COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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

Documento de Alternativas Regulatorias

Diseño Regulatorio

Noviembre de 2025

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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

1. INTRODUCCIÓN

El fraude cibernético mediante servicios móviles constituye uno de los principales desafíos para la protección de los usuarios, la confianza en las telecomunicaciones y la seguridad digital del país. En los últimos años, prácticas como el smishing, el spoofing, el uso indebido de códigos cortos, la suplantación de identidad y la manipulación de la numeración E.164[1] en los identificadores de llamada (CLI) han evolucionado rápidamente, generando afectaciones económicas, sociales y reputacionales tanto para los usuarios como para los operadores, las entidades financieras, las empresas y el ecosistema digital en general.

Frente a esta situación, la Comisión de Regulación de Comunicaciones (CRC) ha adelantado un proceso participativo en desarrollo del proyecto regulatorio *Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles*[2], proceso que ha permitido, tal y como se presenta en este documento, la recepción y análisis de comentarios de múltiples actores del sector respecto del problema inicialmente definido, así como la estructuración de alternativas regulatorias orientadas a mitigar este fenómeno. El presente documento recoge de manera sistemática los resultados de este ejercicio participativo.

En una primera parte se presenta el problema identificado, consistente en la ausencia de herramientas regulatorias suficientes para prevenir y mitigar el contacto fraudulento a los usuarios a través de servicios tradicionales de voz y mensajes de texto. Posteriormente, se consolidan los comentarios recibidos de asociaciones gremiales, operadores, entidades financieras, empresas de tecnología, la academia y organismos de control, destacando coincidencias, divergencias y propuestas específicas; los cuales permitieron ajustar el árbol del problema.

Sobre esta base se establecen los objetivos del proyecto, que buscan diseñar una estrategia regulatoria integral para la prevención y mitigación del fraude cibernético a través de servicios móviles. Para alcanzarlos, se formulan alternativas regulatorias agrupadas en cuatro grandes temáticas:

i) Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)
ii) Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de voz

[1] Numeración utilizada para identificar líneas de telefonía fija y móvil.
[2] Disponible en: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-41-7-1

iii) Temáticas enfocadas en la educación de la ciudadanía
iv) Temáticas objeto de revisión asociadas al régimen de administración de los recursos de identificación bajo el enfoque de simplificación normativa

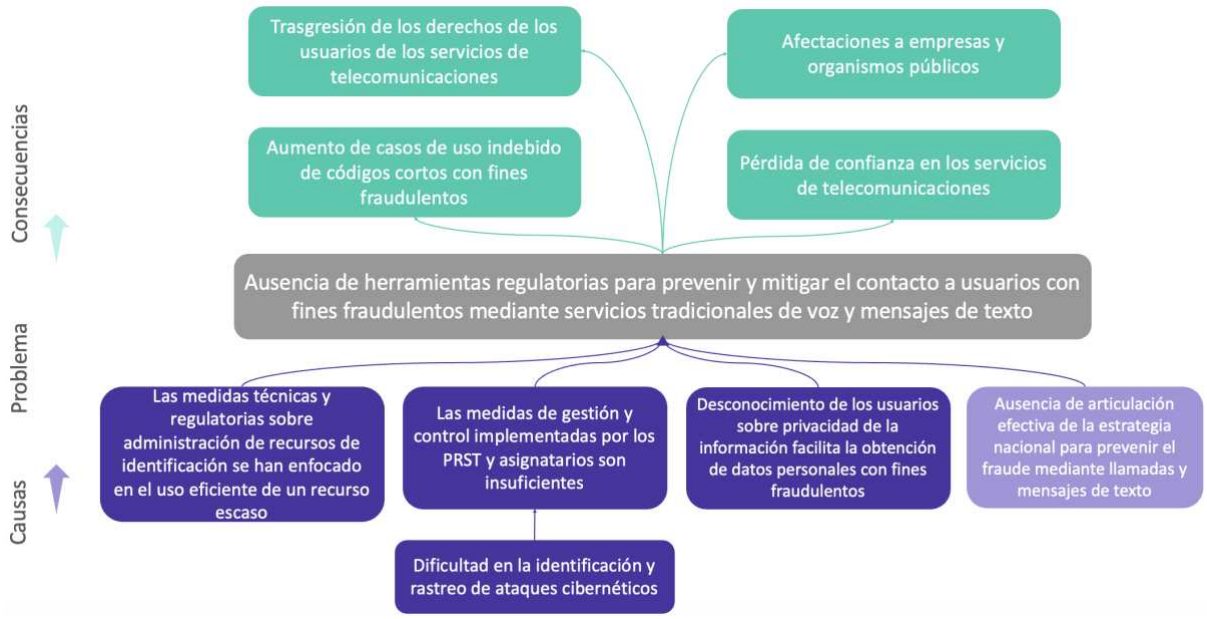
Finalmente, este documento plantea una consulta dirigida a los agentes interesados, con el fin de recoger sus apreciaciones sobre las alternativas propuestas, así como recomendaciones adicionales que permitan fortalecer la pertinencia, viabilidad y eficacia de las medidas a implementar.

De esta manera, se busca consolidar un marco regulatorio que, sin desconocer la dinámica cambiante de las amenazas digitales, defina herramientas efectivas, proporcionales y coordinadas para proteger a los usuarios, fortalecer la confianza en los servicios de telecomunicaciones y aportar a la construcción de una estrategia nacional integral contra el fraude cibernético.

2. 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*[3]. 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»**. El siguiente esquema resume las causas identificadas y las consecuencias que se derivan de la presencia del referido problema.

[3] 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



Fuente: Elaboración CRC

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

3. COMENTARIOS RECIBIDOS A LA FORMULACIÓN DEL PROBLEMA

En este capítulo se recopilan los comentarios recibidos por la CRC en relación con el documento de formulación del problema del proyecto regulatorio *Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles*. Además, se presentan las respuestas de la CRC a cada comentario, fundamentadas en un análisis técnico que da respuesta a las inquietudes planteadas por los interesados.

En este contexto, dentro del término establecido por la Comisión se recibieron comentarios y observaciones respecto de la formulación del problema identificado por la CRC, por parte de los siguientes interesados:

Tabla 1. Relación de agentes del sector que presentaron comentarios a la formulación del problema

Alianza Latinoamericana de Telecomunicaciones	ALT
Asociación Nacional de Empresarios de Colombia	ANDI
Asociación Nacional de Empresas de Servicios Públicos y Comunicaciones	ANDESCO
Asociación Bancaria y de Entidades Financieras de Colombia	ASOBANCARIA
Asociación de la Industria Móvil de Colombia	ASOMÓVIL
Aval Valor Compartido	AVAL
Colombia Móvil S.A. ESP	TIGO
Colombia Telecomunicaciones S.A. ESP BIC	TELEFÓNICA
Comunicación Celular Comcel S.A.	COMCEL
COLCERT – Ministerio de Tecnologías de la Información y las Comunicaciones	COLCERT
Cristóbal Fuentes	CRISTÓBAL FUENTES
Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.	ETB
Fondo para el financiamiento del sector agropecuario	FINAGRO
GSMA Latin America	GSMA
Hablame Colombia S.A. E.S.P.	HABLAME
Inalambria Internacional SAS	INALAMBRIA
MDK Digital GmbH	MDK
Plintron Colombia SAS	PLINTRON
Superintendencia de Industria y Comercio	SIC

Universidad Externado	UNIVERSIDAD EXTERNADO
Virgin Mobile Colombia S.A.S.	VIRGIN

Fuente: Elaboración CRC

Con posterioridad al término establecido se recibieron comentarios por parte de Partners Telecom Colombia S.A.S. y la Superintendencia Financiera de Colombia, los cuales, si bien no serán objeto de una respuesta puntual en el presente documento, fueron revisados como parte de los análisis que adelantó la Comisión para la estructuración de las alternativas regulatorias aquí propuestas.

Considerando lo expuesto anteriormente, en esta sección la Comisión se referirá a los comentarios presentados por los interesados que expresan desacuerdo total o parcial con lo planteado en el árbol de problemas elaborado por la CRC. Para ello, los comentarios serán resumidos y organizados según las temáticas coincidentes referentes al problema identificado, sus causas y consecuencias, sobre las cuales la CRC emitirá su pronunciamiento correspondiente. Lo anterior se indica sin limitar la posibilidad de que los interesados puedan consultar los textos originales de cada documento, los cuales están disponibles en el sitio web oficial de esta Comisión[4].

3.1. Comentarios generales

ALT

Indica que, la CRC debe asumir el liderazgo en la articulación de una estrategia nacional integral para la prevención y mitigación del contacto fraudulento a través de voz, mensajes de texto y otros medios, la cual debe estar alineada con las políticas de ciberseguridad nacional y enfocarse en tres ejes fundamentales: protección normativa, coordinación institucional y concientización ciudadana.

Considera que, para lo anterior, es esencial establecer un marco regulatorio flexible y adaptativo que pueda responder a las nuevas formas de fraude, promover la creación de canales de denuncia interoperables y eficaces, e incentivar la inversión en tecnologías de detección y bloqueo de comunicaciones maliciosas. Asimismo, sugiere fomentar la cooperación público-privada para intercambiar información crítica, facilitar la implementación de buenas prácticas internacionales y promover mecanismos de retroalimentación que mejoren continuamente las políticas públicas. De igual manera, es clave impulsar una narrativa de corresponsabilidad donde usuarios, operadores, entidades gubernamentales y organizaciones civiles trabajen juntos en la defensa del entorno digital.

Afirma que la construcción de esta estrategia nacional permitirá no solo reducir la incidencia del fraude, sino también fortalecer la confianza en los servicios de telecomunicaciones y proteger los derechos digitales de los ciudadanos colombianos.

[4] Los comentarios recibidos pueden ser consultados en el micrositio del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles» que se encuentra en el enlace: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-41-7-1

ANDESCO

Señala que es importante tener en cuenta las siguientes consideraciones:

-No se impone una consecuencia directa y contundente sobre la relación de acceso entre el infractor y los operadores de red.
-La reincidencia no tiene consecuencias claras. El regulador propone recuperar códigos cortos por mal uso, pero no vincula directamente esta reincidencia con consecuencias contractuales, esto puede generar incentivos perversos, pues el costo de la reincidencia puede ser menor al beneficio económico obtenido por facilitar fraude.
-Mientras persista la posibilidad de seguir operando tras múltiples recuperaciones de numeración, no hay un incentivo para el cumplimiento de la regulación.
-La reincidencia sistemática en el uso indebido de códigos cortos demuestra una fallida gestión interna de seguridad por parte del PCA o IT.
-Las prácticas fraudulentas no solo afectan a usuarios, sino que también debilitan la integridad del ecosistema de telecomunicaciones, al erosionar la confianza en los canales tradicionales como el SMS y la voz.
-La repetida intervención del regulador para recuperar numeración demuestra un patrón, no una falla aislada.

ASOMÓVIL

Propone a la CRC adoptar medidas normativas especificas en el marco normativo que cierren brechas utilizadas por delincuentes y eleven los estándares de seguridad, tales como:

-Suspensión de contratos por reincidencia: facultar a los operadores para terminar la relación contractual con PCA o integradores que incurran repetidamente en fraudes, estableciendo sanciones ejemplares.
-Auditorías periódicas a integradores tecnológicos: realizar o exigir evaluaciones regulares para verificar la aplicación de filtros de seguridad, actualización frente a nuevas modalidades y cumplimiento de buenas prácticas.
-Incluir a los generadores de contenido en la cadena antifraude: imponer obligaciones a quienes crean y dirigen campañas de SMS o llamadas maliciosas, integrándolos en los mecanismos de identificación, reporte y sanción.
-Obligaciones a Carrier internacionales: exigir que el tráfico hacia Colombia esté plenamente identificado y corresponda a su país de origen, sin alteraciones ni enmascaramientos, y prohibir que se cursen llamadas o mensajes internacionales como si fueran locales.

COMCEL

Manifiesta que la CRC desconoce que tiene herramientas para mitigar la mayor parte del fraude al que hoy se ven enfrentados, en el que la fuente de fraude proviene de los PCA o IT y envían estos mensajes con contenido fraudulento al usuario final, sin ningún tipo de control o mitigación.

Aclara que, si se finalizan las relaciones o contratos de acceso entre PCA y/o IT y PRST al constatar reincidencia, la conducta sistemática fraudulenta y la recuperación de códigos cortos por indebido uso de la numeración al enviar mensajes con contenido fraudulento, de manera ágil y expedita sin demoras innecesarias, los usuarios no recibirían este tipo de mensajes.

Manifiesta que se ha identificado un patrón de suplantación de identidad a través de llamadas de voz, caracterizado por un alto volumen de llamadas internacionales que son terminadas en usuarios nacionales con numeración nacional (enmascaramiento de la numeración), con el objetivo de engañar a los usuarios y lograr que respondan dichas llamadas. A través de esta modalidad se realizan innumerables fraudes a los usuarios con el presunto fin de robar su información personal, falsearla y realizar actos delictivos.

Señala que es necesario que el regulador expida una regulación orientada a controlar este tipo de fraude. Por lo tanto, solicita que el regulador permita a los PRSTM el bloqueo de las llamadas internacionales que utilicen números locales y utilizar la numeración asignada para las llamadas de LDI.

ETB

Reconoce la relevancia de abordar el fraude cibernético como una amenaza creciente para la confianza digital y la protección del usuario. Sin embargo, observa que el enfoque planteado concentra su análisis desde la perspectiva de los PRST, omitiendo actores clave que tienen un rol determinante en la génesis y proliferación del fraude, lo que incrementa la asimetría regulatoria entre los PRST y estos actores.

Señala que los PRST operan bajo una alta carga regulatoria y una estricta supervisión, pero omite a los actores clave como los PCA, plataformas OTT y *carriers* internacionales, entre otros, quienes operan sin cargas regulatorias y sin control por parte de MinTIC, situación que limita desde ya la eficacia de las medidas que surjan de las posibles alternativas de intervención del análisis de impacto normativo (AIN) del proyecto.

Sugiere que la Comisión tenga en cuenta que la experiencia internacional demuestra que las estrategias más exitosas en la lucha contra el fraude cibernético son aquellas que adoptan enfoques integrales, abordando todos los eslabones de la cadena de valor y estableciendo responsabilidades compartidas proporcionales al nivel de participación de cada actor en el ecosistema digital.

FINAGRO

Señala que el documento de formulación del problema se enfoca principalmente en los operadores de telecomunicaciones, pero debería también considerar a las empresas que usan estos servicios para comunicarse con sus clientes.

GSMA

Indica que la industria móvil ha demostrado un compromiso permanente con la seguridad de sus usuarios, y que los operadores móviles invierten constantemente en herramientas de detección de fraude, filtrado y bloqueo de tráfico malicioso, además de establecer firewalls para SMS y voz; y también, actúan con celeridad ante comportamientos sospechosos, comparten inteligencia con otros sectores y capacitan de forma continua a su personal, al tiempo que educan al consumidor para que pueda identificar y reportar actividades fraudulentas.

