo. Lo resuelto por la CRC será de obligatorio acatamiento por las partes, sin perjuicio de las acciones que puedan iniciarse ante otras autoridades y de las sanciones por incumplimientos regulatorios a que haya lugar».

Modificar el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la Resolución CRC 5050 de 2016, el cual quedará así:

«ARTÍCULO 6.1.1.6. OBLIGACIONES. Las obligaciones del Administrador de los Recursos de Identificación y de los asignatarios de esos recursos son las siguientes:

(…)

6.1.1.6.2. OBLIGACIONES GENERALES DE LOS ASIGNATARIOS DE LOS RECURSOS DE IDENTIFICACIÓN.

6.1.1.6.2.1. Demostrar que los recursos de identificación se usan eficientemente según la solicitud y la consecuente asignación por parte de la Comisión.

6.1.1.6.2.2. Utilizar el recurso de identificación en la forma y aplicación específica para la que le ha sido asignado.

6.1.1.6.2.3. No vender ni comercializar los recursos de identificación. Tampoco cederlos ni transferirlos hasta que no se tenga la autorización del Administrador de los Recursos de Identificación. El recurso de identificación llamado código corto, regulado en el Capítulo 4 del TÍTULO VI de esta resolución, no puede ser objeto de venta, comercialización, cesión o transferencia.

6.1.1.6.2.4. Implementar las acciones necesarias para garantizar el máximo aprovechamiento de cada recurso de identificación asignado, de acuerdo con los criterios de uso eficiente establecidos para tal fin.

6.1.1.6.2.5. Facilitar la información de manera veraz, completa y oportuna que sea solicitada por el Administrador de los Recursos de Identificación.

6.1.1.6.2.6. Tramitar su inscripción en el portal de trámites de la CRC o aquel sistema que lo sustituya, como requisito administrativo para la asignación de los recursos de identificación.

6.1.1.6.2.7. Mantener actualizada su información en el portal de trámites de la CRC o aquel sistema que lo sustituya. Cuando el asignatario deje de prestar sus servicios, se recuperen o se acepte la devolución de todos los recursos de identificación que le sean asignados, deberá cancelar el registro realizado en portal de trámites de la CRC, sin perjuicio de que esta Entidad conserve los datos para el ejercicio de sus funciones.

6.1.1.6.2.8. Implementar los recursos de identificación asignados dentro del término establecido para el efecto, el cual será contado a partir de la ejecutoria del acto administrativo de asignación.

6.1.1.6.2.9. Tener en cuenta los estados de los recursos de identificación registrados en el SIGRI. En el mismo sentido, los PRST deberán considerar ese estado al momento de la implementación de los recursos de identificación en sus redes, de tal forma que se garantice que estos se encuentren en estado de asignación. En todo caso, los recursos de identificación que hayan sido recuperados o se encuentren en estado disponible no podrán estar implementados en la red de los PRST, para lo cual el asignatario deberá informar a los PRST lo correspondiente, una vez la decisión de recuperación se encuentre ejecutoriada.

6.1.1.6.2.10. Devolver de manera oportuna aquellos recursos que ya no use o no necesite, en concordancia con los criterios de uso eficiente definidos.

6.1.1.6.2.11. Usar herramientas y mecanismos que resulten necesarios para garantizar que los recursos de identificación se utilizan conforme fueron asignados.

6.1.1.6.2.12. El asignatario de un código corto deberá contar con la autorización expresa y por escrito del tercero que lo autoriza, cuando los recursos de identificación sean utilizados para enviar contenido en nombre de esos terceros.

6.1.1.6.2.13. En el evento en que un PCA asignatario de un código corto pretenda cambiar su integrador tecnológico para un código corto asignado, deberá informar previamente a la CRC para efectos de modificar las condiciones de asignación iniciales.

6.1.1.6.2.14. Los asignatarios que estén obligados a contar con matrícula mercantil en los términos del Código de Comercio deberán mantenerla debidamente actualizada en los términos ordenados por el artículo 33 del Código de Comercio. De no estar actualizada la CRC puede recuperar los recursos de identificación que tenga esa sociedad asignada.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.1.1.6.2.15. Mantener actualizada su información en el RPCAI en los términos del numeral 4.2.3.2 de esta resolución».

Modificar el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016, el cual quedará así:

«ARTÍCULO 6.1.1.8. RECUPERACIÓN DE LOS RECURSOS DE IDENTIFICACIÓN. Cuando el Administrador de los Recursos de Identificación, mediante los mecanismos de verificación de uso diseñados para tal fin, detecte la presunta configuración de alguna de las causales de recuperación establecidas o el presunto uso ineficiente de algún recurso de identificación asignado, adelantará el procedimiento de recuperación establecido en este artículo, teniendo en cuenta lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA) para las actuaciones administrativas.

(...)

PARÁGRAFO 4o. Los PRST podrán suspender provisionalmente la relación de acceso con los PCA/IT que sean asignatarios de recursos de identificación, en aquellos casos en que a estos agentes la CRC les haya recuperado por segunda vez un código corto por las causales contenidas en los numerales 6.4.3.2.2., 6.4.3.2.8 y 6.4.3.2.9. del artículo 6.4.3.2 de la Resolución CRC 5050 de 2016. En este escenario, los PRST podrán suspender por un mes dicha relación de acceso en forma unilateral, para lo cual deberán informar tanto a la CRC como a la SIC sobre las medidas adoptadas para minimizar los efectos de tal suspensión en los usuarios.

Una vez superado el referido periodo de suspensión, y en el escenario en el que la CRC recupere por tercera vez un código corto por las causales indicadas en este parágrafo, los PRST podrán solicitar a la CRC la autorización para la terminación definitiva de la relación de acceso vigente con los PCA/IT que sean asignatarios de recursos de identificación, en el marco de un trámite administrativo de desconexión definitiva ante la CRC con el fin de que esta Comisión autorice tal terminación.

Esta medida tiene efectos hacía futuro desde la fecha de publicación en el Diario Oficial de la resolución por medio de la cual se adoptó. Por lo tanto, los actos administrativos de recuperación de códigos cortos que se tendrán en cuenta para efectos de aplicar las consecuencias descritas en este parágrafo serán aquellos expedidos por la CRC con posterioridad a la adopción de esta medida»

Modificar el artículo 6.4.2.1. de la Resolución CRC 5050 de 2016, el cual quedará así:

«ARTÍCULO 6.4.2.1. REQUISITOS PARA LA ASIGNACIÓN DE NUMERACIÓN DE CÓDIGOS CORTOS PARA SMS Y USSD. Para solicitar numeración de códigos cortos, el solicitante debe remitir al Administrador de los Recursos de Identificación, a través del trámite unificado de recursos de identificación dispuesto para tal fin, la siguiente información:

6.4.2.1.1. Constancia de inscripción previa en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos (RPCAI), en la que conste la actividad que desarrollará una vez le sean asignados los códigos cortos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.4.2.1.2. Código corto solicitado, el cual debe solicitarse teniendo en cuenta las diferentes modalidades del servicio, de conformidad con el artículo 6.4.1.2. o aquel que lo modifique o sustituya, y según la disponibilidad del recurso en el momento de la solicitud de acuerdo con la información del SIGRI.

6.4.2.1.3. Descripción detallada del servicio que se prestará a través del código corto solicitado donde se especifique, como mínimo, lo siguiente:

i) La indicación de si se trata de un contenido o aplicación.

ii) La descripción del contenido o de aplicación a ofrecer al usuario, con base en la categoría del contenido y las actividades operativas específicas asociadas a la prestación del servicio, lo que deberá incluir la identificación del origen del mensaje y los mecanismos que permiten su trazabilidad a lo largo del flujo de comunicación hasta la notificación al usuario final.

iii) El procedimiento de interacción con el usuario.

iv) La forma de pago prevista, en caso de que no sea un servicio gratuito.

v) Informar en detalle las medidas de control y herramientas tecnológicas que serán empleadas por parte del asignatario y su integrador tecnológico (según aplique) para prevenir fraudes o usos indebidos a través del envío de mensajes SMS o USSD mediante los códigos cortos solicitados, precisando su aplicación según la modalidad o categoría correspondiente.

6.4.2.1.4. En caso de contar con códigos cortos previamente asignados para la misma modalidad de servicio de la solicitud, el estado de implementación de tales códigos, detallando el tráfico, los ingresos y los usuarios haciendo uso del Formato T.5.2 del Título Reportes de Información.

6.4.2.1.5. Justificación detallada de la necesidad del código corto solicitado y el propósito específico del uso del código, así como cualquier otra información que el solicitante considere necesaria, pertinente y útil para soportar la solicitud de asignación.

6.4.2.1.6. Razón social y NIT del integrador tecnológico, si el solicitante soporta sus servicios en uno de ellos. Si el solicitante es un integrador tecnológico, deberá informarlo de forma expresa.

6.4.2.1.7. Certificado de existencia y representación legal vigente del solicitante, expedido con no más de noventa (90) días, en el que conste que la matricula legal está vigente. Además, certificado de existencia y representación legal vigente del integrador tecnológico, en caso de aplicar.

6.4.2.1.8. Declaración suscrita por el representante legal y, en caso de aplicar, por el revisor fiscal, en la que manifiesten quienes son los accionistas de la persona jurídica solicitante del recurso de identificación. Esta declaración deberá ser presentada para solicitar la asignación del respectivo recurso de identificación y, para aquellos asignatarios

que ya cuenten con recursos asignados, estarán obligados a presentarla dentro de los treinta días hábiles siguientes a la fecha de adopción de esta medida».

9.2.4.2 Temática 2: Condiciones para la cesión o transferencia de la asignación de recursos de identificación en códigos cortos.

Situación identificada:	En el marco del proceso de asignación de recursos de identificación, establecido en el parágrafo del artículo 6.1.1.5. de la Resolución CRC 5050 de 2016, se ha identificado la posibilidad de transferir o ceder el recurso de identificación cuando se autorice.
Causa relacionada:	Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso.
Alternativa 1: Statu quo.	Mantener el régimen actual, en el cual la cesión o transferencia de recursos de identificación se permite por lo contemplado en el parágrafo del artículo 6.1.1.5. de la Resolución CRC 5050 de 2016, sin condiciones adicionales, siempre que se cumpla con los requisitos de asignación correspondientes.
Alternativa 2: Imposición de condiciones para la cesión o transferencia	Establecer requisitos específicos para la cesión o transferencia de recursos de identificación, que incluyan, entre otros, la prohibición de cesión a reincidentes, obligación de mantener las condiciones iniciales de asignación, y la trazabilidad del recurso.