Manifiesta que, los principios claves que rigen la combinación de técnicas por parte de los operadores móviles para anticiparse al fraude son: especificidad y adaptabilidad de las estrategias, en lugar de soluciones universales; flexibilidad por sobre mandatos rígidos que corren el riesgo de volverse obsoletos e ineficaces; y visión de futuro mediante enfoques pragmáticos y colaborativos. Expuesto lo anterior recomienda el desarrollo de un marco flexible, preparado para el futuro y pragmático para abordar el fraude, lo cual considera garantizará mayor eficacia continua de las medidas antifraude, protección para los usuarios y el sector, así como espacio para la innovación y la adaptación a medida que evolucionan este tipo de amenazas.

Señala que el enfoque debe ser colaborativo e intersectorial, involucrando a todos los actores de la cadena de valor, con el acompañamiento del regulador. Comparte plenamente la visión de la CRC de que se requiere un enfoque holístico y multilateral. Resalta la importancia de que sea abordado el análisis de todos los servicios asociados a las comunicaciones móviles, pues la lucha contra el fraude exige reconocer la responsabilidad y el margen de acción de cada actor dentro de la cadena de valor.

Considera indispensable avanzar hacia reglas que distribuyan de forma más equitativa las obligaciones y medidas de prevención entre los distintos participantes, de manera proporcional a su exposición y capacidad de intervención.

TIGO

Solicita que este proyecto no se limite a los servicios de llamadas de voz tradicional y mensajes cortos de texto (SMS), sino que también incorpore dentro del análisis el servicio de internet móvil, el cual forma parte del mismo mercado relevante.

Resalta que la CRC debe generar el fortalecimiento de la colaboración interinstitucional entre SIC, Fiscalía, Ministerio TIC y Operadores para lograr que las denuncias que se presenten lleguen a sanciones efectivas en contra de PCA y sus integradores tecnológicos quienes, advierte, en algunos casos desarrollan sistemáticamente estas actividades fraudulentas.

Manifiesta que los PRSTM actúan como canal de comunicación de los mensajes generados por terceros, y por disposición legal no tienen la posibilidad de inspeccionar ni controlar el contenido de dichos mensajes, en cumplimiento del principio de inviolabilidad de las comunicaciones. Por lo cual sugiere que la CRC enfoque sus esfuerzos en el fortalecimiento de los mecanismos de control relacionados con la asignación y el uso de códigos cortos por parte de los PCA.

Respuesta CRC:

Frente a los comentarios planteados por **ALIANZA LATINOAMERICANA DE TELECOMUNICACIONES**, **GSMA** y **TIGO**, en los cuales exponen la necesidad de la creación de una estrategia nacional integral para la prevención y mitigación del fraude, la CRC comparte esta visión, por lo cual ha determinado como uno de los objetivos que se pretenden cumplir con este proyecto regulatorio «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».

Ahora bien, en atención a los comentarios expuestos por **ANDESCO**, **ASOMÓVIL, COMCEL, ETB, FINAGRO, GSMA** y **TIGO**, en los cuales se plantea la necesidad de establecer y fortalecer obligaciones para algunos agentes en materia de prevención y mitigación de fraude; desarrollar un marco flexible, que garantice mayor eficacia continua de las medidas antifraude, protección para los usuarios y el sector, así como espacio para la innovación y la adaptación a medida que evolucionan este tipo de amenazas; y considerar distintas modalidades por medio de las cuales se ejecuta la comisión de los fraudes cibernéticos utilizando llamadas de voz y mensajes de texto, esta Comisión coincide en términos generales con estas preocupaciones.

Teniendo en cuenta lo anterior, la CRC en el marco de sus competencias y con ocasión del desarrollo del presente proyecto regulatorio pretende a su vez 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; evaluar la implementación de herramientas regulatorias que mitiguen el contacto a usuarios con fines fraudulentos, teniendo en cuenta su viabilidad técnica y económica y; determinar la necesidad de implementar acciones educativas que aumenten el conocimiento de los usuarios en la prevención contra el fraude cibernético.

Es así como a través de estas líneas de acción la CRC adelanta el presente proyecto regulatorio con el objetivo de diseñar una estrategia para la prevención y mitigación del contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto.

Finalmente, frente al comentario de **TIGO** relacionado con la incorporación del servicio de internet móvil, es importante recordar que el alcance del presente proyecto regulatorio se limita a los recursos de identificación bajo administración de la CRC. Ahora bien, tal y como se presentará en este documento, esta Comisión propone alternativas orientadas a abordar las problemáticas identificadas y

fortalecer el marco regulatorio aplicable, las cuales permitan limitar el direccionamiento de los usuarios a sitios web fraudulentos, aplicaciones no verificadas o contenidos que faciliten la suplantación de identidad.

3.2 Comentarios sobre el problema planteado

ANDI

Señala que la CRC formula adecuadamente el problema, pero no identifica todos los actores ni elementos del fraude cibernético para comprender la magnitud del fenómeno y los actores involucrados, por lo que señala que los elementos omitidos en el diagnóstico son los siguientes:

El análisis se centra en operadores y PCA/IT formalmente registrados ante la CRC, pero muchos fraudes provienen de actores que no cumplen obligaciones regulatorias.

De otra parte, señala que el fraude por llamadas y SMS (*smishing*, *vishing*) afecta gravemente a usuarios, operadores y al sector financiero, generando riesgos reputacionales y operativos.

Indica que, los usuarios carecen de herramientas para verificar la identidad real de remitentes, lo que facilita la suplantación mediante numeración falsa, SMS con identificadores alterados y llamadas automatizadas que imitan entidades legítimas.

Afirma que, la falta de medidas regulatorias integrales para sancionar el uso indebido de numeración (códigos cortos, E.164) limita la capacidad de respuesta de operadores y del sector financiero.

Propone que se faculte la terminación de contratos entre PRST y PCA/IT en casos de reincidencia, y agilizar el proceso de recuperación de numeración. Señala que, aunque los servicios de voz y SMS decrecen en tráfico, siguen siendo puntos críticos de entrada al fraude, por lo que no deben subestimarse.

ANDESCO

Indica que el problema planteado por la CRC no parte del usuario como centro del perjuicio. En virtud de lo anterior, sugiere reformular el problema con el fin de hacer visible que el fraude es una externalidad del modelo actual de acceso a la red y que, al no interrumpirlo, perpetúa la exposición del usuario a un entorno inseguro, así: «Persistencia de canales habilitados para la comisión de fraudes a usuarios mediante servicios móviles, debido a vacíos regulatorios y a la falta de consecuencias efectivas frente a agentes reincidentes y/o frente a cualquier actor o agente que origine esta práctica fraudulenta.»

ASOBANCARIA

Indica que la formulación del problema se centra en los agentes formalmente registrados ante la CRC, (p. ej. Sistema de Información y Gestión de Recursos de Identificación (SIGRI) o Registro de Proveedores de Contenidos y Aplicaciones e Integradores (RPCAI)), dejando de lado los ataques que se originan desde fuentes no reguladas. La ausencia de herramientas regulatorias para controlar el uso de recursos de identificación ha limitado la capacidad de respuesta del sector financiero.

Por tanto, recomienda incluir la suplantación de identidad de entidades financieras como una de las manifestaciones más críticas del problema, dada su alta frecuencia e impacto económico. Además, los usuarios no están familiarizados con las diferencias de los recursos de identificación, ni la veracidad o legitimidad de estos. En la práctica, no existe para los consumidores una forma clara y segura de verificar si una llamada o mensaje recibido proviene de su entidad financiera o de un actor fraudulento.

Por ello, recomienda que el documento reconozca que existe un crecimiento sostenido del fenómeno, reafirmando la necesidad de definir una nueva aproximación regulatoria de cara al problema, que resulte ágil y fácil de expedir, pero que no subestime las tecnologías por su antigüedad o decrecimiento en volumen de tráfico, sino que reconozca su papel como puntos de entrada al fraude.

ASOMÓVIL

Destaca que en el árbol del problema y el análisis regulatorio presentado por la CRC se centran en servicios tradicionales de voz y mensajería SMS, al ser estos recursos de identificación administrados por la Comisión, sin embargo, señala que el servicio de acceso a internet móvil no ha sido incorporado en la caracterización del problema, pese a ser parte esencial del ecosistema de las telecomunicaciones; expone que si bien los fraudes suelen iniciarse con una llamada o un SMS se concretan o amplifican mediante el internet móvil.

En suma, detalla que un SMS que contiene un enlace malicioso, el usuario al hacer clic es dirigido mediante su conexión de datos móviles a un sitio web fraudulento donde puede entregar sus credenciales o información sensible. Concluye que, hay modalidades de engaño que usan aplicaciones de mensajería de tipo OTT (WhatsApp, Telegram) o correos electrónicos, los cuales operan sobre la red móvil, por lo tanto, sugiere que el análisis regulatorio considere al internet móvil dentro del entorno del problema de forma transversal.

AVAL

Considera que el problema definido por esta Comisión abarca de manera integral el fraude cibernético en servicios de voz y SMS, al reconocer la falta de herramientas regulatorias, identificar las causas técnicas y operativas, y considerar consecuencias económicas, sociales y reputacionales, incluyendo la perspectiva de los actores involucrados. Sugiere complementar con un enfoque de fraudes emergentes (p. ej., IAG para suplantación voz/mensajes) y protección de grupos vulnerables (p. ej., adultos mayores y menores de edad). Además, indica que las causas presentadas son pertinentes y explican la facilidad con la que los actores maliciosos puede explotar los servicios tradicionales para cometer fraudes.

Recomienda agregar la rápida evolución de las técnicas de fraude y la falta de actualización continua de los marcos regulatorios y tecnológicos. Finalmente, considera que las consecuencias son resultado de la falta de controles y de la exposición de los usuarios a campañas fraudulentas.

COLCERT

Indica que los elementos que hacen parte entre el flujo de llamadas y mensajes de texto corresponden a los identificados por el COLCERT.

COMCEL

Manifiesta que el problema planteado por la CRC no parte del usuario como centro del perjuicio. En virtud de lo anterior, solicita reformular el problema con el fin de hacer visible que el fraude es una externalidad del modelo actual de acceso a la red y que, al no interrumpirlo, perpetúa la exposición del usuario a un entorno inseguro: «Persistencia de canales habilitados para la comisión de fraudes a usuarios mediante servicios móviles, debido a la falta de consecuencias efectivas frente a agentes reincidentes.»

CRISTÓBAL FUENTES

Indica que, el problema está bien definido porque se enfoca en la ausencia de regulación y reconoce la intención fraudulenta. Así mismo, considera interesante ver que el alcance ha sido determinado muy claramente desde el principio haciendo énfasis en servicios de SMS y voz. Adicionalmente, señala que los elementos como las vulnerabilidades tecnológicas y la ausencia de mecanismos específicos para la detección del fraude en tiempo real mediante SMS o llamadas, así como la falta de plataformas compartidas de validación y monitorización, son factores críticos, por lo que deberían hacer parte de la definición del problema.

ETB

Considera que la definición del problema no incorpora todos los elementos necesarios para comprender plenamente las dificultades generadas por el fraude cibernético. Si bien identifica correctamente el uso indebido de recursos de identificación —como números telefónicos y códigos cortos— por parte de actores malintencionados, restringe el análisis al canal de transmisión (voz y SMS), sin considerar las múltiples capas tecnológicas y la diversidad de actores involucrados en la gestación y ejecución de estos esquemas fraudulentos.

La definición omite elementos fundamentales que condicionan la eficacia de cualquier respuesta regulatoria, en particular al no contemplar:

i. Ecosistema multiplataforma: aplicaciones OTT, redes sociales, comercio electrónico y mensajería instantánea.

ii. Proveedores de Servicios y Contenidos: exentos del registro TIC, pago de contraprestaciones y obligaciones frente a los usuarios lo que facilita escenarios de suplantación.
iii. Plataformas OTT: ofrecen servicios similares a los tradicionales sin regulación, siendo origen de campañas de fraude y enlaces maliciosos que facilita la suplantación de entidades.
iv. Tráfico internacional (*carriers* internacionales): tráfico entrante que representa vulnerabilidad crítica en casos de *spoofing*.

En consecuencia, propone esta reformulación del problema: «Ausencia de un marco regulatorio integral y de mecanismos de control efectivos sobre actores clave del ecosistema TIC, lo que impide abordar de manera sistémica la cadena del fraude cibernético. Esta situación limita la capacidad de prevenir eficazmente el contacto fraudulento a los usuarios a través de servicios de telecomunicaciones y mantiene vigentes vacíos normativos en materia de originación, trazabilidad y autenticación de las comunicaciones fraudulentas».

HABLAME

Sugiere a la CRC profundizar en dos aspectos adicionales críticos que aún no se tuvieron en cuenta dentro del árbol del problema:

i. Uso de rutas entre los PRSTM y los PCA e IT inseguras vía VPN que se anuncian en internet público, por lo que propone que se incluya dentro de las causas del problema la falta de exigencia de enlaces dedicados punto a punto entre los PCA e IT y los PRTSM, que permitan auditar la trazabilidad y garanticen la seguridad extremo a extremo.
ii. Establecer un marco regulatorio que obligue a la cooperación activa, continua, transparente y eficiente entre los actores del ecosistema y evitar fomentar la desvinculación entre PRSTM e Integradores Tecnológicos, esto con el objetivo de construir una capacidad institucional y técnica coordinada para enfrentar los desafíos del fraude digital. Situación que están aprovechando los cibernautas quienes cada día están más fortalecidos mientras los PRSTM y las entidades de vigilancia y control atacan a los PCA e IT.

Considera que el problema central está bien enfocado, pero podría fortalecerse si incluye de forma explícita:

- La falta de obligatoriedad de enlaces dedicados punto a punto entre PCA y PRTSM, lo que expone al ecosistema a rutas no auditables y vulnerables.
-La falta de cooperación entre los diferentes actores de los contratos de acceso, quienes asumen una posición desafiante y estigmatizante contra los PCA e IT, en lugar de asumir una posición de trabajo mancomunado en beneficio de los usuarios.

MDK

Destaca la importancia de una gobernanza transversal y procedimientos homogéneos de registro entre operadores para prevenir el fraude. Sugiere que la ausencia de un sistema centralizado de registro y validación de servicios SMS y voz representa un riesgo significativo. Recomienda incluir esta funcionalidad como elemento esencial en la definición del problema.

Considera también que el documento presenta un análisis sólido sobre el fraude cibernético en servicios de voz y SMS, y que se identifican elementos clave como el uso indebido de numeraciones, la falta de identificación clara de los remitentes y la escasa información disponible para los usuarios. Identifica como retos clave para Colombia la falta de mecanismos centralizados, insuficiente autenticación técnica de los remitentes, escaso intercambio de información entre actores del ecosistema, y ausencia de filtrado en tiempo real.

PLINTRON

Afirma que, el manejo de *smishing* y la implementación del STIR/SHAKEN generarán problemas en los costos y en la efectividad de las medidas porque ya existen mecanismos de fraude para ambos métodos de control.

SIC

Señala que, si bien el documento identifica adecuadamente la problemática desde la perspectiva técnica en materia de fraude cibernético, es necesario que se incorpore de manera explícita el impacto sobre los derechos de los usuarios de servicios de comunicaciones, pues la ausencia de herramientas regulatorias puede ser una causa de la vulneración de estos derechos.

Considera que si bien el problema planteado contempla la mayoría de la casuística que derivan en una conducta delictiva relacionada con el fraude cibernético a través de servicios móviles, no se encuentra contemplada la modalidad *SIM Swapping* o *reposición de la tarjeta SIM.* Manifiesta que, el problema definido se enfoca en las herramientas para prevenir y mitigar técnicamente el contacto a usuarios con fines fraudulentos, excluyendo aquellos escenarios en los que se realizan fraudes cibernéticos por medio de servicios móviles sin que exista interacción con el titular de la línea móvil.

Resalta que, la red móvil constituye un canal de acceso y autenticación de distintos servicios financieros, lo cual exige que las medidas técnicas y regulatorias que rigen el acceso a la red, así como a la información personal tratada por los operadores, deban ser mucho más exigentes con el fin de brindar una protección efectiva a los usuarios.

Propone la siguiente formulación del problema: «Ausencia de herramientas regulatorias para prevenir y mitigar conductas con fines fraudulentos mediante la red móvil que afecten los servicios y los derechos de los usuarios».

UNIVERSIDAD EXTERNADO

Considera que el problema tal como está formulado, efectivamente incorpora de manera pertinente los elementos relativos a las causas y las consecuencias. Indica que, estos elementos, en efecto permiten evidenciar las dificultades generadas por la comisión de estos fraudes cibernéticos y abarcan los aspectos suficientes para un análisis completo que lleve a la formulación del problema como efectivamente se hizo.

TIGO

Considera que la definición del problema no aborda de manera integral la problemática del fraude cibernético. En primer lugar, señala que, el alcance planteado se encuentra limitado a los servicios tradicionales de voz y mensajes de texto, sin considerar de forma adecuada la totalidad de los servicios que conforman el mercado relevante de «servicios móviles», por lo cual señala que es fundamental incluir el servicio de internet móvil en el análisis regulatorio, dado que este medio es ampliamente utilizado para la ejecución de fraudes cibernéticos y, por tanto, constituye un factor clave en la materialización de estos incidentes.

En segundo lugar, indica que, el problema no radica en la ausencia de herramientas regulatorias, sino en incorporar herramientas específicas y establecer consecuencias claras por su no implementación y/o aplicación. En tercer lugar, manifiesta que, la «ausencia de normas» no es un problema en sí mismo, sino que es una de las causas del problema al que se enfrentan los usuarios de los servicios de SMS, voz y datos móviles, así como los PRSTM que están obligados a proveer el acceso a los PCAs e Integradores Tecnológicos, quienes son la fuente del tráfico presuntamente fraudulento que se origina desde sus clientes finales, y al mismo tiempo los PRSTM están obligados a responder por cargas regulatorias de responsabilidad similares a las de los originadores de ese tráfico.

En cuarto lugar, indica que, el planteamiento del problema no está abordando una de las causas estructurales que propicia que los SMS sean actualmente el medio preferido para la comisión de fraude cibernético a través de servicios móviles, y es que la tarifa de cargos de acceso por SMS que los PCA e Integradores Tecnológicos pagan a los PRSTM por el acceso a sus redes en Colombia es excesivamente baja comparada con todo el entorno regional y mundial, lo que se convierte en uno de los principales incentivos para que los fraudes cibernéticos se inicien a través de SMS por la excesiva rentabilidad (relación costo/beneficio) que percibirán los generadores de contenido fraudulento.

Presenta la siguiente propuesta de redacción para el problema: «El contexto actual requiere que la regulación incorpore herramientas específicas para reducir el riesgo de fraude cibernético ejecutados a través de los servicios móviles frente a los cuales aún no existen lineamientos de intervención directa.»

Respuesta CRC:

Con relación a los comentarios recibidos por parte de **ANDESCO**, **COMCEL** y **SIC** en donde manifiestan que la definición del problema debería partir explícitamente de la afectación a los usuarios como eje

central, al ser quienes sufren directamente las consecuencias del fraude, es importante resaltar que, por mandato del legislador, la protección de los derechos de los usuarios constituye un principio rector de la política regulatoria de esta Comisión. En este sentido, en el documento de formulación del problema del presente proyecto regulatorio se incorpora de manera transversal el enfoque de la protección de los derechos a los usuarios, al identificar en las consecuencias afectaciones como la pérdida de confianza, acceso a información privada y la vulneración de sus derechos.

Así mismo, la formulación del problema pone directamente en su planteamiento la exposición de los usuarios a contactos fraudulentos mediante servicios de voz y SMS; adicionalmente, es necesario considerar que el planteamiento del problema central se sustenta en aquellos aspectos que caracteriza, necesariamente, la situación analizada, sin hacer alusión a sus causas, alternativas regulatorias o consecuencias. Así las cosas, la CRC no estima necesario modificar la redacción del problema en dicho sentido, aunque es pertinente aclarar que el énfasis principal de este proyecto es la protección de los derechos de los usuarios, quienes son los beneficiarios de las medidas regulatorias al concebirse como sujeto de protección de estas mismas.

Ahora bien, dado que la regulación vigente, específicamente el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, en los artículos 2.1.10.7 y 2.1.25.1 de la Resolución CRC 5050 de 2016, contempla por una parte, la obligación para los operadores de hacer uso de herramientas adecuadas para prevenir comisión de fraudes y adelantar controles periódicos respecto de las mismas, y por otra parte, la obligación de verificar la identidad del usuario a través de mecanismos confiables de validación, en los casos que así se requiera; esta Comisión evidencia entonces que no existe una ausencia de herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto, sino que por el contrario las existentes carecen de efectividad.

De conformidad con lo anterior el problema a ser resuelto con ocasión del desarrollo del presente proyecto regulatorio, será modificado y quedará así: «Baja efectividad de las herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto».

Respecto a las observaciones de la **ANDI**, **ASOBANCARIA** y **SIC** en donde señalan que la formulación del problema se concentra en actores formalmente registrados ante la CRC, dejando de lado a otros que operan por fuera de la regulación, se hace necesario precisar que, esta entidad reconoce la existencia de actores irregulares que se encuentran por fuera de la cadena de valor del flujo de las comunicaciones. En este contexto se entiende que, desde una perspectiva global, las acciones irregulares con fines fraudulentos se pueden desarrollar desde la originación de la comunicación, es decir, en un extremo de la cadena de valor, razón que motiva el análisis de suficiencia de los actores acogidos en el Régimen de Administración de los Recursos de Identificación, así como las responsabilidades de cada uno de estos, tal como se plantea en la sección de alternativas regulatorias presentadas en este documento.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En este punto, es fundamental reiterar que el fraude cibernético es una problemática amplia con una diversidad de herramientas y consecuencias que emplea diferentes medios de contacto, lo que demanda la necesidad de implementar acciones por parte de autoridades competentes, así como por el sector financiero y otras entidades involucradas en la prevención, detección y judicialización de estas conductas.

Así las cosas, es preciso considerar que el alcance del actual proyecto regulatorio se circunscribe a las competencias asignadas a esta Comisión mediante el marco legal y regulatorio vigente, establecido por Ley 1341 de 2009, Ley 1978 de 2019, el Decreto 1078 de 2015, entre otras disposiciones. En todo caso, el análisis desarrollado contempla los impactos de prácticas originadas desde fuentes o agentes no regulados, razón por la cual, en el marco de la evaluación de alternativas regulatorias planteadas en la temática 3, denominada «Temáticas enfocadas en la educación de la ciudadanía», se evaluará la adopción de estrategias que puedan responder a la necesidad de fortalecer mecanismos de coordinación interinstitucional para abordar amenazas que trascienden a los agentes registrados y regulados por la CRC.

Frente a los comentarios realizados por **ANDI** y **ASOBANCARIA** por medio de los cuales se indica que la suplantación mediante numeración falsa, códigos cortos o identificadores alterados genera riesgos económicos, reputacionales y operativos tanto para usuarios como para operadores y el sector financiero, es necesario manifestar que esta Comisión destaca la relevancia de este señalamiento y resalta que en el documento de formulación se reconoce que la carencia de mecanismos efectivos de verificación favorece estas prácticas fraudulentas.

Específicamente, el documento de Formulación del Problema[5] plantea la «Pérdida de confianza en los servicios de telecomunicaciones» y, de manera más general, las «Afectaciones a empresas y organismos públicos» como una de las consecuencias de las acciones irregulares con fines de fraude que terminan impactando a diferentes sectores de la economía. De igual manera, se puntualiza que las alternativas regulatorias ponen en consideración la pertinencia de adoptar la trazabilidad de los recursos de identificación, con el fin de aumentar la confianza de los usuarios en los canales de voz y mensajería, lo que a su vez incide en las demás actividades económicas que soportan algunos elementos operativos para el contacto con sus usuarios por medio de estos servicios.

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.

[5] CRC. Documento de formulación del problema del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Página 42. https://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

No obstante, en la sección del presente documento se proponen alternativas regulatorias que plantean la adopción de obligaciones y responsabilidades diferenciadas, así como compartidas entre los diferentes agentes de la cadena de valor, de manera que se garantice una mayor corresponsabilidad frente a la mitigación del fraude. Dentro de las temáticas objeto de revisión asociadas al Régimen de administración de Recursos de Identificación bajo el enfoque de simplificación (numeral 7.4), que se publican para consideraciones y comentarios del sector, se incluye la posibilidad de considerar la reincidencia como un criterio relevante en la administración, asignación y recuperación de códigos cortos, con el fin fortalecer la prevención de acciones irregulares con fines fraudulentos de forma sistemática, así como la aplicación de sanciones para quienes realicen un uso indebido de dicho recurso.

Sobre los comentarios de **ANDI** y **ASOBANCARIA** destacan que, pese al decrecimiento en volumen de tráfico, los servicios tradicionales de voz y SMS siguen siendo canales prioritarios para la comisión de fraudes, es necesario indicar que el énfasis de la formulación del problema se centra en estos servicios, dado que son usados como puerta de entrada a la red de los servicios de telecomunicaciones para el desarrollo de acciones irregulares con fines fraudulentos, para posteriormente capturar de forma irregular información privada y sensible de los usuarios, lo que fortalece el enfoque sobre estos servicios para la presentación de las alternativas regulatorias planteadas.

Con respecto a la solicitud presenta por **ASOMÓVIL**, **ETB**, **SIC** y **TIGO** de ampliar el alcance del problema para incluir el papel del internet y de aplicaciones OTT, esto debido a que los fraudes suelen concretarse o amplificarse a través de enlaces maliciosos o mensajes en estas plataformas, es pertinente señalar que, esta Comisión coincide en la relevancia de este aspecto, sin embargo, el actual proyecto regulatorio se concentra en recursos de identificación bajo administración de esta entidad, en tanto que la CRC no tiene asignadas competencias de manera expresa para regular este tipo de servicios, y en particular aquellas en materia de protección de usuarios[6].

Ahora, teniendo en cuenta que el internet móvil en algunos casos puede ser usado como un habilitador transversal del fraude, en el marco de las alternativas regulatorias propuestas se contemplan medidas que permiten limitar el direccionamiento de los usuarios a sitios web fraudulentos, aplicaciones no verificadas o contenidos que faciliten la suplantación de identidad, garantizando así la consistencia con las competencias regulatorias.

Con relación a la observación de **AVAL** en donde manifiesta la necesidad de establecer medidas diferenciales con enfoques poblacionales que consideren grupos como adultos mayores y menores de edad, se hace necesario indicar que para esta Comisión dicho enfoque resulta consistente con el principio de protección reforzada de usuarios en condiciones de vulnerabilidad, de tal manera que es

[6] El documento del estudio sobre «El rol de los servicios OTT en el sector de las comunicaciones en Colombia - 2024», propone como acción estratégica a cargo de otras entidades, particularmente del legislativo, la necesidad de analizar el sector TIC con la totalidad de los agentes en él involucrados incluidas las plataformas de servicios digitales y aplicaciones y, en consecuencia, asignar funciones explícitas a las autoridades del sector respecto de estos nuevos agentes. Página 203. Disponible en: https://www.crcom.gov.co/es/biblioteca-virtual/estudio-sobre-rol-servicios-over-top-ott-en-colombia-2024

pertinente acogerlo en el marco del análisis de alternativas planteadas en la sección 7.3 del presente documento, en donde se describen las «Temáticas enfocadas en la educación de la ciudadanía».

En relación con los comentarios de **AVAL**, **ETB** y **SIC** sobre la necesidad de incorporar en la formulación del problema modalidades emergentes, como *SIM Swapping* o el uso de IAG (Inteligencia artificial Generativa) para suplantación de voz/mensajes, y la rápida evolución de los fraudes, es necesario indicar que estas modalidades de fraude se encuentran contempladas en la causa denominada «Dificultad en la identificación y rastreo de ataques cibernéticos» del árbol del problema[7], en donde se indica que estos son mecanismos que limitan la efectividad de algunas medidas de mitigación dadas las brechas en los sistemas de autenticación y en la interoperabilidad entre operadores.

En este sentido, es necesario mencionar que los operadores móviles, de manera voluntaria, han avanzado en el desarrollo de herramientas y mecanismos basados en datos disponibles al interior de sus redes a fin de favorecer procesos comerciales y de mitigación del fraude. Mediante estas herramientas, los PRSTM pueden poner a disposición información útil mediante APIs u otras herramientas, como validación de titularidad de línea o detección de cambios recientes en la SIM, herramientas que permitirían robustecer los esquemas de autenticación de múltiples factores mediante mecanismos como el OTP utilizados por otros sectores, como el financiero.

Sin embargo, para que estas iniciativas tengan un efecto estructural en la mitigación del fraude, resulta indispensable que se articulen esfuerzos con las entidades responsables de la regulación y supervisión del sistema financiero, las agremiaciones de dicho sector, y las propias entidades financieras, a fin de definir mecanismos de cooperación técnica, esquemas de gobernanza de datos y responsabilidades compartidas en el uso de estos nuevos mecanismos de validación. Lo anterior no obsta para que, si con ocasión del desarrollo del presente proyecto se evidencia la necesidad, oportunidad y conveniencia de fortalecer las medidas regulatorias vigentes asociadas al cambio de SIM Cards y a la validación que deben adelantar los PRSTM para la autenticación de sus usuarios, esta Comisión modificará o incorporará lo pertinente.

De forma adicional, esta Comisión destaca que en el marco del proyecto regulatorio[8] «Revisión de Medidas Aplicables a Servicios Móviles - Fase 2», mediante la Resolución CRC 7684 de 2025, se adoptaron medidas dirigidas a fortalecer la verificación de la identidad de los titulares de líneas móviles, tanto en modalidad prepago, solicitando el registro y verificación de datos antes de la activación, como en el proceso establecido para la prestación del servicio en la modalidad de pospago.

Estas medidas tienen por objeto reforzar la seguridad en los procesos de acceso a los servicios móviles, disminuyendo las oportunidades de explotación por parte de actores maliciosos. Ahora, se debe señalar

[7] CRC. Documento de formulación del problema del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Página 44. https://crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf
[8] CRC. Proyecto regulatorio «Revisión de Medidas Aplicables a Servicios Móviles - Fase 2». Disponible en: https://crcom.gov.co/es/proyectos-regulatorios/2000-38-3-17-1

que, de acuerdo con la Política de Mejora Regulatoria, el impacto de la medida que trata sobre «la identidad de los titulares de líneas móviles» debe ser determinado en el marco del proceso de evaluación ex post con el fin de verificar su eficacia y ajustar estrategias si se detectan nuevos patrones de fraude.