9.2.4.2.1 Alternativa 1: Statu quo

Esta alternativa propone conservar el marco normativo vigente en relación con la cesión o transferencia de recursos de identificación en códigos cortos. Bajo este esquema, los asignatarios pueden ceder sus recursos a otros actores, conforme lo establecido en el parágrafo del artículo 6.1.1.5. de la Resolución CRC 5050 de 2016 modificado por el artículo 91 de la Resolución 7811 de 2025, cuando el Administrador de los Recursos de Identificación lo autorice de manera expresa, sin necesidad de cumplir requisitos adicionales, más allá de tener que cumplir con todas las obligaciones sobre los recursos de identificación cedidos o transferidos, establecidas en la regulación.

9.2.4.2.2 Alternativa 2: Adopción de condiciones para la cesión o transferencia

La Comisión recuerda que el parágrafo del artículo 6.1.1.5 de la Resolución CRC 5050 de 2016 de manera expresa dispone que los recursos de identificación no pueden ser objeto de venta o comercialización y, además, tampoco pueden ser cedidos o transferidos, excepto cuando el Administrador de los Recursos de Identificación lo autorice de manera expresa, de oficio o a solicitud de parte, para lo cual el nuevo asignatario deberá cumplir los requisitos de asignación correspondientes. Finalmente, en el caso de emitirse una autorización expresa de cesión o transferencia de los derechos de uso de los recursos de identificación, el nuevo asignatario adquiere todas las obligaciones sobre los recursos de identificación cedidos o transferidos.

Sin perjuicio de lo anterior, y con base en los comentarios recibidos, la regla descrita se modificará con la finalidad de prohibir la posibilidad de ceder o transferir el recurso de identificación. Esto, toda vez que la Comisión no encontró algún beneficio objetivo o medible que justifique mantener la

posibilidad de cesión y, por el contrario, puede prestarse para discusiones como las planteadas en los referidos comentarios.

Criterio de simplificación que cumple: Posibilidad de optimización de la disposición regulatoria.

Justificación: Es posible mejorar la formulación y organización interna de ciertas proposiciones normativas relacionadas con la Administración de Recursos de Identificación para que se prohíba la cesión o transferencia de códigos cortos, ya que la disposición actual le resta eficacia al objetivo subyacente de mitigar o prevenir el fraude en servicios móviles de SMS del Régimen de Administración de Recursos de Identificación. En concreto, se modificará el parágrafo del artículo 6.1.1.5. de la Resolución CRC 5050 de 2016 para aclarar que los códigos cortos no pueden ser objeto de cesión o transferencia. Con el mismo objetivo, se modificará el numeral 6.1.1.6.2. del artículo 6.1.1.6.2. de la Resolución CRC 5050 de 2016, para eliminar la posibilidad de que ese recurso de identificación pueda ser objeto de cesión o transferencia.

Propuesta regulatoria:

Modificar las siguientes disposiciones:

«**TÍTULO VI.**
RÉGIMEN DE ADMINISTRACIÓN DE RECURSOS DE IDENTIFICACIÓN.

CAPÍTULO 1.
DISPOSICIONES GENERALES.

SECCIÓN 1.

(…)

ARTÍCULO 6.1.1.5. ASIGNACIÓN DE RECURSOS DE IDENTIFICACIÓN. El Administrador de los Recursos de Identificación, asignará, de oficio o a petición de los solicitantes, recursos de identificación para lo cual tendrá en cuenta las atribuciones definidas para cada recurso que se encuentren registradas en el SIGRI.

La asignación de los recursos de identificación no genera costo, por lo que los asignatarios no podrán cobrar remuneración alguna a sus usuarios por efectos de la asignación y utilización correspondiente.

PARÁGRAFO. Los recursos de identificación no pueden ser objeto de venta o comercialización. Tampoco pueden ser cedidos o transferidos, excepto cuando el Administrador de los Recursos de Identificación lo autorice de manera expresa, de oficio o a solicitud de parte, para lo cual el nuevo asignatario deberá cumplir los requisitos de asignación correspondientes. En el caso de emitirse una autorización expresa de cesión o transferencia de los derechos de uso de los recursos de identificación, el nuevo asignatario adquiere todas las obligaciones sobre los recursos de identificación cedidos o transferidos. El recurso de identificación llamado código corto, regulado en el Capítulo 4 del TÍTULO VI de esta resolución, no puede ser objeto de venta, comercialización, cesión o transferencia.

(…)

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ARTÍCULO 6.1.1.6. OBLIGACIONES. Las obligaciones del Administrador de los Recursos de Identificación y de los asignatarios de esos recursos son las siguientes:

(…)

6.1.1.6.2. OBLIGACIONES GENERALES DE LOS ASIGNATARIOS DE LOS RECURSOS DE IDENTIFICACIÓN.

(…)

6.1.1.6.2.3. No vender ni comercializar los recursos de identificación. Tampoco cederlos ni transferirlos hasta que no se tenga la autorización del Administrador de los Recursos de Identificación. El recurso de identificación llamado código corto, regulado en el Capítulo 4 del TÍTULO VI de esta resolución, no puede ser objeto de venta, comercialización, cesión o transferencia.

(…)»

9.2.4.3 Temática 3: Suspensión del tráfico cursado a través de un código corto en el marco de una actuación administrativa.

Situación identificada:	En el marco de una actuación administrativa de recuperación de un código corto, se ha identificado que el tráfico asociado a dicho recurso continúa cursándose hasta que se emita una decisión definitiva.
Causa relacionada:	Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso.
Alternativa 1: Statu quo.	Mantener el procedimiento actual de recuperación de recursos de identificación, en el cual se contempla la suspensión del tráfico al inicio del proceso administrativo de recuperación.
Alternativa 2: Suspensión preventiva del tráfico en cualquiera etapa de la actuación administrativa y participación de terceros con interés directo	Incorporar en el régimen la posibilidad de suspender temporalmente el tráfico cursado a través de un código corto en cualquier momento de la actuación administrativa, según unos escenarios descritos en la regulación. Además, se incorpora la medida de publicitar el inicio de la actuación administrativa para garantizar la participación de terceros con interés.

9.2.4.3.1 Alternativa 1: Statu quo

Esta alternativa propone mantener el procedimiento actual de recuperación de recursos de identificación, conforme a lo establecido en el régimen vigente. Bajo este esquema, conforme el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016, modificado por el artículo 94 de la Resolución CRC 7811 de 2025, una vez se detecta la presunta configuración de alguna de las causales de recuperación establecidas o el presunto uso indebido de un código corto, esta Comisión inicia una actuación administrativa reglamentada por el CPACA que incluye, oficio de apertura, requerimientos de información, expedición y notificación de una resolución, y modificación del recurso en el Sistema de Información y Gestión de Recursos de Identificación (SIGRI). Sin embargo, durante todo este proceso, el tráfico presuntamente fraudulento asociado al código corto continúa cursándose, lo que permite que los mensajes lleguen a los usuarios sin restricciones.

Es importante recordar que el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016 regula el procedimiento de recuperación de los recursos de identificación. Esta disposición fue modificada de manera expresa por el artículo 94 de la Resolución CRC 7811 de 2025 al incluir el Parágrafo 3°. Según esta disposición, en las actuaciones administrativas de recuperación de códigos cortos iniciadas por las causales señaladas en los numerales 6.4.3.2.2., 6.4.3.2.8. y 6.4.3.2.9. del artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, la CRC puede ordenar, en el acto de apertura de la actuación administrativa, la suspensión temporal del uso del recurso de identificación. Dicha suspensión se mantendrá durante el trámite administrativo y no podrá exceder un plazo máximo de seis (6) meses.

9.2.4.3.2 Alternativa 2: Suspensión preventiva del tráfico en cualquier etapa de la actuación administrativa y participación de terceros con interés directo

Esta alternativa propone incorporar en el régimen de administración la posibilidad de ordenar la suspensión temporal del tráfico cursado a través de un código corto en cualquier momento de la actuación administrativa de recuperación.

En concreto, deben considerarse las condiciones que motivaron el inicio de la actuación administrativa, así como, la posterior existencia de evidencia que demuestre que se reitera la presunta configuración de la causal de uso fraudulento, soportada en la información con la cual cuente la Comisión al momento de suspender de manera preventiva el tráfico durante cualquier etapa de la actuación administrativa.

En otras palabras, esta alternativa contempla la posibilidad de incluir en la regulación la prerrogativa de suspensión provisional que podrá ser ordenada no solo al inicio de las actuaciones de recuperación sino en cualquier etapa del trámite siempre y cuanto se trate de la recuperación de un código corto fundados en unas causales en particular.

Para finalizar, y producto de todos los comentarios recibidos por los agentes interesados, la Comisión considera relevante complementar la medida descrita en el sentido de modificar el trámite administrativo de recuperación de los recursos de identificación regulado en el artículo 6.1.1.8. de la Resolución CRC de 2016, no solo en relación con la facultad de la Comisión de decretar la suspensión del tráfico, sino también para efectos de introducir en el inicio del trámite una publicación del acto administrativo de inicio para efectos de promover y garantizar la participación de cualquier tercero interesado, en los términos de los artículos 37 y 38 del CPACA. Esto garantizaría, de manera efectiva, que cualquier interesado se vincule a los trámites administrativos de recuperación de recursos de identificación para los fines que correspondan, especialmente para aportar y solicitar pruebas. Lo anterior garantizará un mayor nivel de transparencia y, además, le permitirá a la Comisión contar con elementos de juicio adicionales para adoptar decisiones. La Comisión únicamente aceptará la participación de terceros que demuestren de manera cierta, clara y real la existencia de un interés directo en el resultado del trámite administrativo.

Criterio de simplificación que cumple: Posibilidad de optimización de la disposición regulatoria.

Justificación: Es posible mejorar la formulación y organización interna de ciertas proposiciones normativas relacionadas con la Administración de Recursos de Identificación para aclarar que los

terceros interesados tienen una oportunidad para participar en los trámites de recuperación de recursos de identificación y, además, que la facultad de la CRC para suspender provisionalmente el tráfico puede ser ordenado en cualquier estado de la actuación administrativa de recuperación, por unas causales particulares. Esto le permitirá a la CRC, sin cambiar el sentido y finalidad de la norma, contar con más pruebas o elementos de juicio para decidir, así como garantizar la efectividad del mencionado régimen en materia de lucha contra el fraude en servicios móviles relacionados con SMS.