Por otro lado, es importante reconocer que las técnicas de fraude cibernético presentan una dinámica evolutiva acelerada, lo cual representa un reto no solo para la CRC, sino también para otras instituciones del ecosistema digital. Así mismo, la naturaleza compleja del fraude digital exige un trabajo interinstitucional robusto. En este contexto, en el presente proyecto regulatorio se contempla la implementación de acciones orientadas a la articulación con entidades del sector, autoridades judiciales y organismos de ciberseguridad, con el fin de compartir mecanismos conjuntos que contribuyan mitigación y respuesta frente a la aparición de nuevas modalidades fraudulentas.

Con respecto a la observación de **PLINTRON** en donde indica que la implementación de STIR/SHAKEN presenta limitaciones frente a modalidades de fraude y una baja relación de efectividad frente a su costo, es necesario aclarar que la definición de este tipo de estándares técnicos requiere de un estudio específico y detallado en el marco de un análisis de impacto normativo (AIN) para evaluar su viabilidad técnica, legal y económica.

En este sentido, la implementación de este proceso de evaluación garantiza que se estructuren instrumentos regulatorios técnicos, consistentes en términos con el AIN en relación con el problema formulado y los criterios establecidos. Así las cosas, el presente documento de formulación de alternativas regulatorias pone en consideración el método STIR/SHAKEN como una de las opciones para la prevención del fraude, para que sea sujeta del proceso de evaluación determinado en el marco del AIN. Lo anterior no obsta para que los agentes interesados puedan aportar información técnica y económica relevante que sustente la eventual inviabilidad de su implementación como alternativa regulatoria.

En relación con la propuesta de **HABLAME** de incluir como causa del problema la falta de obligatoriedad de enlaces dedicados punto a punto entre los PCA/IT y los PRSTM, esta Comisión reconoce que la seguridad en las rutas de acceso constituye un elemento relevante en la mitigación del fraude. No obstante, es importante precisar que la problemática identificada no está relacionada con vulnerabilidades de infraestructura física, sino con la disposición de canales de acceso que permiten el ingreso de tráfico con contenido irregular, que posteriormente es utilizado para cometer fraudes. Si bien, la utilización de enlaces dedicados punto a punto puede reforzar la seguridad en la transmisión y prevenir ciertas vulneraciones, no necesariamente garantiza la autenticación del originador del tráfico ni evita que se generen comunicaciones con contenido fraudulento desde un actor irregular.

Adicionalmente, es importante considerar que la Resolución CRC 5050 de 2016, en su Título IV que trata sobre las condiciones para el acceso e interconexión de redes de telecomunicaciones, establece en su artículo 4.1.1.3, que los PRSTM deben garantizar condiciones seguras, transparentes y no discriminatorias en la provisión de acceso, dejando abierta la posibilidad de implementar distintos mecanismos técnicos que cumplan con estos fines. A la luz de esta disposición regulatoria, la exigencia

de un único tipo de enlace podría entrar en tensión con el principio de neutralidad tecnológica, mientras que un enfoque más amplio, basado en requisitos de seguridad, trazabilidad y autenticación en los canales de acceso, resultaría más consistente con las competencias regulatorias de la CRC y con las mejores prácticas internacionales.

En relación con la observación de **TIGO** en donde señala que las bajas tarifas de cargos de acceso a SMS constituyen un incentivo estructural para la proliferación de fraudes, esta Comisión precisa que, si bien el tema planteado no se encuentra dentro del alcance definido para el presente proyecto regulatorio, dado que se relaciona con aspectos de remuneración de las relaciones de acceso entre operadores, es importante aclarar que este tipo de cargos responden a criterios de eficiencia económica, transparencia y orientación a costos, buscando garantizar condiciones de competencia y un uso eficiente de los recursos de red en consistencia con lo establecido en el numeral 3 del artículo 2 de la Ley 1341 de 2009, denominado «uso eficiente de la infraestructura y de los recursos escasos».

En ese sentido, la definición de esquemas de remuneración de interconexión, incluyendo los cargos de acceso, han sido abordados en proyectos regulatorios específicos[9] que se sustentan en una metodología técnica y económica, los cuales tienen el propósito de asegurar la adecuada recuperación de costos y promover la sostenibilidad de la prestación del servicio.

Es preciso indicar que esta temática hace parte del alcance proyecto regulatorio denominado «Esquema de remuneración mayorista de redes móviles», en donde la revisión de las tarifas de remuneración aplicables al servicio de mensajes móviles resulta altamente pertinente y coherente con los objetivos establecidos. Por tanto, no corresponde su tratamiento en el marco del presente proyecto, cuyo alcance se concentra en la caracterización y mitigación del fraude a través de servicios móviles tradicionales de voz y mensajes de texto.

3.3. Comentarios sobre las causas del problema

ANDESCO

Sugiere incluir como causas: i) la falta de consecuencias estructurales frente a la reincidencia, ii) el vacío regulatorio y la inhabilitación a los PRSTM para implementación de medidas de control permiten la propagación y crecimiento exponencial de los fraudes de voz y SMS; y iii) imposibilidad de terminar relación de acceso con PCA o IT reincidente en el envío de SMS con contenido fraudulento.

ASOMÓVIL

Destaca en su escrito que aunque la CRC recupera los códigos cortos que son usados indebidamente, estas acciones son insuficientes para enfrentar el fraude cibernético móvil debido a:

[9] CRC. Proyecto regulatorio «Revisión de los esquemas de remuneración móvil». Disponible en: https://crcom.gov.co/es/proyectos-regulatorios/2000-38-3-2

-Poca efectividad de la medida: al infractor solo se le retira el código, pero su contrato con el operador permanece, lo que le permite solicitar nuevos recursos o seguir operando por otros medios.
-Falta de sanción a reincidentes: no existen medidas acumulativas ni inhabilitaciones, por lo que el impacto real sobre el infractor es bajo frente al perjuicio ocasionado a usuarios y operadores.
-Respuesta limitada de otras autoridades: ni MinTIC, ni SIC, ni la Fiscalía actúan con la rapidez o alcance necesarios, lo que deja un vacío en la sanción integral y en la protección a las víctimas.
-Ausencia de regulación sobre *Spoofing*: no hay medidas para controlar esta modalidad de fraude, especialmente en lo que respecta a los Carrier internacionales, quienes no tienen obligaciones regulatorias para prevenir ni responder frente al fraude.

COLCERT

Considera que las causas planteadas por la CRC son las adecuadas y soportan la problemática identificada.

COMCEL

Sugiere incluir como causas: i) la falta de consecuencias estructurales frente a la reincidencia, ii) el vacío regulatorio y la inhabilitación a los PRSTM para implementación de medidas de control permiten la propagación y crecimiento exponencial de los fraudes de voz y SMS; y iii) imposibilidad de terminar relación de acceso con PCA o IT reincidente en el envío de SMS con contenido fraudulento.

CRISTÓBAL FUENTES

Indica que, la definición del problema plantea que la combinación de un entorno regulatorio que no aborda adecuadamente la prevención del fraude, junto con medidas preventivas inadecuadas por parte de los proveedores de servicios, la falta de conciencia de los usuarios y una débil coordinación institucional crea un entorno propicio para el desarrollo de actividades fraudulentas mediante el uso de los servicios de comunicación tradicionales.

ETB

Considera que se omiten las siguientes causas estructurales: la ausencia de obligaciones regulatorias para los PCA, la desregulación de los *carriers* internacionales, la inexistencia de una estrategia de trazabilidad y monitoria integral, la omisión del rol de las OTT como canal principal de fraude y su falta de cooperación efectiva con autoridades, y la ausencia de control por parte de MinTIC a actores como los PCA y otros, a pesar de estar inmersos en la definición del artículo 6 de la Ley 1341 de 2009.

MDK

Coincide con las causas señaladas en el documento, pero recomienda complementar las causas con el siguiente planteamiento: «La ausencia de un sistema obligatorio, estandarizado a nivel nacional, para el registro y verificación de servicios A2P de SMS y voz impide un control y trazabilidad efectivos. Esta situación se agrava por la falta de una plataforma de datos centralizada con acceso coordinado entre actores clave, así como por la falta de claridad regulatoria y de interoperabilidad técnica.»

Afirma que solo a través de un modelo obligatorio y estandarizado se podrá garantizar una protección contra el fraude que sea sostenible y efectiva.

PLINTRON

Señala que es la primera aproximación real regulatoria al problema.

SIC

Manifiesta que si bien, las causas identificadas son acertadas, se ha dejado la autogestión y control de la plataforma y sus recursos a los PRST, PCA e Integradores Tecnológicos, quienes conforme el requerimiento general formulado por la CRC, no han adoptado medidas verdaderamente seguras para prevenir de manera efectiva las conductas fraudulentas.

Señala que, las medidas que debían haber implementado los PRST no deben limitarse a prevenir el contacto fraudulento con los usuarios, sino también a evitar la obtención de servicios de manera fraudulenta por medio de la suplantación de identidad de sus usuarios o de violación de sus datos personales.

Indica que, los PRST, PCA e IT han manifestado que el fraude es ajeno a sus redes o a la prestación del servicio, desconociendo así, la importancia de proteger los datos personales de los usuarios y establecer medios efectivos para evitar la suplantación de identidad al acceder a sus servicios o a sus redes.

Señala que, este proyecto regulatorio, responde a la *Estrategia Nacional de Seguridad Digital.*

TIGO

Propone las siguientes causas:

-Falta de herramientas para realizar un debido control y vigilancia de los recursos de identificación por parte del administrador y entidades de vigilancia y control.
-Falta de mecanismos más estrictos para la asignación de los códigos cortos y recuperación de estos cuando se den usos indebidos.

-Optimizar los procedimientos asociados a la recuperación de códigos cortos en los casos en donde se identifiquen usos indebidos, para que las acciones puedan tomarse de manera más oportuna, protegiendo así a los usuarios de posibles fraudes.
-Ausencia de herramientas especificas regulatorias para que los PRSTM tengan la posibilidad de dar por terminada la relación de acceso y proceder con su desconexión de la red del operador, cuando se presente reincidencia.
-Desconocimiento de los usuarios sobre las modalidades de fraude cibernético y como ellos se constituyen en un pilar clave para mitigar este flagelo.
-Las obligaciones regulatorias recaen sólo sobre unos actores de la cadena de valor, son asimétricas y en otros casos difusas.
-Contacto sin el consentimiento previo y explícito de los usuarios, pues el consentimiento otorgado a un PRSTM no puede extenderse a todos los actores que intervienen en la cadena de valor de la comunicación por SMS, llamadas y correos electrónicos, y es necesario que cada actor gestione las respectivas autorizaciones, lo cual incluye no sólo a las entidades originadoras de los mensajes, sino también a sus socios comerciales, PCA, los integradores tecnológicos y proveedores de contenido OTT.
-Escasa coordinación entre PRSTM, la CRC, la SIC y las demás entidades y autoridades que intervienen en la prevención, vigilancia y control de fraudes cibernéticos.
-La regulación focaliza sus esfuerzos en los servicios de conectividad, mientras que la regulación relacionada con servicios sobre contenidos mediante plataformas digitales es limitada.

UNIVERSIDAD EXTERNADO

Sugiere tener en cuenta que existe una limitada cooperación internacional y dificultad para perseguir responsables: Manifiesta que, teniendo en cuenta que muchos fraudes provienen de números extranjeros o de redes y que hace falta una coordinación internacional que permita una mayor efectividad en la persecución de los responsables, ya que el fraude cibernético es por definición transnacional; y que, sin acuerdos o mecanismos ágiles de cooperación internacional, identificar a los responsables reales y cortar el fraude desde la fuente es casi imposible.

Respuesta CRC:

Frente a los comentarios de **ANDESCO** y **COMCEL**, esta Comisión aclara que estas posibles situaciones se pueden entender recogidas dentro de la causa «las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso», es así como dentro del marco de la regulación y administración de dichos recursos, no se ha explorado la definición de reglas específicas orientadas a generar información o a establecer condiciones regulatorias para mitigar el fraude, como la suplantación de identidad o el uso indebido de la numeración. Por lo cual una revisión de las medidas del Régimen de Recursos de Identificación, la cual se surtirá con ocasión del presente proyecto regulatorio, permitirá 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.

En relación con los comentarios de **ASOMÓVIL** y **ETB** se reitera lo expuesto previamente, en el sentido que las acciones asociadas a posibles vacíos en la regulación vigente, serán objeto de análisis dentro de este proyecto regulatorio. Ahora bien, frente a la respuesta limitada de otras autoridades, esta Comisión pretende con este proyecto regulatorio, entre otras medidas, definir líneas de acción y recomendaciones para la construcción conjunta de una estrategia nacional de prevención en el contacto a usuarios con fines fraudulentos.

Respecto de lo expuesto por **MDK,** esta Comisión considera que la redacción planteada en el comentario contiene elementos que se entienden inmersos en la causa «las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso», por lo cual no se considera pertinente limitar esta causa a circunstancias puntuales que podrían llegar a limitar la revisión integral que se pretende adelantar con este proyecto regulatorio.

En cuanto a los comentarios de la **SIC**, la CRC coincide en que existe una ineficiencia de las medidas de autogestión y autocontrol que han implementado los diferentes agentes intervinientes en el flujo de la comunicación con los usuarios finales, y que es deber de estos agentes adoptar las medidas necesarias para prevenir el fraude. Ahora bien, estos elementos ya se encuentran cubiertos por la causa «Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes», por tanto, estos agentes, así como la posible necesidad y pertinencia de establecer desde la regulación medidas que generen nuevas acciones a adoptar por parte de los mismos, serán objeto de análisis en desarrollo del presente proyecto regulatorio.

Acerca de los comentarios de **TIGO**, en primer lugar, es importante aclarar que las medidas adoptadas como resultado de este proyecto regulatorio serán estrictamente cobijadas dentro del marco de nuestras competencias. Lo cual no obsta para que se generen recomendaciones para todos los agentes que pueden verse vinculados en la mitigación y prevención del fraude cibernético a través de servicios de voz y mensajes de texto.

Por otra parte, si bien se considera que las circunstancias expuestas ya se encuentran cubiertas dentro de las causas propuestas por la CRC en el Documento de Formulación del Problema de este proyecto regulatorio, llama la atención de esta Entidad, la necesidad de ampliar el alcance de la causa preliminarmente denominada «Desconocimiento de los usuarios sobre privacidad de la información facilita la obtención de datos personales con fines fraudulentos» pues es cierto que en el caso que nos ocupa, la materialización del problema no solo ocurre por el desconocimiento de los derechos que le asisten en relación con el tratamiento de sus datos personales; sino que también es necesario reconocer la ausencia de información y conocimiento de estos agentes respecto de las diferentes modalidades de ataque y las acciones de prevención y respuesta que deben tomar.

De acuerdo con lo anterior se procederá a modificar la referida causa, la cual pasará a ser una consecuencia y quedará así: «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»

Finalmente, en relación con el comentario de la **UNIVERSIDAD EXTERNADO** en el que sugiere considerar la limitada cooperación internacional que existe y la dificultad para perseguir los responsables, cuando el fraude proviene de números extranjeros, se reitera que el alcance del presente proyecto regulatorio se limita a los agentes sujetos de regulación de acuerdo con el marco competencial de esta Comisión. Ahora bien, de ninguna manera esto implica que se desconozca en el análisis que se está haciendo la existencia de terceros actores y la posibilidad de establecer recomendaciones o planes de acción para fortalecer dicha cooperación internacional.

3.3.1. Comentarios a la causa «Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso»

ANDI

Señala que las medidas técnicas y regulatorias en torno a la administración de los recursos de identificación se han enfocado principalmente en garantizar su uso eficiente, bajo la lógica de tratarse de un recurso escaso. No obstante, expone que este enfoque ha dejado de lado la necesidad de contar con mecanismos regulatorios robustos que permitan diferenciar entre comunicaciones legítimas y fraudulentas, así como de establecer obligaciones claras para que los operadores verifiquen o monitoreen el uso adecuado de los números asignados.

Señala que el marco vigente resulta insuficiente, pues no disuade de manera efectiva a los Proveedores de Contenidos y Aplicaciones (PCA) o Integradores Tecnológicos (IT) reincidentes en malas prácticas, ni impone consecuencias directas sobre su relación de acceso con los operadores de red. En la actualidad, la reincidencia carece de sanciones claras, y los incentivos son débiles: el costo de reincidir puede ser menor que el beneficio económico obtenido por facilitar fraudes. De este modo, mientras exista la posibilidad de seguir operando tras múltiples recuperaciones de numeración, el cumplimiento regulatorio seguirá siendo frágil.

La reiteración en el uso indebido de códigos cortos refleja deficiencias en la gestión interna de seguridad de los PCA e IT y evidencia que no se trata de fallas aisladas, sino de un patrón sostenido. Estas prácticas fraudulentas no solo impactan directamente a los usuarios, sino que también erosionan la confianza en el ecosistema de telecomunicaciones y en las instituciones suplantadas, debilitando la legitimidad de canales tradicionales como el SMS y la voz.

Adicionalmente, se resalta la ausencia de una taxonomía unificada de fraudes y la falta de coordinación interinstitucional para regular y mitigar adecuadamente este fenómeno. Es indispensable incorporar consecuencias estructurales frente a la reincidencia, superar los vacíos regulatorios que impiden a los operadores implementar medidas de control efectivas, habilitar la terminación de relaciones de acceso con PCA e IT que reiteradamente envíen mensajes fraudulentos y fortalecer la participación activa del MinTIC en la materia.

ASOBANCARIA

Considera que resulta necesario contar con mecanismos regulatorios robustos que permitan distinguir entre comunicaciones legítimas y suplantadas, así como que los operadores verifiquen o monitoreen el uso adecuado de los números asignados. Ha identificado la falta de una taxonomía unificada sobre fraudes que requiere una articulación interinstitucional. Observa diferencias entre el marco normativo aplicable a las entidades vigiladas por la SFC y la CRC, en lo relacionado con seguridad de la información, fraudes, ciberseguridad y el régimen de responsabilidad correspondiente. Indica que podría resultar valiosa la experiencia de la SFC para la construcción de un marco regulatorio integral que abarque a todos los actores involucrados en los denominados *riesgos cibernéticos*.

Recomienda incluir como causa adicional la ausencia de mecanismos obligatorios de validación de identidad del originador de llamadas y mensajes, lo que facilita la suplantación de entidades legítimas, como instituciones financieras.

Indica que, actualmente, el sector financiero y el de telecomunicaciones cuentan con una relación estrecha en la vinculación y prestación de los servicios financieros. En concreto, como mecanismos de autenticación durante la vinculación a un producto financiero (p. ej., códigos *One Time Password*) o durante el inicio de sesión en los canales digitales de entidades financieras. No obstante, los operadores no cuentan con exigencias igual de robustas a las entidades financieras, de cara a los requisitos y condiciones asociadas a los procesos de debida diligencia, conocimiento y autenticación de las personas que poseen y utilizan SIM y eSIM.

Finalmente, propone considerar las siguientes iniciativas:

i. Obligación de los operadores de telefonía móvil de contar con mecanismos fuertes de autenticación y validación de identidad para clientes.
ii. Requisitos para controlar la emisión y reexpedición de SIM y eSIM por parte de operadores de telefonía móvil.
iii. Creación de un registro de titulares de líneas de telefonía móvil. Este registro contendría los titulares de las líneas de telefonía móvil para identificar a los titulares.

ASOMÓVIL

Expone que la CRC en ejercicio de sus funciones en materia de recursos de identificación, principalmente recuperando los códigos cortos, ha detectado la reincidencia de ciertos PCA e Integradores Tecnológicos en el uso fraudulento de numeración, reutilizando códigos cortos y numeración para campañas engañosas, incluso tras sanciones de tipo recuperación.

Señala que esta situación, deja en evidencia fallas en controles y falta de efecto disuasivo, poniendo en riesgo la integridad del sistema y la confianza de los usuarios. Propone que se reconozca dentro del

problema la existencia de actores reincidentes específicos, e implementar mecanismos que eviten que un mismo sujeto pueda seguir reutilizando numeración o infraestructura de otro operador tras sanciones leves. Expone que la trazabilidad total de quién está detrás de cada campaña y la publicidad de los infractores reiterativos son elementos clave para romper ese ciclo de fraude.

HABLAME

No está de acuerdo con la causa que indica que «las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso», como si esto fuera el origen del problema. Considera que la raíz del problema es que la CRC no tiene un entendimiento actualizado y profundo del funcionamiento real del mercado de mensajería A2P ni de la cadena de valor involucrada en los servicios de SMS, particularmente en lo relacionado con los roles PCA, los Integradores Tecnológicos y los operadores internacionales.

Adicionalmente, señala que el enfoque regulatorio actual desconoce dinámicas clave del ecosistema, como:

-La participación de múltiples actores fuera del control directo del asignatario del recurso.
-La complejidad de la trazabilidad cuando intervienen integradores internacionales o rutas de tránsito.
-La necesidad de establecer estándares técnicos y contractuales que protejan el recurso en toda la cadena.

Así mismo, manifiesta que mientras la CRC no evolucione su comprensión del mercado y no se actualice en línea con las tendencias globales en trazabilidad, autenticación, enrutamiento responsable y filtrado de tráfico, no será posible garantizar un uso eficiente del recurso ni generar condiciones adecuadas que respalden a los actores responsables como los PCA e integradores serios.

En ese sentido, concluye que más que un problema de «uso eficiente», lo que se requiere es una regulación alineada con la realidad operativa, tecnológica y comercial actual del ecosistema de SMS, que permita implementar mecanismos efectivos de seguridad, control y prevención, sin castigar o entorpecer la operación de quienes sí cumplen.

UNIVERSIDAD EXTERNADO

Señala que existe una falta de interoperabilidad y estandarización de medidas de prevención entre operadores y que, sin medidas coordinadas, el control es parcial y el fraude persiste, por lo cual, es importante que la causa en cuestión no sea sólo que las medidas son insuficientes sino que no hay una estandarización e interoperabilidad de estas, por lo cual, la causa en cuestión podría complementarse o agregarse de manera independiente al análisis.

Respuesta CRC:

Frente a los comentarios de la **ANDI** y **ASOMÓVIL**, es pertinente precisar que, de acuerdo con la normativa vigente, pueden ser asignatarios de códigos cortos los Proveedores de Contenidos y Aplicaciones (PCA), los Integradores Tecnológicos (IT) que ofrecen servicios vía SMS y USSD, así como los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) actuando en calidad de PCA. En este marco, la regulación contempla dos aspectos centrales: i) el uso eficiente de los códigos cortos, lo cual implica su implementación y utilización constante desde el momento de la asignación, verificado a través del Formato T.5.2. REPORTE DE CÓDIGOS CORTOS, y ii) las causales de recuperación del recurso de identificación, entre las cuales se destacan el uso distinto al autorizado o el envío de mensajes en nombre de terceros sin autorización previa, expresa y escrita. En consecuencia, la CRC puede recuperar un código corto cuando se configuran dichas causales, incluso si este ha sido asignado a un PRST en su condición de PCA. Asimismo, el procedimiento de asignación dispone que, si en el año anterior la CRC recuperó uno o más códigos cortos a un mismo asignatario, no procederá la asignación de nuevos recursos a su favor.

Así, el problema no se limita a terceros asignatarios de códigos cortos (PCA o IT), sino que también puede involucrar a los operadores móviles asignatarios en calidad de PCA. Esta situación no exime el cumplimiento de la norma, dado que la CRC, en virtud de las funciones que le otorga la Ley 1341 de 2009, ejerce la facultad de recuperación sin distinguir si el asignatario es un PRST en condición de PCA o un agente PCA/IT. En todos los casos, la obligación de cumplimiento recae sobre el asignatario.

En este sentido, frente al escenario planteado por la **ANDI** y **ASOMÓVIL** respecto a los PCA e IT reincidentes en el uso indebido de los códigos cortos, así como la necesidad de establecer mecanismos normativos que impidan que un mismo sujeto pueda continuar reutilizando numeración o infraestructura de un operador móvil tras la imposición de sanciones leves —como la recuperación del recurso—, e incluso ante la propuesta de evaluar la reincidencia de dichos actores y la posibilidad de terminar las relaciones comerciales con esos actores, resulta necesario precisar que si bien se adelantará el respectivo análisis regulatorio, el mismo debe extenderse igualmente a los PRST asignatarios de códigos cortos en calidad de PCA.

En consecuencia, las medidas regulatorias que puedan derivarse del presente proyecto no deben desnaturalizar la condición de asignatario del código corto, independientemente de que este actúe como IT, PCA o PRST en condición de PCA. Por lo tanto, las medidas regulatorias que se definan no pueden aplicarse de manera discriminada, sino que deben considerar de forma integral las condiciones de recuperación del recurso y las medidas aplicables a todos los actores involucrados, incluidos los PRST que ostenten la calidad de PCA y que, eventualmente, puedan incurrir en incumplimientos normativos.

Sin perjuicio de lo anterior, lo señalado será objeto de análisis dentro de los límites de las facultades de la CRC y en concordancia con el alcance del presente proyecto regulatorio.

En este contexto, y en relación con el comentario de **ASOBANCARIA** resulta oportuno tener en cuenta que la asignación de un recurso de identificación es una autorización concedida por la CRC 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, por tanto, ese asignatario debe cumplir las obligaciones dispuestas para tal fin en la Resolución CRC 5050 de 2016, así como los criterios de uso eficiente para el recurso de identificación asignado. Adicionalmente, debe evitar incurrir en alguna de las causales de recuperación definidas, so pena de recuperación del recurso de identificación correspondiente. De manera que los recursos de identificación asignados deben ser utilizados de forma eficiente.

Visto lo anterior, el uso eficiente de un recurso escaso como los códigos cortos no se limita únicamente a su utilización o implementación, sino que, conforme a la normativa vigente, implica también obligaciones generales y específicas para los asignatarios (PCA e Integradores Tecnológicos). Estos deben emplear herramientas tecnológicas que prevengan fraudes mediante SMS o USSD, así como realizar controles periódicos que permitan evaluar la efectividad de dichos mecanismos. Sin embargo, es preciso señalar que, como se ha indicado en otra causal, las medidas de gestión y control adoptadas tanto por los PRST como por los asignatarios de recursos de identificación han resultado insuficientes.

Finalmente, respecto al registro de SIM y eSIM es de señalar que esta Entidad expidió la Resolución CRC 7684 de 2025[10], la cual dispone el procedimiento para la activación de servicios móviles (adquisición, proceso de activación de servicios móviles, recolección de datos de identificación del usuario, y verificación de identidad del usuario).

De otra parte, si bien **HABLAME** señala la complejidad del ecosistema de mensajería A2P y la participación de múltiples actores en la cadena de valor, este argumento no desvirtúa o conlleva a la necesidad de complementar la causa «Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso», dado que, otra de las causas identificadas es la ausencia de medidas de control concretas y verificables por parte de los asignatarios de los recursos de identificación. Adicional a lo anterior, es importante aclarar que, la regulación vigente ya establece obligaciones claras para PCA y PRST en materia de seguridad, prevención de fraude y monitoreo de tráfico, de modo que no es cierto que se carezca de lineamientos por efecto del desconocimiento del ecosistema de mensajería.

El hecho de que existan múltiples intermediarios o rutas internacionales no exime a los asignatarios de su deber de implementar controles eficaces que aseguren el uso legítimo de los códigos cortos. De hecho, en otros mercados internacionales con condiciones similares de complejidad, los operadores y asignatarios han demostrado que sí es posible aplicar mecanismos de trazabilidad, filtrado y monitoreo con resultados tangibles en la reducción del fraude.

Por tanto, el problema no radica en una supuesta ausencia de entendimiento por parte de la CRC respecto de la cadena de valor asociada al envío de mensajes cortos de texto (SMS), liderada por el

[10] «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»

asignatario del recurso de identificación, sino en la ineficacia de las medidas adoptadas por los propios asignatarios, que no han mostrado resultados contundentes frente al fraude en SMS, a pesar de contar con un marco normativo que lo exige y que se señalará en la siguiente sección.

En consecuencia, la finalidad del proyecto es justamente cerrar esa brecha: reforzar el marco normativo declarativo a alternativas que permitan verificar el cumplimiento real y los resultados frente a las prácticas fraudulentas.

Finalmente, frente al comentario de la **UNIVERSIDAD EXTERNADO** se valora el aporte realizado en cuanto a la necesidad de contar con mayor interoperabilidad y estandarización de medidas de prevención entre operadores, como condición para que los controles resulten efectivos y sostenibles en el tiempo. Este planteamiento será tenido en cuenta dentro de los objetivos del proyecto, de manera que las acciones propuestas no solo aborden la insuficiencia de medidas actuales en materia de administración de recursos de identificación, sino que también promuevan esquemas coordinados que fortalezcan la prevención del fraude en el ecosistema de mensajería.

3.3.2. Comentarios a la causa «Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes»

ANDI

Señala como causa del problema la insuficiencia de las medidas de gestión y control adoptadas por los PRST y asignatarios de recursos de identificación, sin reconocer las limitaciones regulatorias, técnicas y operativas que enfrentan estos agentes. Indica que, no es posible exigirles una prevención efectiva sin que exista habilitación normativa ni capacidades operativas para ello, pues los operadores no cuentan con competencias legales ni con una instancia de coordinación que les permita bloquear, filtrar o prevenir de manera proactiva conductas fraudulentas que ocurren en cuestión de segundos.

Además, expone que en fraudes como el *smishing* o las llamadas falsas que inducen a transferencias bancarias, los efectos se materializan de manera inmediata, por lo que cualquier acción posterior resulta tardía. Las medidas reactivas, por tanto, no son un error de diseño, sino la única herramienta actualmente disponible frente a amenazas ya ejecutadas.

En este contexto, señala que lo prioritario es reconocer que el marco regulatorio y operativo actual no permite implementar medidas más eficaces. Para avanzar hacia un esquema preventivo, recomienda facultar expresamente a los PRST y asignatarios para bloquear tráfico o numeración sospechosa de forma preventiva sin exponerse a sanciones regulatorias, y permitir la suspensión provisional o terminación definitiva de la relación de acceso con PCA o IT que usen indebidamente la numeración, de manera que se resuelva de raíz la problemática.

ASOBANCARIA

Indica que el documento señala como una de las causas del problema la supuesta insuficiencia de las medidas adoptadas por los PRST y asignatarios de recursos de identificación, sin considerar las limitaciones regulatorias, técnicas y operativas para actuar de forma eficaz frente al fraude.