Para materializar lo anterior, se modificará el numeral 6.1.1.8.1 del artículo 6.1.1.8. de la Resolución CRC 5050 de 2016 para precisar la forma en la que terceros interesados podrán participar en el marco de los trámites administrativos de recuperación de códigos cortos. Además, se modificará el parágrafo 3° del mismo artículo referenciado, para que la prerrogativa de la CRC de suspender el tráfico pueda ser decretada en cualquier momento del trámite administrativo.

Propuesta regulatoria:

Modificar las siguientes disposiciones:

«ARTÍCULO 6.1.1.8. RECUPERACIÓN DE LOS RECURSOS DE IDENTIFICACIÓN. Cuando el Administrador de los Recursos de Identificación, mediante los mecanismos de verificación de uso diseñados para tal fin, detecte la presunta configuración de alguna de las causales de recuperación establecidas o el presunto uso ineficiente de algún recurso de identificación asignado, adelantará el procedimiento de recuperación establecido en este artículo, teniendo en cuenta lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA) para las actuaciones administrativas.

6.1.1.8.1. El Administrador de los Recursos de Identificación remitirá un oficio de apertura de actuación administrativa de recuperación al asignatario donde justifique las razones por las cuales se ha identificado el presunto uso ineficiente del recurso, especificando expresamente las faltas a los criterios de uso eficiente o las causales de recuperación en las que está incurriendo, con el objeto de garantizar el derecho a la defensa y al debido proceso.

Este oficio de apertura de la actuación administrativa de recuperación será publicado por la CRC en un micrositio contenido en su página web al que tendrá acceso cualquier persona, con la finalidad de garantizar los escenarios contemplados en el artículo 38 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA).

La persona que acredite ante la CRC un interés directo e individual en la actuación administrativa tendrá el carácter de tercero interesado y podrá, dentro de los cinco (5) días hábiles posteriores a la publicación del oficio de apertura de la actuación administrativa de recuperación en la página web de la CRC, intervenir aportando las consideraciones y pruebas que pretendan hacer valer para que la CRC las tenga en cuenta al momento de decidir. La CRC resolverá de plano la solicitud del tercero, ya sea para reconocer su participación en la actuación o negarla, y contra esta decisión no procederá recurso alguno.

La CRC dará traslado al asignatario de los documentos y pruebas aportadas por los terceros mediante documento en el que también fijará un término para que los asignatarios se pronuncien sobre lo aportado.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

(…)

PARÁGRAFO 3o. En las actuaciones administrativas de recuperación de códigos cortos iniciadas por las causales señaladas en los numerales 6.4.3.2.2., 6.4.3.2.8. y 6.4.3.2.9. del artículo 6.4.3.2. de la presente resolución, la CRC podrá ordenar, en el acto de apertura de la actuación administrativa, o en cualquier estado del trámite administrativo, la suspensión temporal del uso del recurso de identificación. Dicha suspensión se mantendrá durante el trámite administrativo y no podrá exceder un plazo máximo de seis (6) meses. Para los recursos de identificación código corto A2P y SENDER ID, la suspensión temporal se regirá por los parágrafos 2 de los artículos 6.4.3.2 y 6.12.3.2 de la presente resolución, respectivamente.

(…)»

9.2.4.4 Temática 4: Condiciones asociadas a la vigencia y obligaciones de actualización de la asignación de recursos de identificación.

Situación identificada:	Los asignatarios de los recursos de identificación, en particular los asociados con los códigos cortos, no actualizan la información depositada en el RPCAI cuando se presentan novedades en términos de su existencia y representación, lo que dificulta la trazabilidad de los requerimientos por uso indebido de este recurso de identificación.
Causa relacionada:	Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso.
Alternativa 1: Statu quo.	Mantener el procedimiento de asignación de recursos de identificación establecido en artículo 6.1.1.5 de la Resolución CRC 5050 de 2016.
Alternativa 2: Vigencias y actualización de la asignación del código corto.	Adicionar condiciones al Régimen de recursos de Identificación asociadas a la vigencia de la asignación del código corto, así como la obligación de actualizar la información del asignatario del código corto.

9.2.4.4.1 Alternativa 1: Statu quo

Bajo esta alternativa se mantendrían las condiciones para la asignación de recursos de identificación por parte de la CRC, teniendo en cuenta un único registro obligatorio en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores (RPCAI) para los solicitantes y asignatarios de códigos cortos, de manera que solamente los agentes debidamente inscritos puedan solicitar a la CRC y hacer uso de códigos cortos.

Esta opción supondría la continuidad de una vigencia indefinida en la asignación de los recursos de identificación, lo que permitiría que, posterior a dicha asignación, el asignatario que no cumpla con las habilitaciones o requisitos necesarios para la prestación de servicios en Colombia mantenga la titularidad de los recursos asignados.

9.2.4.4.2 Alternativa 2: Vigencias y actualización de la asignación del código corto.

Producto de los comentarios analizados en este documento, la Comisión considera relevante adecuar las medidas planteadas en el sentido de:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Incluir una nueva causal de recuperación de la numeración de códigos cortos para SMS y USSD, en el evento en el que el asignatario se encuentre en la imposibilidad de continuar ejerciendo su objeto social, por ejemplo, cuando entra en estado de liquidación judicial o voluntaria.

- Modificar el numeral 6.4.3.1.3. del artículo 6.4.3.1. de la Resolución CRC 5050 de 2016, para que disponga que los códigos cortos implementados no deberán reportar ausencia de tráfico en periodos consecutivos iguales o superiores a seis (6) meses y no a doce (12) meses, ya que el plazo actualmente no es óptimo para efectos de la evaluación de la utilización eficiente del recurso de identificación correspondiente. Bajo ese mismo sentido, se modificaría la causal de recuperación establecida en el numeral 6.4.3.2.4. del artículo 6.4.3.2. en relación con el periodo referenciado.

Lo anterior se complementa con las nuevas obligaciones que ya fueron incorporadas en materia de actualización de la matricula mercantil y el RPCAI y que fueron expuestas en líneas precedentes.

Criterio de simplificación que cumple: Posibilidad de optimización de la disposición regulatoria.

Justificación: Es posible mejorar la formulación y organización interna de ciertas proposiciones normativas relacionadas con la Administración de Recursos de Identificación para aclarar que a aquellas sociedades que ya no puedan ejercer su objeto social, o que no reporten tráfico en un periodo razonable de seis (6) meses, se les recuperarán los respectivos códigos cortos. Esto, sin perjuicio de las normas sobre actualización de matrícula mercantil y del RPCAI, las cuales se adicionaron como obligaciones y, de manera consecuencial, como causales de recuperación del recurso de identificación. Todas estas reformulaciones apuntan a materializar la finalidad de las normas que integran el Régimen de Administración de Recursos de Identificación, para que en el ecosistema de mensajería SMS únicamente operen sociedades que tengan tráfico y operaciones reales en la práctica.

Propuesta regulatoria:

Modificar las siguientes disposiciones:

ARTÍCULO 6.4.3.1. CRITERIOS DE USO EFICIENTE. El Administrador de los Recursos de Identificación verificará el uso eficiente de la numeración de códigos cortos para SMS y USSD asignada, en observancia de los siguientes criterios:

6.4.3.1.1. Los asignatarios deberán dar pleno cumplimiento a las obligaciones generales definidas en el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la presente resolución.

6.4.3.1.2. Los códigos cortos asignados deben ser implementados en un término máximo de seis (6) meses contados a partir de la firmeza del acto administrativo de asignación.

6.4.3.1.3. Los códigos cortos implementados no deberán reportar ausencia de tráfico en periodos consecutivos iguales o superiores a seis (6) meses.

6.4.3.1.4. Los códigos cortos implementados no deberán reportar tráfico para un único usuario por un periodo superior a tres (3) meses.

(…)

ARTÍCULO 6.4.3.2. CAUSALES DE RECUPERACIÓN DE LA NUMERACIÓN DE CÓDIGOS CORTOS PARA SMS Y USSD. El Administrador de los Recursos de Identificación podrá recuperar total o parcialmente la numeración de códigos cortos para SMS y USSD asignada conforme el procedimiento de recuperación establecido en el artículo 6.1.1.8. de la presente resolución, cuando el asignatario incumpla con alguno de los criterios de uso eficiente establecidos en el artículo 6.4.3.1. de la presente resolución, o incurra en alguna de las siguientes causales de recuperación:

(…)

6.4.3.2.4. Cuando no se reporte tráfico asociado al código corto durante un periodo de seis (6) meses.

(…)

6.4.3.2.11. Cuando el asignatario se encuentra en la imposibilidad para continuar ejerciendo su objeto social, por ejemplo, pero sin limitarse a ello, cuando entra en estado de liquidación judicial o voluntaria».

(…)»

10. PARTICIPACIÓN DEL SECTOR

Atendiendo el procedimiento establecido en el artículo 2.2.13.3.2 del Decreto 1078 de 2015, se invita a todos los usuarios, proveedores de redes y servicios de telecomunicaciones, agentes del sector, y demás entidades interesadas, para que envíen observaciones o sugerencias al proyecto de resolución «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones», así como con respecto al presente documento soporte.

Esta propuesta estará sometida a consideración de los agentes interesados entre el 5 de junio de 2026 al y el 23 de junio de 2026, como fecha límite para la recepción de comentarios y observaciones. Los comentarios a la propuesta regulatoria serán recibidos a través del correo electrónico: medidasantifraude@crcom.gov.co, vía fax al (+57) 601 319 8301, o en las oficinas de la CRC ubicadas en la Calle 59A Bis No. 5 – 53 Piso 9, Edificio Link Siete Sesenta, de la ciudad de Bogotá D.C. A través de los anteriores medios podrá contactarse a las personas a quienes podrá solicitarse información sobre el proyecto.