Resalta que parece complejo exigir prevención sin que medie una habilitación normativa ni que exista una capacidad operativa para esos efectos, y que, los operadores no cuentan ni con las competencias legales, ni con una instancia de coordinación institucional que les permita bloquear, filtrar o prevenir proactivamente conductas fraudulentas que se materializan a través de sus redes y se ejecutan en cuestión de segundos. Las medidas reactivas no son una falla de diseño, sino el único recurso disponible frente a una amenaza ya ejecutada.

Es importante reconocer las limitaciones del marco regulatorio y operativo que dificultan la implementación de medidas eficientes y oportunas. Por tanto, se proponen las siguientes recomendaciones, con miras a fortalecer un ecosistema más orientado a la prevención que a la reacción:

i. Facultar de forma expresa a los PRST y asignatarios de recursos de numeración para bloquear tráfico o numeración sospechosa de forma preventiva, sin que ello implique riesgos regulatorios por afectación de servicios legítimos.
ii. Implementar un protocolo de bloqueo rápido de URL maliciosas, de origen nacional e internacional, cuando estas sean identificadas con coordinación interinstitucional (CRC, SFC, MinTIC). Algo parecido a lo que ocurre con el bloqueo de URL para prestar servicios de juegos de suerte y azar no autorizados por Coljuegos.

HABLAME

No está de acuerdo con la afirmación según la cual «las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes», ya que desconoce que actualmente tanto los PRST, como los PCA e Integradores Tecnológicos, cuentan con diversas herramientas técnicas, contractuales y operativas para mitigar el fraude en el ecosistema de mensajería.

Así mismo señala que los actores responsables implementan controles de acceso, validaciones de origen, filtros de contenido, trazabilidad, monitoreo automatizado, protocolos de reporte, auditorías periódicas y mecanismos de bloqueo preventivo. Propone entender que el fraude, particularmente el asociado a ingeniería social mediante SMS, es un fenómeno que evoluciona constantemente, adaptándose a nuevas medidas de defensa y explotando cualquier vulnerabilidad en la cadena, incluyendo incluso al propio usuario.

En este contexto, señala que pretender que los agentes del mercado puedan eliminar por completo un delito global, que existe desde antes de la telefonía móvil y que ha mutado desde el correo electrónico hasta el canal SMS, resulta ingenuo e irrealista. El fraude no se erradica, se administra, se reduce, se contiene. Ninguna regulación en el mundo ha podido erradicarlo por completo, ni siquiera en los entornos más controlados.

Por lo tanto, manifiesta que la CRC no puede formular un diagnóstico que parte de una expectativa desproporcionada, como si fuera posible construir un entorno libre de fraude. La regulación debe enfocarse en fortalecer capacidades, fomentar la colaboración entre actores, incentivar buenas prácticas, y permitir la innovación en esquemas de defensa, pero con los pies en la tierra: el fraude muta y seguirá existiendo. Lo razonable es minimizar su impacto.

Respuesta CRC:

Esta Comisión, en cumplimiento de lo dispuesto en el artículo 4 de la Ley 1341 de 2009, y con el objetivo de promover condiciones de seguridad en la prestación de servicios al usuario final, ha incorporado en su marco regulatorio obligaciones específicas para los PRST, PCA e IT asignatarios orientadas a la prevención del fraude, la seguridad informática y las redes.

En este sentido, es importante destacar que, considerando las observaciones planteadas por **ANDI**, **ASOBANCARIA** y **HABLAME** en cuanto a la insuficiencia de las medidas, en la regulación vigente existen disposiciones que obligan a los operadores y asignatarios a implementar herramientas de prevención de fraudes.

Entre estas medidas podemos resaltar disposiciones asociadas a la protección de los derechos de los usuarios de servicios de comunicaciones, tales como el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016, el cual consagra que los operadores tienen la obligación de hacer uso de herramientas tecnológicas para prevenir que se cometan fraudes al interior de sus redes y deben hacer controles periódicos respecto a la efectividad de estos mecanismos. Asimismo, el artículo 2.1.20.1. dispone que el operador deberá informar las políticas de uso razonables y las posibles acciones que se pueden tomar para evitar la comisión de fraudes, así como las condiciones aplicables.

Por su parte, tratándose específicamente de las disposiciones asociadas a recursos de identificación, el artículo 2.1.18.4 de la Resolución CRC 5050 de 2016, señala que los PCA e integradores tecnológicos que sean asignatarios de códigos cortos deberán hacer uso de herramientas tecnológicas para prevenir fraudes a través del envío de mensajes SMS o USSD y efectuar controles periódicos respecto de la efectividad de los mecanismos dispuestos para tal fin.

Asimismo, el artículo 4.2.2.1 de la citada resolución, consagra en cabeza de los PRST la obligación establecer de mutuo acuerdo, conforme a criterios de proporcionalidad y razonabilidad, el uso de herramientas tecnológicas a cargo de cada parte para prevenir fraudes a través de sus respectivas redes, plataformas o sistemas y efectuar controles periódicos respecto de la efectividad de los mecanismos dispuestos para tal fin.

Como se señaló en el documento de formulación del problema, esta Comisión reconoce que los operadores cumplen con los lineamientos mínimos establecidos en la regulación vigente. Sin embargo, los hallazgos evidencian que estas medidas, en muchos casos, se limitan a enfoques operativos y

administrativos, sin incorporar mecanismos robustos de trazabilidad, ausencia de sistemas integrados de prevención y alerta temprana. En relación con las alternativas propuestas por los distintos actores, como la facultad para bloquear tráfico o numeración sospechosa y la implementación de protocolos de bloqueo rápido de URL maliciosas, estas serán consideradas dentro de la revisión que se adelantará de la regulación vigente en aras de adoptar medidas para la mitigación del fraude.

Respecto al comentario de **HABLAME** sobre el alcance del problema, se aclara que, como se indicó en la sección anterior, el presente proyecto regulatorio tiene como objetivo diseñar una estrategia para la prevención y mitigación del contacto a usuarios con fines fraudulentos mediante servicios de voz y mensajes de texto. Además, se contempla la evaluación de acciones educativas dirigidas a los usuarios, con el fin de minimizar el impacto del fraude cibernético en los servicios tradicionales.

Finalmente, si bien tal y como se explicó, actualmente la regulación vigente consagra medidas de gestión y control tendientes a la prevención del fraude, así como obligaciones de monitoreo sobre los mecanismos implementados, con ocasión del desarrollo del presente proyecto regulatorio se adelantará una revisión de las disposiciones relacionadas con recursos de identificación, lo cual permitirá evidenciar oportunidades de modificar o establecer nuevas medidas.

3.3.3. Comentarios a la causa «Desconocimiento de los usuarios sobre privacidad de la información facilita la obtención de datos personales con fines fraudulentos»

ANDI

En su escrito plantea que la CRC otorga un énfasis excesivo al desconocimiento de los usuarios sobre la privacidad de la información como causa de los fraudes digitales. Si bien la falta de conciencia puede incidir, los ataques de ingeniería social se caracterizan por manipular rasgos humanos como la confianza o el deseo de ayudar, adaptándose incluso a usuarios con buen conocimiento en seguridad digital.

Indica que, el aumento de ciberdelitos desde 2020, reportado por la Fiscalía y la Corporación Excelencia en la Justicia, muestra que la existencia de normas como la Ley 1266 de 2008 y la Ley 1581 de 2012 no ha sido suficiente para contener el fenómeno; lo cual refleja que no se trata únicamente de desconocimiento normativo, sino de una amenaza dinámica, cada vez más sofisticada y con mayor volumen.

Señala que, factores adicionales explican este crecimiento: la actividad de grupos de amenazas en Colombia, el auge del comercio electrónico y la banca digital —con un crecimiento anual del 27% de las billeteras virtuales en Latinoamérica—, la desactualización de sistemas, la fuga de talento en ciberseguridad y la rápida digitalización de sectores como el financiero, que amplía la superficie de ataque.

Afirma que, a pesar de los lineamientos emitidos por la Superintendencia Financiera en materia de ciberseguridad, el incremento sostenido de fraudes digitales evidencia que estas medidas no han tenido impacto disuasorio suficiente. En este sentido, aunque la educación y concientización de los usuarios es importante, no constituye un mecanismo capaz de contrarrestar por sí sola los escenarios de ataque, dado que la ingeniería social evoluciona constantemente y explota vulnerabilidades más allá del nivel de conocimiento del usuario.

ASOBANCARIA

Sugiere tener en cuenta que, si bien la socialización y concientización de los usuarios sobre los riesgos asociados a fraudes digitales puede prevenir escenarios de ataques cibernéticos, la ingeniería social tiene muchas variantes en las que el usuario puede caer desprevenidamente en estos escenarios.

HABLAME

Manifiesta que más que enfocarse únicamente en endurecer la regulación sobre los actores del mercado, la CRC debe liderar, impulsar y coordinar campañas nacionales de educación digital y alfabetización en ciberseguridad orientadas al usuario final, que incluyan a operadores, entidades financieras, comercios y sector público, pues sin usuarios informados, no hay ecosistema seguro posible.

Respuesta CRC:

Frente a los comentarios de la **ANDI**, es importante aclarar que, la CRC de ninguna manera considera que el desconocimiento por parte de los usuarios es la única causa para la materialización del problema formulado, y por ende que la educación a los usuarios de servicios de voz y mensajes de texto, podría ser una solución integral que conlleve a prevenir y a mitigar la comisión de fraude a través de los referidos servicios.

Es así como, con ocasión del desarrollo del presente proyecto regulatorio, si bien se evaluará la pertinencia de implementar acciones educativas que aumenten el conocimiento de los usuarios en la prevención contra el fraude cibernético, también se analizará la viabilidad e idoneidad de la implementación de herramientas regulatorias que mitiguen el contacto con los usuarios con fines fraudulentos, así como de la definición de líneas de acción para la construcción de una estrategia nacional conjunta de prevención contra el referido fraude; sin obviar por supuesto, la necesidad de revisar e identificar aspectos del régimen de recursos de identificación vigente que sean susceptibles de modificación.

En relación con los comentarios formulados por **ASOBANCARIA**, esta Comisión coincide con su posición, en el sentido que la ingeniería social tiene muchas variantes en las que el usuario puede caer desprevenidamente en estos escenarios, por lo cual, en desarrollo de este proyecto regulatorio, pretende determinar las acciones pertinentes desde el ámbito de su competencia para prevenir y mitigar el contacto a los usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de

texto. Ahora bien, en atención a los comentarios esta situación planteada como causa, será considerada como una consecuencia del problema identificado, pues coincide la CRC que la misma se deriva de una baja efectividad de las herramientas regulatorias vigentes para la prevención del contacto con los usuarios.

Finalmente, respecto del comentario de **HABLAME**, la CRC reitera que precisamente uno de los objetivos de este proyecto, es la definición de 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, en la cual se espera se pueda contar con la participación de todos los agentes vinculados.

3.3.4. Comentarios a la causa «Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto»

ANDI

Señala en su escrito que la falta de articulación interinstitucional efectiva es una de las causas estructurales del problema y constituye un elemento clave para una estrategia coordinada contra el fraude cibernético. Resalta la necesidad de implementar medidas que permitan terminar relaciones con PCA o IT reincidentes en el envío de mensajes fraudulentos.

Recomienda:
- Automatizar la asignación y recuperación de recursos de identificación mediante plataformas interoperables.
- Establecer criterios de uso seguro de dichos recursos, además del uso eficiente.
- Incluir cláusulas de revocación inmediata ante evidencia de fraude.
- Permitir auditorías cruzadas entre operadores, CRC y entidades afectadas.
- Imponer medidas regulatorias a PCA e IT, en especial a quienes enrutan tráfico potencialmente fraudulento.
- Incorporar herramientas que permitan a los PRST bloquear tráfico proveniente de PCA e IT vinculados con fraude.

Respuesta CRC:

Tal como se expuso en la formulación del problema, la CRC considera que la falta de articulación interinstitucional constituye una de las causas estructurales que limita la efectividad de las acciones para prevenir el fraude mediante llamadas y mensajes de texto en la medida que si bien la normativa vigente establece que tanto los PRST y los asignatarios de códigos cortos deben implementar mecanismos y herramientas para la prevención de fraude a través del uso de numeración; existen escenarios en los que es necesaria la trazabilidad de los contenidos enviados al usuario para las

autoridades que en el ejercicio de sus competencias lo requieran, como son la Fiscalía General de la Nación, la Superintendencia de Industria y Comercio (SIC), entre otras.

En cuanto a las recomendaciones planteadas en el comentario, estas serán evaluadas dentro del ámbito de las facultades de la CRC y valoradas en el marco del proyecto, sin perder de vista que aún persisten retos que requieren una estrategia nacional efectiva, coordinada y transversal que involucre el fortalecimiento de relaciones entre autoridades públicas, sector privado, sociedad civil y operadores de telecomunicaciones, a fin de generar respuestas integrales frente a fenómenos como el fraude digital y la ingeniería social, cuyas técnicas evolucionan de manera acelerada y requieren soluciones dinámicas, conjuntas y técnicamente sólidas.

3.4. Comentarios sobre las consecuencias del problema

ANDI

En su escrito señala que el sector financiero ha enfrentado crecientes costos por compensaciones, atención a incidentes y campañas educativas, mientras que los PRST realizan esfuerzos para identificar mensajes fraudulentos enviados por PCA e IT. A esto se suma un régimen de responsabilidad desarticulado y la obligación de mantener relaciones con actores que difunden fraude, lo que afecta la confianza de los usuarios, limita el uso de canales digitales y repercute en la inclusión financiera y la eficiencia operativa. Expone que se trata de un desafío de alcance global, no exclusivo de Colombia ni de la región.

ANDESCO

Sugiere que se deben adicionar las siguientes consecuencias:
i. Incremento en los costos operativos de mitigación. Las empresas deben invertir en soluciones tecnológicas como firewalls, IA, monitoreo de tráfico, auditorías y personal especializado para suplir la ausencia de consecuencias para el PCA o IT infractor por el envío de mensajes con contenido presuntamente fraudulento.
ii. Continuidad en la relación de acceso entre PCA y/o IT y PRSTM.

COLCERT

Señala que, las consecuencias engloban la problemática que genera el fraude a través de mensajes y SMS.

COMCEL

Sugiere que se deben adicionar las siguientes consecuencias:
i. Incremento en los costos operativos de mitigación. Las empresas deben invertir en soluciones tecnológicas como firewalls, IA, monitoreo de tráfico, auditorías y personal especializado para suplir la

ausencia de consecuencias para el PCA o IT infractor por el envío de mensajes con contenido presuntamente fraudulento.
ii. Continuidad en la relación de acceso entre PCA y/o IT y PRSTM.

ETB

Indica que, aunque las consecuencias expuestas en el documento se relacionan directamente con el problema identificado, son insuficientes para reflejar la verdadera magnitud y complejidad de los impactos generados por el actual enfoque regulatorio fragmentado. Señala que, dicho enfoque provoca efectos como la imposición de nuevas obligaciones a los PRST, el incentivo a la migración de actividades ilícitas hacia plataformas no reguladas, y el deterioro de la confianza del usuario en todo el sector de telecomunicaciones.