11. BIBLIOGRAFÍA

1. Australia. Department of Infrastructure, Transport, Regional Development, Communications and the Arts. SMS Sender ID Register: Cost-Benefit Analysis [en línea]. Canberra: Australian Government, 2024 [consultado: 14 de mayo de 2026]. Disponible en: https://oia.pmc.gov.au/sites/default/files/posts/2024/12/Appendix%20A%20-%20SMS%20Sender%20ID%20Register%20Cost-Benefit%20Analysis.pdf
2. CHEUNG, H. Tourism in Kenya's national parks: a cost-benefit analysis. En: SURG Journal. Vol. 6, no. 1 (2012), p. 31-40. Disponible en: https://doi.org/10.21083/surg.v6i1.2019
3. CRC. Documento de alternativas regulatorias del proyecto «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles» [en línea]. Bogotá D.C.: CRC, s.f. Disponible

en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-alternativas-regulatorias-identificacion-medida-fraude-cibernetico-servicios-moviles.pdf
4. CRC. Documento de formulación del problema: identificación de medidas para mitigar el fraude cibernético en servicios móviles. Bogotá D.C.: CRC, s.f.
5. CRC. Documento soporte del proyecto regulatorio «Esquemas de remuneración mayorista de redes móviles» [en línea]. Bogotá D.C.: CRC, 2026. Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-9/Propuestas/documento-soporte-esquemas-remuneracion-mayorista-redes-moviles.pdf
6. CRC. Esquemas de Remuneración Mayorista de Redes Móviles [en línea]. Bogotá D.C.: CRC, 2026. Disponible en: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-41-7-9
7. CRC. Resolución 5050 de 2016: «Por la cual se compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones» [en línea]. Bogotá D.C.: CRC, 2016. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/resolucion_crc_5050_2016.htm
8. CRC. Resolución CRC 7684 de 2025 «Por la cual se adoptan medidas para la promoción de la competencia, se modifican algunas disposiciones de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones» [en línea]. Bogotá D.C.: CRC, 2025. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/resolucion_crc_7684_2025.htm
9. COMREG. Economic assessment of measures to address CLI spoofing and scam calls [en línea]. Irlanda: Commission for Communications Regulation, 2023 [consultado: 14 de mayo de 2026]. Disponible en: https://www.comreg.ie/media/2023/06/ComReg-2352a.pdf
10. CTIA. Messaging Principles and Best Practices. Washington D.C.: CTIA, 2025.
11. DEAN, Marco. Multi-criteria analysis. En: Advances in Transport Policy and Planning. Vol. 6 (2020), p. 165-224. Disponible en: https://www.sciencedirect.com/science/article/pii/S2543000920300147
12. DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT. Multi-criteria analysis: a manual [en línea]. Londres: Communities and Local Government, 2009. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191506/Multcrisis_analysis_a_manual.pdf
13. DEPARTMENT OF TELECOMMUNICATIONS (DoT). DOT and TRAI have taken widespread action for curbing Unsolicited Commercial Communication (UCC) [en línea]. Nueva Delhi: DoT, 2026. Disponible en: https://www.dot.gov.in/static/uploads/2026/02/2f35b2d58f60cbbeb8fe3447f609445c.pdf
14. DNP. Documentos CONPES de confianza y seguridad digital. Bogotá D.C.: DNP, s.f. Disponible en: https://dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx
15. DNP. Documento CONPES 3816 Mejora Normativa: Análisis de Impacto [en línea]. Bogotá D.C.: DNP, 2014. Disponible en: https://bit.ly/3SmXIu9
16. DNP. Guía Metodológica de Análisis de Impacto Normativo [en línea]. Bogotá D.C.: DNP, 2016. Disponible en: https://bit.ly/2RSQRII
17. DOLDÁN, Félix. Métodos de decisión basados en criterios cualitativos: una comparación entre los métodos AHP y REMBRANT. Universidad de La Coruña, 1999.
18. EUROPE ECONOMICS. Scam Calls and Texts in Ireland – Costs and Benefits of Interventions [en línea]. Reino Unido: Europe Economics, 2023. Disponible en: https://www.comreg.ie/media/2023/06/ComReg-2352a.pdf
19. Federal Communications Commission. Directrices para tráfico Non-Consumer (A2P). Washington D.C.: FCC, s.f.

20. ISMS.ONLINE. ISO 27002 Control 6.3: Information Security Awareness, Education and Training. Brighton: ISMS.online, s.f. Disponible en: https://www.isms.online/iso-27002/control-6-3-information-security-awareness-education-and-training/
21. INFOCOMM MEDIA DEVELOPMENT AUTHORITY (IMDA). Enhanced measures against scam SMS [en línea]. Singapur: IMDA, 2023. Disponible en: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/enhanced-measures-against-scam-sms
22. INFOCOMM MEDIA DEVELOPMENT AUTHORITY (IMDA). Full SMS Sender ID Registry Regime (Full SSIR Regime Guidelines). Singapur: IMDA, 2023.
23. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Ginebra: ISO, 2022. Disponible en: https://www.iso.org/standard/27001
24. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Ginebra: ISO, 2022. Disponible en: https://www.iso.org/standard/75652.html
25. ISHIZAKA, Alessio y NEMERY, Philippe. Multi-Criteria Decision Analysis. Methods and Software. Wiley, 2013.
26. MEYDIS. Mensajería RCS: qué es, cómo funciona y ventajas vs SMS [en línea]. España: Meydis, 2026. Disponible en: https://www.meydis.com
27. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MinTIC). La Estrategia Nacional de Seguridad Digital llega para enfrentar las crecientes amenazas cibernéticas. Bogotá D.C.: MinTIC, 2025. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403023:La-Estrategia-Nacional-de-Seguridad-Digital-llega-para-enfrentar-las-crecientes-amenazas-ciberneticas
28. MIRAMIRKANI, Niloofar; STAROV, Oleksii; et al. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators [en línea]. En: NDSS Symposium, 2020. Disponible en: https://www.ndss-symposium.org/wp-content/uploads/2020/02/24286.pdf
29. MOBILE ECOSYSTEM FORUM (MEF). SMS SenderID Protection Registry [en línea]. Londres: MEF, s.f. Disponible en: https://mobileecosystemforum.com/sms-senderid-protection-registry/
30. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Building an Information Technology Security Awareness and Training Program. Special Publication 800-50 Revision 1. Gaithersburg: NIST, 2003. Disponible en: https://csrc.nist.gov/pubs/sp/800/50/r1/final
31. PHELPS, C. E.; MUSHLIN, A. I. On the (Near) Equivalence of Cost-Effectiveness and Cost-Benefit Analyses. En: International Journal of Technology Assessment in Health Care. Vol. 7 (1991), p. 12-21.
32. SAATY, Thomas L. Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors: the analytic hierarchy/network process. En: RACSAM. Vol. 102, no. 2 (2008), p. 251-318. Disponible en: https://link.springer.com/article/10.1007/BF03191825
33. SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Remisión de información sobre la afectación económica de los usuarios por fraude cibernético (smishing y vishing). Radicado No. 2025166778-000-000. Bogotá D.C.: Superfinanciera, 24 septiembre 2025.
34. TELECOM REGULATORY AUTHORITY OF INDIA (TRAI). Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018 [en línea]. Nueva Delhi: TRAI, 2018. Disponible en: https://www.trai.gov.in/sites/default/files/2024-09/RegulationUcc19072018.pdf
35. YASUI, S. A Critical Review of the Traditional Methodology of Cost-Benefit Analysis and a Proposed Alternative. En: Human and Ecological Risk Assessment. Vol. 11, no. 2 (2005), p. 411-432.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

12. FUENTES DE INFORMACIÓN UTILIZADAS

1. COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC). *Requerimiento de información No. 2026-002. Información relacionada con fraude cibernético por medio de servicios de telecomunicaciones móviles*. Bogotá D.C.: CRC, 2026.

2. COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC). *Radicado de salida 202600188. Asunto: Requerimiento de información No. 2026-010. Información relacionada con la implementación de las medidas para mitigar el fraude cibernético por medio de servicios de telecomunicaciones móviles*. Bogotá D.C.: CRC, 2026.

3. COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC). *Registro de Proveedores de Contenidos y Aplicaciones e Integradores (RPCAI)*. Bogotá D.C.: CRC, 2026.

4. SUPERINTENDENCIA FINANCIERA DE COLOMBIA. *Remisión de información sobre la afectación económica de los usuarios por fraude cibernético (smishing y vishing). Radicado No. 2025166778-000-000*. Bogotá D.C.: Superfinanciera, 24 septiembre 2025.

13. ANEXOS

Anexo 1. Soporte del análisis de decisión multicriterio de la temática: Falta de identificación clara del remitente en SMS A2P.

Tabla 11. Matriz de importancias relativas de los subcriterios de la temática: Falta de identificación clara del remitente en SMS A2P.

Criterio	Prevención de suplantación	Trazabilidad del originador	Confianza en el canal SMS	Cobertura sobre actores del ecosistema	Costos de cumplimiento para los agentes	Costos de supervisión	Mitigación de la migración de canales	Rapidez de despliegue	Riesgo de implementación	Necesidad de coordinación
Prevención de suplantación	1,00	2,00	2,00	3,00	4,00	5,00	3,00	4,00	2,00	4,00
Trazabilidad del originador	0,50	1,00	1,00	2,00	3,00	4,00	4,00	3,00	2,00	4,00
Confianza en el canal SMS	0,50	1,00	1,00	3,00	3,00	4,00	1,00	4,00	3,00	3,00
Cobertura sobre actores del ecosistema	0,33	0,50	0,33	1,00	4,00	5,00	2,00	3,00	0,50	1,00
Costos de cumplimiento para los agentes	0,25	0,33	0,33	0,25	1,00	3,00	0,33	0,33	0,25	0,50
Costos de supervisión	0,20	0,25	0,25	0,20	0,33	1,00	0,25	0,25	0,25	0,33
Mitigación de la migración de canales	0,33	0,25	1,00	0,50	3,00	4,00	1,00	3,00	0,50	0,50
Rapidez de despliegue	0,25	0,33	0,25	0,33	3,00	4,00	0,33	1,00	0,33	0,33
Riesgo de implementación	0,50	0,50	0,33	2,00	4,00	4,00	2,00	3,00	1,00	0,50

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Criterio	Prevención de suplantación	Trazabilidad del originador	Confianza en el canal SMS	Cobertura sobre actores del ecosistema	Costos de cumplimiento para los agentes	Costos de supervisión	Mitigación de la migración de canales	Rapidez de despliegue	Riesgo de implementación	Necesidad de coordinación
Necesidad de coordinación	0,25	0,25	0,33	1,00	2,00	3,00	2,00	3,00	2,00	1,00

Fuente: Elaboración CRC.

Tabla 12. Matriz normalizada de subcriterios, Ponderadores y prueba de consistencia de la temática: Falta de identificación clara del remitente en SMS A2P.

Criterio	Prevención de suplantación	Trazabilidad del originador	Confianza en el canal SMS	Cobertura sobre actores del ecosistema	Costos de cumplimiento para los agentes	Costos de supervisión	Mitigación de la migración de canales	Rapidez de despliegue	Riesgo de implementación	Necesidad de coordinación	Ponderador
Prevención de suplantación	24,29%	31,17%	29,27%	22,58%	14,63%	13,51%	18,85%	16,27%	16,90%	26,37%	21,4%
Trazabilidad del originador	12,15%	15,58%	14,63%	15,06%	10,98%	10,81%	25,13%	12,20%	16,90%	26,37%	16,0%
Confianza en el canal SMS	12,15%	15,58%	14,63%	22,58%	10,98%	10,81%	6,28%	16,27%	25,35%	19,78%	15,4%
Cobertura sobre actores del ecosistema	8,10%	7,79%	4,88%	7,53%	14,63%	13,51%	12,57%	12,20%	4,23%	6,59%	9,2%
Costos de cumplimiento para los agentes	6,07%	5,19%	4,88%	1,88%	3,66%	8,11%	2,09%	1,36%	2,11%	3,30%	3,9%
Costos de supervisión	4,86%	3,90%	3,66%	1,51%	1,22%	2,70%	1,57%	1,02%	2,11%	2,20%	2,5%
Mitigación de la migración de canales	8,10%	3,90%	14,63%	3,76%	10,98%	10,81%	6,28%	12,20%	4,23%	3,30%	7,8%
Rapidez de despliegue	6,07%	5,19%	3,66%	2,51%	10,98%	10,81%	2,09%	4,07%	2,82%	2,20%	5,0%
Riesgo de implementación	12,15%	7,79%	4,88%	15,06%	14,63%	10,81%	12,57%	12,20%	8,45%	3,30%	10,2%
Necesidad de coordinación	6,07%	3,90%	4,88%	7,53%	7,32%	8,11%	12,57%	12,20%	16,90%	6,59%	8,6%
Total	24,29%	31,17%	29,27%	22,58%	14,63%	13,51%	18,85%	16,27%	16,90%	26,37%	21,4%
										Prueba de Consistencia	7,5%
										Consistente	

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 13. Desempeño de las alternativas regulatorias frente a los criterios establecidos de la temática: Falta de identificación clara del remitente en SMS A2P.

Criterio	Ponderador	Statu Quo	Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)	Asignación y uso de código alfanumérico solo para tráfico transaccional
Prevención de suplantación	21,4%	10,0%	69,5%	20,5%
Trazabilidad del originador	16,0%	9,6%	70,2%	20,2%
Confianza en el canal SMS	15,4%	8,9%	71,6%	19,6%
Cobertura sobre actores del ecosistema	9,2%	11,9%	56,7%	31,4%
Costos de cumplimiento para los agentes	3,9%	67,3%	11,7%	21,1%
Costos de supervisión	2,5%	46,3%	21,9%	31,8%
Mitigación de la migración de canales	7,8%	50,0%	20,4%	29,6%
Rapidez de despliegue	5,0%	65,0%	11,3%	23,7%
Riesgo de implementación	10,2%	60,7%	14,0%	25,4%
Necesidad de coordinación	8,6%	66,7%	12,2%	21,1%
Total	**100%**	**29,0%**	**48,0%**	**23,0%**

Fuente: Elaboración CRC.

Anexo 2. Soporte del análisis de decisión multicriterio de la temática: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

Tabla 14. Matriz de importancias relativas de los subcriterios de la temática: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

Criterio	Capacidad de Reacción	Medidas Preventivas	Mercado Secundario de SMS	Actualización dinámica	Experiencia de usuario	Rapidez de despliegue	Riesgo de implementación	Necesidad de coordinación
Capacidad de Reacción	1,00	0,33	3,00	1,00	1,00	4,00	1,00	3,00
Medidas Preventivas	3,00	1,00	4,00	3,00	1,00	4,00	1,00	1,00
Mercado Secundario de SMS	0,33	0,25	1,00	0,50	0,50	3,00	2,00	2,00
Actualización dinámica	1,00	0,33	2,00	1,00	0,50	3,00	2,00	1,00
Experiencia de usuario	1,00	1,00	2,00	2,00	1,00	3,00	3,00	2,00
Rapidez de despliegue	0,25	0,25	0,33	0,33	0,33	1,00	0,50	0,50
Riesgo de implementación	1,00	1,00	0,50	0,50	0,33	2,00	1,00	3,00

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Criterio	Capacidad de Reacción	Medidas Preventivas	Mercado Secundario de SMS	Actualización dinámica	Experiencia de usuario	Rapidez de despliegue	Riesgo de implementación	Necesidad de coordinación
Necesidad de coordinación	0,33	1,00	0,50	1,00	0,50	2,00	0,33	1,00

Fuente: Elaboración CRC.

Tabla 15. Matriz normalizada de subcriterios, Ponderadores y prueba de consistencia de la temática: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

Criterio	Capacidad de Reacción	Medidas Preventivas	Mercado Secundario de SMS	Actualización dinámica	Experiencia de usuario	Rapidez de despliegue	Riesgo de implementación	Necesidad de coordinación	Ponderador
Capacidad de Reacción	11,95%	5,93%	21,77%	10,22%	17,80%	17,82%	8,86%	21,51%	13,9%
Medidas Preventivas	35,86%	17,80%	29,02%	30,66%	17,80%	17,82%	8,86%	7,17%	18,8%
Mercado Secundario de SMS	3,98%	4,45%	7,26%	5,11%	8,90%	13,36%	17,73%	14,34%	9,8%
Actualización dinámica	11,95%	5,93%	14,51%	10,22%	8,90%	13,36%	17,73%	7,17%	11,3%
Experiencia de usuario	11,95%	17,80%	14,51%	20,44%	17,80%	13,36%	26,59%	14,34%	16,0%
Rapidez de despliegue	2,99%	4,45%	2,42%	3,41%	5,93%	4,45%	4,43%	3,58%	5,5%
Riesgo de implementación	11,95%	17,80%	3,63%	5,11%	5,93%	8,91%	8,86%	21,51%	10,7%
Necesidad de coordinación	3,98%	17,80%	3,63%	10,22%	8,90%	8,91%	2,95%	7,17%	8,7%
Total	2,99%	4,45%	1,81%	2,56%	4,45%	1,11%	2,22%	1,79%	3,1%
								Prueba de Consistencia	7,8%
								Consistente	

Fuente: Elaboración CRC.

Tabla 16. Desempeño de las alternativas regulatorias frente a los criterios establecidos de la temática: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

Criterio	Ponderador	Statu Quo	Control de patrones de tráfico atípicos	Límite de SMS P2P por usuario
Capacidad de Reacción	13,9%	18,9%	58,2%	22,8%
Medidas Preventivas	18,8%	12,5%	42,7%	44,8%
Mercado Secundario de SMS	9,8%	36,8%	29,3%	33,9%

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Criterio	Ponderador	Statu Quo	Control de patrones de tráfico atípicos	Límite de SMS P2P por usuario
Actualización dinámica	11,3%	16,8%	58,8%	24,4%
Experiencia de usuario	16,0%	52,2%	31,2%	16,6%
Rapidez de despliegue	5,5%	56,2%	16,8%	26,9%
Riesgo de implementación	10,7%	46,8%	15,5%	37,6%
Necesidad de coordinación	8,7%	40,1%	26,0%	33,9%
Total	**100%**	**51,2%**	**18,2%**	**30,6%**

Fuente: Elaboración CRC.

Anexo 3. Soporte del análisis de decisión multicriterio de la temática: Falta de una instancia de coordinación para la articulación y el intercambio de alertas

Tabla 17. Matriz de importancias relativas de los subcriterios de la temática: Falta de una instancia de coordinación para la articulación y el intercambio de alertas

Criterio	Detección temprana de campañas fraudulentas	Integración de actores	Protección de información sensible	Riesgo de implementación	Costos de desarrollo e implementación	Costos de operación y mantenimiento	Costos de supervisión
Detección temprana de campañas fraudulentas	1,00	1,00	2,00	3,00	3,00	3,00	3,00
Integración de actores	1,00	1,00	2,00	3,00	3,00	3,00	3,00
Protección de información sensible	0,50	0,50	1,00	2,00	4,00	4,00	4,00
Riesgo de implementación	0,33	0,33	0,50	1,00	3,00	3,00	3,00
Costos de desarrollo e implementación	0,33	0,33	0,25	0,33	1,00	4,00	5,00
Costos de operación y mantenimiento	0,33	0,33	0,25	0,33	0,25	1,00	2,00
Costos de supervisión	0,33	0,33	0,25	0,33	0,20	0,50	1,00

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 18. Matriz normalizada de subcriterios, Ponderadores y prueba de consistencia de la temática: Falta de una instancia de coordinación para la articulación y el intercambio de alertas

Criterio	Detección temprana de campañas fraudulentas	Integración de actores	Protección de información sensible	Riesgo de implementación	Costos de desarrollo e implementación	Costos de operación y mantenimiento	Costos de supervisión	Ponderador
Detección temprana de campañas fraudulentas	26,09%	26,09%	32,00%	30,00%	20,76%	16,22%	14,29%	23,6%
Integración de actores	26,09%	26,09%	32,00%	30,00%	20,76%	16,22%	14,29%	23,6%
Protección de información sensible	13,04%	13,04%	16,00%	20,00%	27,68%	21,62%	19,05%	18,6%
Riesgo de implementación	8,70%	8,70%	8,00%	10,00%	20,76%	16,22%	14,29%	12,4%
Costos de desarrollo e implementación	8,70%	8,70%	4,00%	3,33%	6,92%	21,62%	23,81%	11,0%
Costos de operación y mantenimiento	8,70%	8,70%	4,00%	3,33%	1,73%	5,41%	9,52%	5,9%
Costos de supervisión	8,70%	8,70%	4,00%	3,33%	1,38%	2,70%	4,76%	4,8%
Total	26,09%	26,09%	32,00%	30,00%	20,76%	16,22%	14,29%	23,6%
							Prueba de Consistencia	9,6%
							Consistente	

Fuente: Elaboración CRC.