Como consecuencias adicionales propone:
-Crecimiento sostenido del ecosistema del fraude, que se adapta rápidamente a vacíos regulatorios y tecnológicos.
-Sobrecarga de responsabilidad sobre los PRST, que deben asumir los costos operativos, reputacionales y regulatorios sin tener control sobre el origen de muchas prácticas fraudulentas.
-Debilitamiento de la seguridad digital nacional, al carecer de trazabilidad y mecanismos de respuesta articulada frente al fraude transfronterizo.
-Erosión de la confianza en el entorno digital en su conjunto, que afecta no solo a las telecomunicaciones, sino también a servicios financieros, estatales y de comercio electrónico.

CRISTÓBAL FUENTES

Señala que las consecuencias tienen relación directa con la materialización del problema debido al aumento del uso indebido de códigos cortos con fines fraudulentos y no para su uso original la cual es consecuencia directa de la ausencia de normas más específicas permitiendo así a actores maliciosos explotar estos códigos para el *smishing* y el robo de identidad. Así también la falta de medidas preventivas aumenta el riesgo que los derechos de los usuarios a la protección de datos personales, el secreto de las comunicaciones y la protección contra la publicidad indebida sean vulnerados.

MDK

Afirma que las consecuencias descritas «pérdida de confianza, aumento del fraude, daños económicos, limitada capacidad de respuesta por los operadores» están relacionadas con efectos directos de la falta de una estructura técnica y regulatoria capaz de prevenir el fraude de forma sistemática. Indica que tales relaciones causales también se han observado en otros mercados antes de la implementación de sistemas obligatorios de registro y verificación, por ejemplo, el modelo MDK en Alemania.

Añade otras consecuencias relevantes desde la práctica:

- Retiro de marcas legítimas del canal por falta de seguridad.
- Fragmentación de estructuras de cumplimiento entre operadores.
- Daños reputacionales para los operadores.
- Debilitamiento de estrategias nacionales de transformación digital.

Propone la inclusión de la siguiente consecuencia:

«La falta de control sobre actores y contenidos en los servicios móviles de comunicación no solo aumenta el riesgo de fraude y la pérdida de confianza, sino que también debilita a largo plazo el canal como soporte de innovación digital y como plataforma económica para marcas, entidades públicas y consumidores.»

Sugiere ampliar el análisis para incluir impactos económicos, regulatorios y reputacionales, y reafirma que un modelo de registro obligatorio, transparente e interoperable puede mitigar estos riesgos de forma efectiva.

PLINTRON

Señala que es una buena aproximación a los detalles del problema, pero se ve que las soluciones ya fueron evadidas con anterioridad. Considera que, la idea es reforzar una estrategia más allá de los sistemas informáticos de los actores.

SIC

Indica que, desde el punto de vista de protección de los usuarios, la transgresión a sus derechos se está presentando tanto por el contacto a los usuarios con fines fraudulentos, como mediante conductas fraudulentas que se ejecutan por medio de servicios móviles sin que exista contacto con el usuario.

Reitera que debe existir un deber adicional a los prestadores de servicios móviles de proteger los derechos y los datos personales de los usuarios de utilizan sus redes. Considera que, la ausencia de medidas regulatorias, así como la falta de mecanismos eficaces de autocontrol y gestión contribuye al debilitamiento de la confianza de los usuarios en los servicios de telecomunicaciones, especialmente para los servicios móviles, lo cual puede derivar en que los usuarios eviten cuando es posible el uso de las redes móviles para realizar sus principales transacciones.

Señala que, en un ecosistema digital, la confianza en las redes de telecomunicaciones, así como en los medios electrónicos es fundamental y, la falta de prevención y mitigación de conductas fraudulentas por medio de los servicios móviles lleva a un estancamiento de la evolución de dicho ecosistema.

UNIVERSIDAD EXTERNADO

Considera que las consecuencias descritas en el documento están debidamente relacionadas con la materialización del problema identificado, pues reflejan impactos directos tanto en el funcionamiento del sector como en la experiencia y confianza de los usuarios. Sin embargo, sugiere incluir, como consecuencia adicional, la afectación de la reputación del país como destino digital, la cual aunque es indirecta, resulta relevante porque la persistencia de prácticas de fraude cibernético no controladas puede generar percepciones negativas en inversionistas, empresas tecnológicas y plataformas internacionales, afectando el posicionamiento del país como un entorno seguro y confiable para el desarrollo de servicios digitales e innovaciones basadas en telecomunicaciones móviles.

Manifiesta que, incluir esta dimensión contribuiría a una caracterización más completa del problema, evidenciando que sus impactos trascienden el ámbito estrictamente económico o individual de los usuarios, y pueden incidir en la competitividad y proyección internacional del ecosistema digital colombiano.

TIGO

Afirma que, si bien las consecuencias señaladas en el documento pueden representar un primer acercamiento, es importante profundizar en ellas para reflejar de forma más completa la dimensión del problema considerando incluir el impacto causado en el servicio de internet móvil.

Sugiere incluir la siguiente consecuencia: «Crecimiento sostenido de las modalidades de fraude dirigidos a los usuarios a través de los servicios móviles». Al respecto argumenta que, si bien se observa una problemática pronunciada en los casos de fraude por la modalidad de *smishing*, esta no es la única modalidad que genera consecuencias, modalidades como el *Robocall*, están generando un impacto relevante en las empresas y usuarios. Por lo cual, señala que, al incluir el servicio de internet móvil en el alcance del proyecto, se pueden abordar de una forma más amplia las medidas para los casos de *phishing* y otras modalidades que se presentan sobre el servicio de internet.

Respuesta CRC:

Con respecto a los comentarios de **ANDI**, **ANDESCO** y **COMCEL** en donde manifiestan que la problemática identificada tiene consecuencias en términos de incremento de costos asociados a compensaciones, atención de incidentes, campañas educativas y la adopción de soluciones tecnológicas, y de forma complementaria, los comentarios de **ETB** y **MDK** que señalan el crecimiento sostenido del ecosistema de fraude y sobrecarga de responsabilidad como consecuencias adicionales, es importante indicar que el documento de formulación publicado reconoce que el fraude genera cargas operativas y económicas significativas para los agentes del sector y para sectores conexos como el financiero. En particular, esta visión se materializa en la consecuencia establecida en el árbol de problema como «Afectaciones a empresas y organismos públicos»[11], así como en la sección 4.1.2. del mismo documento,

[11] CRC (2025). Documento de formulación del problema del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Página 42. https://crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf

denominada «Requerimiento de información sobre el fraude cibernético por medio del servicio de llamadas de voz y SMS»[12] en la cual se logra establecer una valoración económica de las actividades y afectaciones atribuibles al fraude mediante el envío de SMS o llamadas de voz desde tres conceptos de gasto: prevención, impactos y respuesta frente al fraude cibernético.

En este contexto, es necesario indicar que en el marco de las alternativas regulatorias postuladas se valorará la pertinencia de mecanismos de trazabilidad y verificación de remitentes incluyendo criterios que internalicen tantos los costos de mitigación, como los beneficios derivados de la prevención y la eficiencia en la respuesta, en línea con el enfoque de protección al usuario.

Frente a las observaciones expresadas por la **ANDI** en donde se señala su preocupación dada su visión de un régimen de responsabilidad desarticulado y, además, en consistencia con lo también expresado por **COMCEL**, en relación con la continuidad de relaciones con actores que difunden fraude, es necesario manifestar que el ejercicio regulatorio desarrollado por esta Comisión se ha fundamentado en el objetivo de alinear incentivos y responsabilidades a lo largo de la cadena de valor del canal de mensajería y de voz. Sin perjuicio de lo anterior, la redefinición de deberes, cargas y consecuencias para cada agente exige un análisis integral de la relación de acceso entre PRSTM y PCA/IT, el régimen de protección de usuarios y la administración de los recursos de identificación. En consistencia, en la sección 3.2 de este documento se propone la posibilidad de establecer obligaciones y responsabilidades diferenciadas y, cuando aplique, compartidas, así como incluir criterios como la reincidencia, como elemento para tener en cuenta en la administración y recuperación de recursos de identificación.

En relación con la observación de la **ANDI** y **COLCERT** en donde manifiesta que el fraude cibernético representa un desafío de alcance global, que no es exclusivo de Colombia ni de la región, esta Comisión reconoce que la dimensión del problema identificado sobre pasa el ámbito de aplicación de la política regulatoria desarrollada por esta entidad. En este contexto, se refuerza la necesidad de adoptar medidas compatibles con las mejores prácticas internacionales que se ajusten al marco regulatorio colombiano, conforme con lo dispuesto en la Ley 1341 de 2009 y desarrollado en la Resolución CRC 5050 de 2016. De forma consistente, en el marco de las alternativas presentadas en la sección 63.2 para abordar la temática asociada a «Acciones educativas que aumenten el conocimiento de los usuarios» de este documento se postulan alternativas en donde se propone acciones para abordar el fraude desde una visión de articulada con otras entidades del Estado.

Sobre la recomendación realizada por **ETB**, **MDK**, **SIC** y **TIGO** por medio de la cual sugieren la necesidad de profundizar en los impactos dada la insuficiencia en las consecuencias y frente a los comentarios de la **SIC** y la **UNIVERSIDAD EXTERNADO**, que señalan la pérdida de confianza y afectación a la reputación de país, esta Comisión, en primera medida destaca que el riesgo de migración de actividades ilícitas hacia plataformas no reguladas es un impacto que se puede derivar de la problemática identificada. Sin embargo, es preciso considerar que este elemento se incluye en la causa «Dificultad en la identificación y rastreo de los ataques cibernéticos», en la cual se reconoce la dinámica

[12] Ibid. Página 29.

evolutiva de esta problemática y la capacidad de los actores maliciosos de adaptarse rápidamente a los controles regulatorios y tecnológicos, trasladando sus operaciones hacia canales alternativos menos vigilados, como las aplicaciones OTT, el tráfico internacional o el internet móvil. En segunda medida, en línea con la respuesta que trata sobre las observaciones allegadas sobre la problemática identificada en la sección 3.2, el documento de formulación[13] del actual proyecto regulatorio incorpora la pérdida de confianza y las afectaciones a empresas y organismos públicos como consecuencias derivadas en el árbol del problema, lo cual refleja que la caracterización inicial contempla los principales impactos señalados por los agentes.

Frente a la observación de **TIGO** en donde señala el crecimiento sostenido de modalidades de fraude y la necesidad de incorporar el servicio de internet móvil dentro del alcance del proyecto, es necesario manifestar que la CRC coincide en la necesidad de actualizar permanentemente el diagnóstico sobre esta problemática, que como se indicó en anteriormente, el fenómeno evoluciona rápidamente, por lo que es pertinente considerar medidas adaptativas y basadas en riesgo, así como la necesidad de reforzar la articulación con autoridades competentes para tratamiento de fraude transfronterizo y de nuevas técnicas de suplantación. Ahora, con respecto a la solicitud de incluir el impacto del internet móvil dentro del alcance del proyecto, es preciso indicar que, si bien el proyecto se centra en recursos de identificación bajo administración de la CRC, se reconoce que el internet móvil actúa como habilitador transversal. En este sentido, las alternativas regulatorias propuestas en este documento incluyen herramientas que tienen como fin limitar el direccionamiento a sitios fraudulentos, aplicaciones no verificadas o contenidos que faciliten la suplantación, cuidando la consistencia con las competencias regulatorias.

Por último, con respecto a la observación de **PLINTRON** en donde recomienda reforzar la estrategia más allá de los sistemas informáticos de los actores, es importante reiterar que la adopción de mecanismos específicos, como por ejemplo herramientas de autenticación o incorporación de estándares técnicos, requiere de la aplicación del AIN que evalúe viabilidad técnica, legal y económica y su consistencia con el problema regulatorio, priorizando interoperabilidad, trazabilidad y cooperación como ejes de política.

3.4.1. Comentarios a la consecuencia «Pérdida de confianza en los servicios de telecomunicaciones»

ASOMÓVIL

Expone en su escrito que el incremento de fraude por smishing y spoofing ha crecido de forma alarmante, afectando a usuarios y operadores móviles mediante engaños que roban datos o dinero, generan desconfianza y aumenta las PQR a los operadores de telecomunicaciones. De ahí que, aunque el uso de voz y SMS disminuye, el fraude en estos canales sigue en alza, con delincuentes que

[13] Ibid. Página 42.

enmascaran llamadas internacionales como nacionales para inducir al error y cometer delitos, debilitando aún más la confianza en las comunicaciones.

Respuesta CRC:

Frente al comentario, en el documento de formulación del problema se comparte la preocupación expresada frente al incremento de prácticas fraudulentas como el *smishing* y el *spoofing*, que afectan tanto a usuarios como a operadores y generan un deterioro en la confianza hacia los servicios de telecomunicaciones. Este señalamiento confirma la pertinencia de la consecuencia identificada en el análisis, dado que la pérdida de confianza constituye uno de los impactos más graves del fraude, en la medida en que afecta la percepción de seguridad de los usuarios, incrementa las PQR y compromete la sostenibilidad de los servicios TIC en el país.

Bajo este contexto, el proyecto incorpora esta perspectiva como un elemento clave para orientar las medidas propuestas, de manera que no solo se fortalezcan los mecanismos de control frente al fraude, sino que se contribuya a restablecer y proteger la confianza de los usuarios en los servicios de voz y SMS.

3.5. Comentarios sobre los grupos de valor

ANDI

Propone que se amplie los grupos de valor, incluyendo no solo a las entidades financieras sino también a las Fintech, dado su alto nivel de exposición al fraude cibernético en servicios móviles, cuyo impacto compromete la confianza de los clientes y la estabilidad del sistema financiero. Asimismo, sugiere incorporar a entidades como MinTIC, la Fiscalía, la SFC, la Superintendencia de Economía Solidaria y el Ministerio de Hacienda, entre otras, para asegurar una coordinación interinstitucional que establezca reglas homogéneas y permita un abordaje integral de la problemática.

ANDESCO y COMCEL

Indican que se deben considerar dentro de los grupos de valor, los siguientes:

-Plataformas de mensajería y agregadores internacionales: Manifiesta que, muchos fraudes se originan desde plataformas o rutas internacionales (A2P SMS, OTTs, etc.), por lo cual la regulación debe considerar cómo se integran estos actores en la cadena de valor y cómo se les puede exigir trazabilidad, autenticación de remitentes, responsabilidad y cumplimiento de normas locales.

-Entidades del sector educativo y académico (universidades, centros de investigación): Señala que pueden apoyar en el diseño de campañas de sensibilización digital y estudios de impacto del fraude, y que, su participación puede fortalecer la base técnica y metodológica de las medidas regulatorias.

COLCERT

Sugiere la inclusión del Coordinador Nacional de Seguridad Digital (Es quien puede articular medidas y controles de seguridad digital para prevenir el fraude); y la Dirección de Vigilancia Inspección y Control (la que tiene como obligaciones, el cumplimiento del régimen de telecomunicaciones y vigila la prestación eficiente y adecuada de los servicios de telecomunicaciones).

CRISTÓBAL FUENTES

Considera que los grupos de valor mencionados son los afectados directamente, por lo cual no hacen falta otros grupos de valor.

COMCEL

Sugiere la adición de los medios de comunicación y plataformas digitales, pues argumenta son canales clave para la difusión de alertas de fraude, campañas de prevención y educación al usuario, y que, su inclusión puede potenciar el alcance de las estrategias pedagógicas propuestas por la CRC.