Tabla 19. Desempeño de las alternativas regulatorias frente a los criterios establecidos de la temática: Falta de una instancia de coordinación para la articulación y el intercambio de alertas

Criterio	Ponderador	Statu Quo	Creación de una plataforma nacional de intercambio de alertas	Creación de un mecanismo formal de articulación y coordinación
Detección temprana de campañas fraudulentas	23,6%	12,2%	49,9%	37,9%
Integración de actores	23,6%	11,3%	44,7%	44,0%
Protección de información sensible	18,6%	31,0%	30,8%	38,2%
Riesgo de implementación	12,4%	63,5%	10,5%	26,0%
Costos de desarrollo e implementación	11,0%	65,2%	11,7%	23,0%
Costos de operación y mantenimiento	5,9%	63,9%	11,1%	25,1%

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Criterio	Ponderador	Statu Quo	Creación de una plataforma nacional de intercambio de alertas	Creación de un mecanismo formal de articulación y coordinación
Costos de supervisión	4,8%	63,2%	12,0%	24,8%
Total	**100%**	**33,2%**	**31,9%**	**34,9%**

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Anexo 4. Soporte del análisis de decisión multicriterio de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas

Tabla 20. Matriz de importancias relativas de los subcriterios de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas.

Criterio	Señalización del tráfico	Precisión del sistema	Promoción de reglas homogéneas	Prevención del fraude	Experiencia de usuario	Confianza en el canal voz	Mitigación de la migración de tráfico	Estigmatización en el uso del servicio de voz	Compatibilidad tecnológica	Fatiga por alertas	Rapidez de despliegue	Riesgo de implementación	Actualización dinámica	Costos de adecuación tecnológica	Costos operativos y administrativos	Costos de supervisión
Señalización del tráfico	1,00	1,00	2,00	0,33	0,33	0,50	3,00	3,00	0,50	1,00	2,00	3,00	1,00	3,00	3,00	4,00
Precisión del sistema	1,00	1,00	3,00	1,00	1,00	1,00	3,00	2,00	0,50	2,00	4,00	3,00	2,00	3,00	3,00	4,00
Promoción de reglas homogéneas	0,50	0,33	1,00	0,50	0,50	0,50	3,00	2,00	0,50	1,00	3,00	3,00	1,00	3,00	3,00	4,00
Prevención del fraude	3,00	1,00	2,00	1,00	1,00	1,00	3,00	2,00	1,00	2,00	4,00	2,00	3,00	3,00	3,00	4,00
Experiencia de usuario	3,00	1,00	2,00	1,00	1,00	1,00	3,00	3,00	1,00	1,00	3,00	3,00	2,00	3,00	3,00	4,00
Confianza en el canal voz	2,00	1,00	2,00	1,00	1,00	1,00	3,00	3,00	1,00	1,00	3,00	3,00	2,00	3,00	3,00	4,00
Mitigación de la migración de tráfico	0,33	0,33	0,33	0,33	0,33	0,33	1,00	1,00	0,33	0,50	1,00	0,50	1,00	3,00	3,00	4,00
Estigmatización en el uso del servicio de voz	0,33	0,50	0,50	0,50	0,33	0,33	1,00	1,00	0,50	1,00	3,00	3,00	1,00	3,00	3,00	4,00
Compatibilidad tecnológica	2,00	2,00	2,00	1,00	1,00	1,00	3,00	2,00	1,00	1,00	3,00	2,00	2,00	3,00	3,00	4,00
Fatiga por alertas	1,00	0,50	1,00	0,50	1,00	1,00	2,00	1,00	1,00	1,00	3,00	1,00	1,00	3,00	3,00	4,00
Rapidez de despliegue	0,50	0,25	0,33	0,25	0,33	0,33	1,00	0,33	0,33	0,33	1,00	0,50	0,50	2,00	2,00	3,00
Riesgo de implementación	0,33	0,33	0,33	0,50	0,33	0,33	2,00	0,33	0,50	1,00	2,00	1,00	0,50	3,00	3,00	4,00
Actualización dinámica	1,00	0,50	1,00	0,33	0,50	0,50	1,00	1,00	0,50	1,00	2,00	2,00	1,00	3,00	3,00	4,00
Costos de adecuación tecnológica	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,50	0,33	0,33	1,00	1,00	1,00
Costos operativos y administrativos	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,33	0,50	0,33	0,33	1,00	1,00	1,00
Costos de supervisión	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,33	0,25	0,25	1,00	1,00	1,00

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 21. Matriz normalizada de subcriterios, Ponderadores y prueba de consistencia de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas.

Criterio	Señalización del tráfico	Precisión del sistema	Promoción de reglas homogéneas	Prevención del fraude	Experiencia de usuario	Confianza en el canal voz	Mitigación de la migración de tráfico	Estigmatización en el uso del servicio de voz	Compatibilidad tecnológica	Fatiga por alertas	Rapidez de despliegue	Riesgo de implementación	Actualización dinámica	Costos de adecuación tecnológica	Costos operativos y administrativos	Costos de supervisión	Ponderador
Señalización del tráfico	5,91%	9,38%	10,86%	3,64%	3,48%	5,13%	10,03%	13,28%	5,22%	6,78%	5,66%	10,75%	5,29%	7,32%	7,32%	7,41%	7,3%
Precisión del sistema	5,91%	9,38%	16,29%	10,91%	10,43%	10,26%	10,03%	8,86%	5,22%	13,56%	11,32%	10,75%	10,57%	7,32%	7,32%	7,41%	9,7%
Promoción de reglas homogéneas	2,96%	3,13%	5,43%	5,45%	5,22%	5,13%	10,03%	8,86%	5,22%	6,78%	8,49%	10,75%	5,29%	7,32%	7,32%	7,41%	6,5%
Prevención del fraude	17,73%	9,38%	10,86%	10,91%	10,43%	10,26%	10,03%	8,86%	10,43%	13,56%	11,32%	7,16%	15,86%	7,32%	7,32%	7,41%	10,6%
Experiencia de usuario	17,73%	9,38%	10,86%	10,91%	10,43%	10,26%	10,03%	13,28%	10,43%	6,78%	8,49%	10,75%	10,57%	7,32%	7,32%	7,41%	10,1%
Confianza en el canal voz	11,82%	9,38%	10,86%	10,91%	10,43%	10,26%	10,03%	13,28%	10,43%	6,78%	8,49%	10,75%	10,57%	7,32%	7,32%	7,41%	9,8%
Mitigación de la migración de tráfico	1,97%	3,13%	1,81%	3,64%	3,48%	3,42%	3,34%	4,43%	3,48%	3,39%	2,83%	1,79%	5,29%	7,32%	7,32%	7,41%	4,0%
Estigmatización en el uso del servicio de voz	1,97%	4,69%	2,71%	5,45%	3,48%	3,42%	3,34%	4,43%	5,22%	6,78%	8,49%	10,75%	5,29%	7,32%	7,32%	7,41%	5,5%
Compatibilidad tecnológica	11,82%	18,75%	10,86%	10,91%	10,43%	10,26%	10,03%	8,86%	10,43%	6,78%	8,49%	7,16%	10,57%	7,32%	7,32%	7,41%	9,8%
Fatiga por alertas	5,91%	4,69%	5,43%	5,45%	10,43%	10,26%	6,69%	4,43%	10,43%	6,78%	8,49%	3,58%	5,29%	7,32%	7,32%	7,41%	6,9%
Rapidez de despliegue	2,96%	2,34%	1,81%	2,73%	3,48%	3,42%	3,34%	1,48%	3,48%	2,26%	2,83%	1,79%	2,64%	4,88%	4,88%	5,56%	3,1%
Riesgo de implementación	1,97%	3,13%	1,81%	5,45%	3,48%	3,42%	6,69%	1,48%	5,22%	6,78%	5,66%	3,58%	2,64%	7,32%	7,32%	7,41%	4,6%
Actualización dinámica	5,91%	4,69%	5,43%	3,64%	5,22%	5,13%	3,34%	4,43%	5,22%	6,78%	5,66%	7,16%	5,29%	7,32%	7,32%	7,41%	5,6%
Costos de adecuación tecnológica	1,97%	3,13%	1,81%	3,64%	3,48%	3,42%	1,11%	1,48%	3,48%	2,26%	1,42%	1,19%	1,76%	2,44%	2,44%	1,85%	2,3%
Costos operativos y administrativos	1,97%	3,13%	1,81%	3,64%	3,48%	3,42%	1,11%	1,48%	3,48%	2,26%	1,42%	1,19%	1,76%	2,44%	2,44%	1,85%	2,3%
Costos de supervisión	1,48%	2,34%	1,36%	2,73%	2,61%	2,56%	0,84%	1,11%	2,61%	1,69%	0,94%	0,90%	1,32%	2,44%	2,44%	1,85%	1,8%
																Prueba de consistencia	9,8%

COMISIÓN DE REGULACIÓN DE COMUNICACIONES

Criterio	Señalización del tráfico	Precisión del sistema	Promoción de reglas homogéneas	Prevención del fraude	Experiencia de usuario	Confianza en el canal voz	Mitigación de la migración de tráfico	Estigmatización en el uso del servicio de voz	Compatibilidad tecnológica	Fatiga por alertas	Rapidez de despliegue	Riesgo de implementación	Actualización dinámica	Costos de adecuación tecnológica	Costos operativos y administrativos	Costos de supervisión	Ponderador
																Consistente	

Fuente: Elaboración CRC.

Tabla 22. Desempeño de las alternativas regulatorias frente a los criterios establecidos de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas.

Criterio	Ponderador	Statu Quo	Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial	Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias
Señalización del tráfico	7,3%	10,0%	63,7%	26,2%
Precisión del sistema	9,7%	14,2%	55,6%	30,2%
Promoción de reglas homogéneas	6,5%	10,8%	52,7%	36,4%
Prevención del fraude	10,6%	17,1%	57,2%	25,7%
Experiencia de usuario	10,1%	12,0%	57,7%	30,4%
Confianza en el canal voz	9,8%	9,3%	64,5%	26,1%
Mitigación de la migración de tráfico	4,0%	41,2%	26,5%	32,3%
Estigmatización en el uso del servicio de voz	5,5%	51,7%	23,6%	24,7%
Compatibilidad tecnológica	9,8%	40,7%	22,2%	37,1%
Fatiga por alertas	6,9%	44,1%	18,9%	37,0%
Rapidez de despliegue	3,1%	61,1%	16,6%	22,2%
Riesgo de implementación	4,6%	64,3%	11,5%	24,2%
Actualización dinámica	5,6%	24,1%	47,2%	28,7%
Costos de adecuación tecnológica	2,3%	65,6%	13,0%	21,4%
Costos operativos y administrativos	2,3%	62,3%	14,4%	23,3%
Costos de supervisión	1,8%	38,6%	32,9%	27,3%
Total	**100%**	**28,1%**	**42,5%**	**29,4%**

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Anexo 5. Soporte del análisis de decisión multicriterio de la temática: Falta de estandarización en la aplicación de listas de no originación (DNO)

Tabla 23. Matriz de importancias relativas de los subcriterios de la temática: Falta de estandarización en la aplicación de listas de no originación (DNO).

Criterio	Medidas preventivas	Riesgo de afectación a tráfico legítimo	Uniformidad de criterios	Actualización dinámica	Rapidez de despliegue	Gobernanza de listas	Riesgo de implementación	Costos de adecuación técnica (CAPEX)	Costos operativos (OPEX)
Medidas preventivas	1,00	3,00	2,00	1,00	3,00	2,00	1,00	4,00	4,00
Riesgo de afectación a tráfico legítimo	0,33	1,00	1,00	0,50	1,00	1,00	2,00	4,00	4,00
Uniformidad de criterios	0,50	1,00	1,00	1,00	3,00	1,00	2,00	4,00	4,00
Actualización dinámica	1,00	2,00	1,00	1,00	3,00	0,50	3,00	4,00	4,00
Rapidez de despliegue	0,33	1,00	0,33	0,33	1,00	0,33	0,50	4,00	4,00
Gobernanza de listas	0,50	1,00	1,00	2,00	3,00	1,00	3,00	4,00	4,00
Riesgo de implementación	1,00	0,50	0,50	0,33	2,00	0,33	1,00	4,00	4,00
Costos de adecuación técnica (CAPEX)	0,25	0,25	0,25	0,25	0,25	0,25	0,25	1,00	1,00
Costos operativos (OPEX)	0,25	0,25	0,25	0,25	0,25	0,25	0,25	1,00	1,00

Fuente: Elaboración CRC.

Tabla 24. Matriz normalizada de subcriterios, Ponderadores y prueba de consistencia de la temática: Falta de estandarización en la aplicación de listas de no originación (DNO).

Criterio	Medidas preventivas	Riesgo de afectación a tráfico legítimo	Uniformidad de criterios	Actualización dinámica	Rapidez de despliegue	Gobernanza de listas	Riesgo de implementación	Costos de adecuación técnica (CAPEX)	Costos operativos (OPEX)	Ponderador
Medidas preventivas	18,63%	29,41%	26,55%	14,56%	17,96%	29,13%	7,58%	13,11%	13,11%	18,3%
Riesgo de afectación a tráfico legítimo	6,21%	9,80%	13,27%	7,28%	5,99%	14,56%	15,15%	13,11%	13,11%	11,1%
Uniformidad de criterios	9,32%	9,80%	13,27%	14,56%	17,96%	14,56%	15,15%	13,11%	13,11%	13,3%
Actualización dinámica	18,63%	19,61%	13,27%	14,56%	17,96%	7,28%	22,73%	13,11%	13,11%	15,3%
Rapidez de despliegue	6,21%	9,80%	4,42%	4,85%	5,99%	4,85%	3,79%	13,11%	13,11%	7,9%
Gobernanza de listas	9,32%	9,80%	13,27%	29,13%	17,96%	14,56%	22,73%	13,11%	13,11%	15,6%

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Criterio	Medidas preventivas	Riesgo de afectación a tráfico legítimo	Uniformidad de criterios	Actualización dinámica	Rapidez de despliegue	Gobernanza de listas	Riesgo de implementación	Costos de adecuación técnica (CAPEX)	Costos operativos (OPEX)	Ponderador
Riesgo de implementación	18,63%	4,90%	6,64%	4,85%	11,98%	4,85%	7,58%	13,11%	13,11%	9,8%
Costos de adecuación técnica (CAPEX)	4,66%	2,45%	3,32%	3,64%	1,50%	3,64%	1,89%	3,28%	3,28%	3,3%
Costos operativos (OPEX)	4,66%	2,45%	3,32%	3,64%	1,50%	3,64%	1,89%	3,28%	3,28%	3,3%
Total	3,73%	1,96%	2,65%	2,91%	1,20%	2,91%	1,52%	1,64%	1,64%	2,3%
									Prueba de Consistencia	4,8%
									Consistente	

Fuente: Elaboración CRC.

Tabla 25. Desempeño de las alternativas regulatorias frente a los criterios establecidos de la temática: Falta de estandarización en la aplicación de listas de no originación (DNO).

Criterio	Ponderador	Statu Quo	Estándar Mínimo Obligatorio de DNO con «listas propias» por PRST	DNO definida dinámicamente por los PRST de manera colaborativa
Medidas preventivas	18,3%	10,5%	52,6%	36,9%
Riesgo de afectación a tráfico legítimo	11,1%	44,2%	27,2%	28,6%
Uniformidad de criterios	13,3%	12,0%	57,2%	30,8%
Actualización dinámica	15,3%	18,0%	29,9%	52,1%
Rapidez de despliegue	7,9%	64,6%	18,2%	17,1%
Gobernanza de listas	15,6%	12,6%	60,1%	27,3%
Riesgo de implementación	9,8%	66,3%	16,9%	16,8%
Costos de adecuación técnica (CAPEX)	3,3%	59,3%	19,5%	21,2%
Costos operativos (OPEX)	3,3%	59,9%	22,4%	17,7%
Total	**100%**	**29,9%**	**39,2%**	**31,0%**

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Anexo 6. Soporte del análisis de decisión multicriterio de la temática: Acciones educativas y de interacción con la ciudadanía que aumenten el conocimiento de los usuarios

Tabla 26. Matriz de importancias relativas de los subcriterios de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas.

Criterio	Empoderamiento de usuarios	Cambio de comportamiento	Fatiga Informativa	Cobertura poblacional	Frecuencia e Intensidad	Coordinación entre actores	Riesgo de implementación	Sostenibilidad en el tiempo	Articulación con políticas de seguridad	Costos de diseño	Costos de coordinación institucional	Costo de implementación y seguimiento
Empoderamiento de usuarios	1,00	1,00	2,00	2,00	1,00	3,00	3,00	1,00	3,00	4,00	4,00	5,00
Cambio de comportamiento	1,00	1,00	3,00	4,00	1,00	3,00	3,00	1,00	2,00	4,00	4,00	5,00
Fatiga Informativa	0,50	0,33	1,00	2,00	1,00	0,50	3,00	0,50	0,50	4,00	4,00	5,00
Cobertura poblacional	0,50	0,25	0,50	1,00	1,00	1,00	2,00	0,50	1,00	4,00	4,00	5,00
Frecuencia e Intensidad	1,00	1,00	1,00	1,00	1,00	0,50	2,00	0,50	0,50	4,00	4,00	5,00
Coordinación entre actores	0,33	0,33	2,00	1,00	2,00	1,00	3,00	0,50	1,00	4,00	4,00	5,00
Riesgo de implementación	0,33	0,33	0,33	0,50	0,50	0,33	1,00	0,50	0,50	4,00	4,00	5,00
Sostenibilidad en el tiempo	1,00	1,00	2,00	2,00	2,00	2,00	2,00	1,00	2,00	4,00	4,00	5,00
Articulación con políticas de seguridad	0,33	0,50	2,00	1,00	2,00	1,00	2,00	0,50	1,00	4,00	4,00	5,00
Costos de diseño	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	1,00	1,00	2,00
Costos de coordinación institucional	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	1,00	1,00	2,00
Costo de implementación y seguimiento	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,50	0,50	1,00

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 27. Matriz normalizada de subcriterios, Ponderadores y prueba de consistencia de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas.

Criterio	Empoderamiento de usuarios	Cambio de comportamiento	Fatiga Informativa	Cobertura poblacional	Frecuencia e Intensidad	Coordinación entre actores	Riesgo de implementación	Sostenibilidad en el tiempo	Articulación con políticas de seguridad	Costos de diseño	Costos de coordinación institucional	Costo de implementación y seguimiento	Ponderador
Empoderamiento de usuarios	14,93%	15,50%	13,76%	13,16%	8,20%	23,02%	13,82%	14,93%	24,59%	10,39%	10,39%	14,4%	14,93%
Cambio de comportamiento	14,93%	15,50%	20,64%	26,32%	8,20%	23,02%	13,82%	14,93%	16,39%	10,39%	10,39%	15,4%	14,93%
Fatiga Informativa	7,46%	5,17%	6,88%	13,16%	8,20%	3,84%	13,82%	7,46%	4,10%	10,39%	10,39%	8,4%	7,46%
Cobertura poblacional	7,46%	3,88%	3,44%	6,58%	8,20%	7,67%	9,22%	7,46%	8,20%	10,39%	10,39%	7,7%	7,46%
Frecuencia e Intensidad	14,93%	15,50%	6,88%	6,58%	8,20%	3,84%	9,22%	7,46%	4,10%	10,39%	10,39%	9,0%	14,93%
Coordinación entre actores	4,98%	5,17%	13,76%	6,58%	16,39%	7,67%	13,82%	7,46%	8,20%	10,39%	10,39%	9,6%	4,98%
Riesgo de implementación	4,98%	5,17%	2,29%	3,29%	4,10%	2,56%	4,61%	7,46%	4,10%	10,39%	10,39%	5,8%	4,98%
Sostenibilidad en el tiempo	14,93%	15,50%	13,76%	13,16%	16,39%	15,35%	9,22%	14,93%	16,39%	10,39%	10,39%	13,4%	14,93%
Articulación con políticas de seguridad	4,98%	7,75%	13,76%	6,58%	16,39%	7,67%	9,22%	7,46%	8,20%	10,39%	10,39%	9,4%	4,98%
Costos de diseño	3,73%	3,88%	1,72%	1,64%	2,05%	1,92%	1,15%	3,73%	2,05%	2,60%	2,60%	2,6%	3,73%
Costos de coordinación institucional	3,73%	3,88%	1,72%	1,64%	2,05%	1,92%	1,15%	3,73%	2,05%	2,60%	2,60%	2,6%	3,73%
Costo de implementación y seguimiento	2,99%	3,10%	1,38%	1,32%	1,64%	1,53%	0,92%	2,99%	1,64%	1,30%	1,30%	1,8%	2,99%
												Prueba de consistencia	4,7%
												Consistente	

Fuente: Elaboración CRC.

Tabla 28. Desempeño de las alternativas regulatorias frente a los criterios establecidos de la temática: Falta de lineamientos específicos para proporcionar información al usuario sobre las llamadas recibidas.

Criterio	Ponderador	Statu Quo	Acciones de pedagogía, transparencia e interacción	Sistema de trazabilidad de PQR relacionadas con fraude a través de mensajes de texto o llamadas de voz
Empoderamiento de usuarios	14,4%	14,2%	59,0%	26,8%
Cambio de comportamiento	15,4%	11,2%	60,8%	27,9%
Fatiga Informativa	8,4%	45,3%	19,9%	34,8%
Cobertura poblacional	7,7%	13,2%	54,3%	32,6%
Frecuencia e Intensidad	9,0%	11,1%	63,2%	25,6%
Coordinación entre actores	9,6%	10,7%	57,1%	32,2%
Riesgo de implementación	5,8%	40,6%	34,6%	24,7%
Sostenibilidad en el tiempo	13,4%	39,6%	34,2%	26,2%
Articulación con políticas de seguridad	9,4%	14,7%	45,3%	40,0%
Costos de diseño	2,6%	58,5%	17,9%	23,6%
Costos de coordinación institucional	2,6%	60,1%	15,0%	24,9%
Costo de implementación y seguimiento	1,8%	60,3%	18,2%	21,5%
Total	**100%**	**23,8%**	**46,9%**	**29,3%**

Fuente: Elaboración CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Anexo 7. Enfoque metodológico para la construcción de los costos de las alternativas regulatorias

La estimación de los costos asociados a las alternativas regulatorias evaluadas en el marco del proyecto «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles» se desarrolló mediante un modelo de costeo regulatorio modular, construido específicamente para evaluar los requerimientos técnicos, operativos, administrativos y de supervisión derivados de la implementación de mecanismos orientados a fortalecer la prevención y mitigación del fraude mediante servicios SMS y voz móvil.

El enfoque metodológico fue aplicado particularmente en la evaluación de las temáticas «Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude» y «Limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)», dado que dichas problemáticas involucran alternativas regulatorias con impactos económicos significativos asociados al despliegue de infraestructura tecnológica, adecuaciones de red, plataformas de monitoreo, mecanismos de autenticación, capacidades de supervisión y operación continua de los sistemas de control.

En términos generales, el modelo de costeo fue construido bajo un enfoque bottom-up, mediante la identificación detallada de los componentes tecnológicos, operativos y regulatorios requeridos para implementar cada alternativa. A partir de estos componentes se estimaron inversiones iniciales, costos recurrentes de operación y costos de supervisión regulatoria, permitiendo construir una evaluación consistente y comparable entre las distintas opciones regulatorias.

a. Variables y parámetros generales del modelo

La construcción de los costos se fundamentó en un conjunto transversal de variables técnicas, operativas y macroeconómicas que alimentan los distintos módulos del modelo. Entre los principales parámetros considerados se incluyeron:

Tabla 29. Parámetros generales utilizados en el modelo de costos

Variable	Valor de referencia	Unidad
TRM promedio	4.052,86	COP/USD
Tasa de descuento (WACC)	11,57%	Porcentaje
Horizonte de evaluación	3	Años
Ciclo de reinversión CAPEX	6	Años
Número estimado de PRST	4	Operadores
Líneas móviles activas	95.796.445	Líneas
Número estimado de PCA e integradores	185	Empresas
Salario ingeniero senior	15.000.000	COP/mes
Salario analista especializado	8.000.000	COP/mes
Eventos potenciales de fraude	500.000	Eventos/año

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

Así mismo, se adoptó un horizonte de evaluación de tres (3) años, considerando que las alternativas regulatorias evaluadas presentan ciclos relativamente cortos de evolución tecnológica y adaptación operativa. Adicionalmente, el modelo contempló ciclos de reinversión en CAPEX cada seis (6) años, particularmente relevantes para plataformas core de autenticación, monitoreo y procesamiento de tráfico.

b. Clasificación de costos

El modelo diferenció los costos conforme a su naturaleza económica y funcional, agrupándolos principalmente en tres categorías:

Tabla 30. Clasificación general de costos regulatorios

Tipo de costo	Descripción	Ejemplos
CAPEX	Inversiones iniciales de infraestructura y adecuación tecnológica	Plataformas, servidores, licencias, SBC, IMS
OPEX	Costos recurrentes de operación y mantenimiento	Monitoreo, soporte, procesamiento analítico
Supervisión	Costos regulatorios de seguimiento y control	Auditorías, monitoreo CRC, validación de reportes

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

- Costos de inversión o adecuación técnica (CAPEX)

Corresponden a las inversiones iniciales requeridas para implementar infraestructura tecnológica, plataformas de monitoreo, sistemas de autenticación, servidores, licenciamiento, integraciones de red, adecuaciones sobre SMS-C, SBC, IMS y demás componentes tecnológicos necesarios para la operación de las medidas regulatorias.

- Costos operativos recurrentes (OPEX)

Incluyen los costos asociados a la operación continua, mantenimiento, actualización y gestión de las medidas regulatorias implementadas.

- Costos de supervisión regulatoria

Corresponden a los recursos requeridos por la CRC para verificar el cumplimiento de las obligaciones regulatorias, auditar los mecanismos implementados y realizar seguimiento a la operación de las medidas.

c. Construcción modular de costos por alternativa

Cada alternativa regulatoria fue modelada mediante módulos funcionales independientes, permitiendo identificar de manera diferenciada los componentes tecnológicos y operativos requeridos en cada caso.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 31. Componentes considerados para alternativas de SMS A2P

Componente	Validación centralizada	DLT distribuido	Sender ID / numeración
Plataforma de autenticación	✓	✓	✓
Infraestructura blockchain	✗	✓	✗
Registro de originadores	✓	✓	✓
Integración con SMS-C	✓	✓	✓
Monitoreo de campañas	✓	✓	Parcial
Gestión de reputación	✓	✓	✗
Validación de contenido y enlaces	✓	✓	✗

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

En las alternativas basadas en DLT se incorporaron adicionalmente costos asociados a nodos blockchain, infraestructura distribuida, mecanismos de consenso y mayor complejidad de interoperabilidad.

Tabla 32. Componentes considerados para alternativas de voz móvil

Componente	STIR/SHAKEN/RCD	STIR/SHAKEN/RCD	STIR/SHAKEN/RCD	STIR/SHAKEN/RCD
TI-VS	✓	✗	✗	✗
Infraestructura PKI	✓	✗	✗	✗
Motores de monitoreo	✓	✓	✓	Parcial
Etiquetado de llamadas	✓	✓	✗	✗
Listas DNO	Parcial	Parcial	✓	✗
Plataforma de alertas	✓	✓	✗	✓
Integración SBC/IMS	✓	Parcial	✗	✗

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

En el caso de STIR/SHAKEN/RCD se identificaron costos significativamente superiores derivados de la necesidad de migración hacia arquitecturas full IP, integración SIP extremo a extremo y despliegue de mecanismos de certificación digital e interoperabilidad internacional.

d. Consideración de sinergias y economías de escala

El modelo incorporó un enfoque de sinergias regulatorias y economías de escala, particularmente relevante en aquellas alternativas con componentes tecnológicos compartidos entre distintas temáticas.

Tabla 33. Principales sinergias consideradas en el modelo

Componente compartido	Alternativas beneficiadas
SOC y SIEM	SMS y voz
Motores de monitoreo	Etiquetado, DNO, STIR/SHAKEN
Infraestructura cloud	Todas
Plataformas de reportería	Todas
Herramientas analíticas	SMS y voz
Sistemas de alertamiento	Coordinación y monitoreo
SBC/IMS	STIR/SHAKEN y etiquetado

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

Lo anterior permitió evitar doble contabilización de inversiones y construir escenarios más consistentes de costos agregados, especialmente en la evaluación transversal de la alternativa STIR/SHAKEN/RCD frente al paquete de medidas regulatorias seleccionadas mediante análisis multicriterio.

e. Fuentes de información utilizadas

La construcción de los costos se fundamentó en múltiples fuentes de información técnica, operativa y regulatoria.

Tabla 34. Fuentes utilizadas para la estimación de costos

Fuente	Tipo de información
Requerimientos de información a PRST	Costos operativos y de red
Integradores y proveedores tecnológicos	Referencias de infraestructura
Estándares internacionales	Requerimientos técnicos
Experiencias internacionales	Despliegues regulatorios
Bases de datos CRC	Tráfico y usuarios
Estudios regulatorios previos	Parámetros financieros y operativos

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

Adicionalmente, para las variables macroeconómicas y financieras se utilizaron parámetros regulatorios previamente definidos por la CRC, incluyendo el WACC estimado en el proyecto regulatorio «Esquemas de remuneración mayorista de redes móviles».

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

f. Limitaciones y sensibilidad del modelo

Finalmente, es importante señalar que los resultados del modelo de costeo se encuentran sujetos a distintos factores de sensibilidad, asociados principalmente a la evolución tecnológica y al grado de madurez de las redes.

Tabla 35. Principales variables de sensibilidad del modelo

Variable de sensibilidad	Posible impacto
Migración a redes full IP	Reduce costos de STIR/SHAKEN
Evolución del fraude	Incrementa costos operativos
Interoperabilidad internacional	Afecta autenticación de llamadas
Costos de licenciamiento	Modifica CAPEX
Evolución de IA y analítica	Reduce costos de monitoreo
Necesidad de reinversión tecnológica	Incrementa costos de largo plazo

Fuente: Elaboración CRC con base en el modelo de costeo regulatorio.

Por esta razón, los costos estimados deben interpretarse como aproximaciones regulatorias razonables para efectos comparativos y de evaluación de alternativas, más que como valores exactos o definitivos de implementación.