ASOBANCARIA

Sugiere incluir como grupo de valor no solo a las entidades financieras sino también a las *Fintech*, dado que son actores altamente expuestos al fraude cibernético mediante servicios móviles. Indica que, para estas, los canales de contacto con clientes (SMS, llamadas, notificaciones, entre otros) son esenciales para la operación, y cualquier afectación en su seguridad impacta directamente la relación con el cliente y la estabilidad del ecosistema financiero.

Adicionalmente, sugiere incluir dentro de los grupos de valor identificados a actores clave como lo son la SFC, la Superintendencia de Economía Solidaria y el Ministerio de Hacienda y Crédito Público, entre otros, con el fin de lograr una coordinación interinstitucional alineada y coordinada, que someta a sus vigilados a reglas homogéneas y de aplicación igualitaria a las Telcos y, de esa forma abordar de manera integral la problemática, conectando inclusive con Fiscalía y otros agentes que doten de herramientas a todos los actores.

AVAL

Considera que el documento incluye los principales grupos de valor del sector de telecomunicaciones. Sin embargo, sugiere la inclusión de empresas de ciberseguridad como aliados tecnológicos, asociaciones de protección al consumidor digital y medios de comunicación en su rol educativo y como alerta temprana.

ETB

Indica que, el enfoque adoptado en el documento de la CRC identifica adecuadamente algunos grupos de valor, como los PRST y los usuarios, pero omite actores esenciales que no solo participan activamente en el ecosistema, sino que también son responsables, directa o indirectamente, de la gestación de escenarios de fraude. Entre ellos se encuentran los PCA, *carriers* internacionales, plataformas OTT, autoridades judiciales y de protección al consumidor (como la Fiscalía, la SIC y la SFC), proveedores de servicios en la nube, que alojan infraestructura para operaciones fraudulentas, agregadores internacionales de SMS que operan sin supervisión local, y autoridades regulatorias extranjeras como la FCC, CRTC y OFCOM. Considera que, la inclusión de estos actores es indispensable si se pretende un abordaje comprehensivo y balanceado de la problemática, evitando que la carga de las soluciones recaiga exclusivamente sobre los PRST.

HÁBLAME

Considera que deben incluirse los siguientes grupos de valor:

- Proveedores de Servicios de Internet (ISP): dado que tienen una responsabilidad directa en la prevención del acceso a contenidos maliciosos, ya que es a través de su infraestructura que se materializa el ingreso de los usuarios a enlaces fraudulentos asociados a campañas de phishing, smishing o suplantación de identidad.
- Policía Nacional y Fiscalía General de la Nación: Estas autoridades deben ser actores estratégicos en la identificación, investigación y judicialización de estructuras criminales que operan a través de servicios móviles. La experiencia acumulada por sus unidades especializadas en cibercrimen y delitos económicos es clave para alimentar el diseño regulatorio con evidencia, alertas tempranas y mecanismos de respuesta ante nuevas modalidades de fraude.
-Instituto Nacional Penitenciario y Carcelario – INPEC: La evidencia señala que muchas llamadas extorsivas y mensajes de texto fraudulentos se originan desde centros carcelarios, haciendo uso de equipos y líneas móviles ilegales. La inclusión del INPEC como actor regulatorio permitirá articular medidas como el uso de inhibidores de señal, el control y bloqueo selectivo de dispositivos, y la identificación de patrones de actividad sospechosa.

MDK

Considera fundamental involucrar a otros grupos estratégicos en el proceso de desarrollo e implementación del proyecto regulatorio, especialmente en lo relacionado con la interoperabilidad, la estandarización, la ejecución técnica y la aceptación por parte del mercado.

Recomienda incluir operadores de plataformas de registro centralizadas, entidades de verificación, Marcas, anunciantes, proveedores de servicios, Proveedores de tecnología, plataformas API y Organizaciones de consumidores y de protección de datos.

Indica que un sistema moderno, eficaz y confiable contra el fraude en el ámbito móvil no puede basarse únicamente en el control técnico de los MNOs o la regulación estatal, pues requiere una colaboración

abierta y coordinada entre todos los actores del ecosistema. Afirma que, en mercados donde se busca recuperar la confianza en la comunicación digital, este enfoque multiactor resulta clave para el éxito.

PLINTRON

Afirma que, hay una parte de los actores que hacen falta y son los jugadores de redes sociales y Big Tech, pues las actuales formas de evasión usan estos actores.

SIC

Sugiere que desde el inicio del proyecto, se involucre a todos aquellos actores vinculados al CONPES 3995 de 2020 *Política Nacional de Confianza y Seguridad Digital* y a la *Estrategia Nacional de Seguridad Digital 2025 -2027*.

Asimismo, recomienda incluir en los grupos de valor a Entidades del sector financiero, como las FINTECH, entendidas estas como empresas que buscan innovar en el sector financiero a través de soluciones digitales, prestan servicios financieros a usuarios finales y que su principal medio de comunicación con los usuarios son los servicios móviles.

Considera pertinente valorar la inclusión de las agremiaciones del sector financiero en los grupos de valor, en función de su representatividad y el rol que desempeñan en la articulación de prácticas y estándares dentro del ecosistema financiero.

TIGO

Sugiere incluir a los siguientes grupos de valor para lograr una estrategia integral y sostenible de mitigación de este flagelo a todos los actores que intervienen en las redes móviles:

-OTT: Indica que, estos actores juegan un papel fundamental en el ecosistema de seguridad cibernética, ya que diversas modalidades de fraude, especialmente aquellas basadas en ingeniería social se ejecutan a través de sus plataformas.

-Entidades del ecosistema de ciberseguridad del Estado: Afirma que, incluir a actores como el Centro Cibernético de la Policía Nacional, la Fiscalía General de la Nación, ColCERT del MinTIC, y eventualmente la UIAF, permitiría fortalecer los canales de intercambio de información, construir alertas tempranas y mejorar la trazabilidad de eventos.

-Titulares de datos y representantes de derechos digitales: Señala que, las personas afectadas no siempre son técnicamente usuarios de los operadores móviles, pues muchas veces el fraude alcanza a ciudadanos sin una relación contractual directa (niños, adultos mayores,turistas, etc.), lo que justifica involucrar a asociaciones de consumidores, defensores de derechos digitales, y expertos en protección

de datos personales, para garantizar un enfoque centrado en las personas, con especial énfasis en los grupos más vulnerables.

UNIVERSIDAD EXTERNADO

Sugiere incluir a las plataformas tecnológicas integradoras (proveedores de soluciones SMS/USSD); empresas de ciberseguridad que pueden ofrecer herramientas de detección y respuesta ante fraudes; organismos judiciales y de control; y, la academia y sociedad civil.

Respuesta CRC:

Con base en los comentarios recibidos, esta Comisión presenta una tabla complementaria que incorpora nuevos grupos de valor identificados por los actores del sector. Es importante aclarar que su inclusión en el análisis no implica que las medidas regulatorias propuestas en el marco de este proyecto les sean aplicables.

No.	Grupo de valor identificado	Descripción	Interés en el proyecto	Impacto del proyecto
10	Fintech	Empresas que ofrecen servicios financieros digitales mediante soluciones tecnológicas.	Alto. Similar a las entidades del sector financiero, dada su exposición al fraude en canales móviles.	Alto. Podrían beneficiarse indirectamente de medidas que fortalezcan la seguridad en los canales de comunicación.
11	Otras entidades (MinHacienda, Fiscalía, Policía, INPEC, SuperSociedades)	Entidades públicas con funciones en seguridad, justicia, control y política económica.	Medio. Su articulación puede fortalecer la respuesta institucional frente al fraude.	Medio. Las medidas regulatorias pueden ser insumo para acciones coordinadas en sus respectivos ámbitos.
12	Entidades del sector educativo, académico y medios de comunicación.	Instituciones educativas, centros de investigación y medios de difusión.	Medio. Pueden apoyar en la sensibilización, formación y divulgación de buenas prácticas.	Medio. Su participación puede potenciar el alcance de las estrategias educativas y preventivas.
13	Marcas y anunciantes	Empresas que ofrecen/utilizan servicios móviles como canales comerciales y/o publicitarios.	Alto. Interés en que los canales móviles sean seguros y confiables para proteger reputación de su modelo de negocio.	Alto. Las medidas que fortalezcan la seguridad en los servicios móviles pueden mejorar la confianza del consumidor y reducir el riesgo de suplantación asociado a sus marcas.
14	Empresas de ciberseguridad	Empresas especializadas en servicios de consultoría, pruebas de penetración y monitoreo de seguridad para proteger las infraestructuras	Medio. Interés en los lineamientos regulatorios para alinear sus soluciones con las necesidades del sector y ofrecer servicios	Medio. Aunque no son destinatarios directos de la regulación, pueden verse involucrados como aliados técnicos en la implementación de medidas

		digitales de las empresas contra ciberataques.	complementarios a los agentes regulados.	de prevención y monitoreo de fraude.
15	Otros agentes de interés	Actores privados o internacionales que participan en el ecosistema digital sin regulación (Agregadores internacionales, plataformas tecnológicas, OTT, Big Tech, etc).	Bajo. Aunque pueden tener un rol técnico en los servicios tradicionales, no tienen una relación directa con la posible regulación ni están obligados a su cumplimiento.	Bajo. Estos agentes no se encuentran regulados y su participación dependerá de su voluntad o articulación por parte de los demás agentes.

En cuanto a las asociaciones de protección al consumidor, defensores de derechos digitales y expertos en protección de datos personales, se considera que sus intereses están representados institucionalmente a través de la SIC como autoridad competente de protección al consumidor y datos personales, ya incluida como grupo de valor en el documento de formulación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4. ÁRBOL DEL PROBLEMA AJUSTADO

En línea con lo expuesto en el acápite 3.3 del presente documento, con ocasión de los comentarios allegados frente al árbol del problema inicialmente publicado, esta Comisión evidenció la necesidad de modificar el alcance de la causa preliminarmente denominada «Desconocimiento de los usuarios sobre privacidad de la información facilita la obtención de datos personales con fines fraudulentos» pues coincide con las observaciones, según las cuales la materialización del problema no solo ocurre por el desconocimiento de los derechos que le asisten en relación con el tratamiento de sus datos personales; sino que también se debe reconocer la ausencia de información y conocimiento de estos agentes respecto de las diferentes modalidades de ataque y las acciones de prevención y respuesta que deben tomar.

Es así como, se procede a modificar la referida causa, la cual será considerada una consecuencia del problema y quedará así: «Desconocimiento de los usuarios respecto de la seguridad y privacidad de la información, de las modalidades de ataque y de sus posibles acciones de prevención y mitigación; facilita la obtención de información y datos personales, así como la comisión de fraudes»

Asimismo, tal y como se explicó en el acápite 3.2 del presente documento, el problema inicialmente planteado será modificado, en tanto si bien las herramientas regulatorias vigentes no son suficientes para prevenir el contacto a los usuarios con fines fraudulentos, es necesario reconocer que el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, actualmente contempla obligaciones en cabeza de los PRST para prevenir estas acciones fraudulentas y para adoptar mecanismos de verificación de la identidad del usuario.

De acuerdo con lo anterior, el problema a ser resuelto con ocasión del presente proyecto regulatorio quedará así: «Baja efectividad de las herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto».

En la siguiente ilustración se presenta el correspondiente árbol de problema con la incorporación de los ajustes previamente enunciados.

Fuente: Elaboración CRC

El problema, así como las causas y consecuencias expuestas en esta gráfica, se encuentran desarrolladas en el documento de formulación del problema publicado con ocasión del presente proyecto regulatorio[14]

5. OBJETIVOS DEL PROYECTO

5.1. 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.

5.2. Objetivos específicos

a) 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.

[14] 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

b) Evaluar la implementación de herramientas regulatorias que mitiguen el contacto a usuarios con fines fraudulentos, teniendo en cuenta su viabilidad técnica y económica.
c) Determinar la necesidad de implementar acciones educativas que aumenten el conocimiento de los usuarios en la prevención contra el fraude cibernético.
d) 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.

6. EXPERIENCIAS INTERNACIONALES

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.

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; y,
iii. Ejercer control de contenidos.

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:** 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.
3. **Cortafuegos (Firewall) de voz:** Consistente en implementar sistemas informáticos que permiten 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 deben realizar los Agregadores de SMS sobre la identidad y los antecedentes de sus clientes.
3. **Registro de Identificación (ID) de Remitentes:** Las organizaciones legítimamente constituidas que deseen remitir SMS publicitarios o realizar algún tipo de notificación comercial a sus usuarios, deben registrarse y acceder a los identificadores alfanuméricos que utilizarán para su envío.

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 siguiente Tabla 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 2. 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[15]	SI	Si					Si	Si	
Estados Unidos			Si						
India[16]							Si		
Irlanda	Si	Si		Si		Si	Si		
Jordania[17]									
Malasia									Si
Polonia	Si	Si					Si	Si	
Portugal	Si	Si							
Singapur[18]							Si	Si	
Reino Unido	Si	Si[19]			Si	Si[20]	Si[21]	Si[22]	

[15] 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.

[16] 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.

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

[18] 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 comprobará el incumplimiento de alguna de las directrices definidas para combatir el fraude.

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

[20] 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.

[21] 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.

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

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7. ALTERNATIVAS REGULATORIAS

En atención a los aportes y observaciones recibidos durante la consulta pública puesta a consideración de los interesados junto con el Documento de Formulación del Problema, se revisaron todas las propuestas y aportes remitidos por los diferentes actores involucrados en el proceso.

Como resultado de este análisis participativo, y teniendo en cuenta las causas y consecuencias plasmadas en el árbol del problema ajustado, la CRC ha estructurado un conjunto de alternativas regulatorias agrupadas en cuatro grandes temáticas, cada una dirigida a abordar causas y consecuencias específicas del problema identificado. Estas temáticas comprenden: (i) la mitigación del contacto fraudulento a usuarios a través de los servicios móviles tradicionales de mensajes cortos de texto (SMS); (ii) la mitigación del contacto fraudulento mediante los servicios tradicionales de voz; (iii) el fortalecimiento de la educación y la capacidad de los usuarios para identificar y prevenir prácticas fraudulentas; y (iv) la revisión y simplificación normativa del régimen de administración de los recursos de identificación, con el fin de dotarlo de herramientas que contribuyan a la prevención y control del fraude.

Cada temática general se desarrolla a través de subtemáticas específicas que abordan aspectos críticos como la trazabilidad y control de originadores de contenido, la diferenciación y gestión de numeración comercial y publicitaria, la estandarización de mecanismos de bloqueo y autenticación de llamadas, la articulación de plataformas de monitoreo y alerta, y la implementación de acciones pedagógicas y de reporte ciudadano. Las alternativas regulatorias propuestas en cada caso han sido diseñadas para responder a las debilidades estructurales del ecosistema móvil, considerando la viabilidad técnica, operativa y jurídica, así como la necesidad de coordinación interinstitucional y la protección efectiva de los derechos de los usuarios.

En este sentido, el presente capítulo refleja de manera sistemática las alternativas regulatorias identificadas para cada temática, detallando los mecanismos regulatorios, operativos y tecnológicos que permitirían fortalecer la seguridad, la trazabilidad y la confianza en los servicios móviles, y aportando insumos para la evaluación de impacto normativo y la construcción de una estrategia nacional integral contra el fraude cibernético.

7.1 Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

En el presente apartado se abordan tres problemáticas asociadas con la mitigación del contacto a usuarios con fines fraudulentos mediante el servicio tradicional de mensajes cortos de texto (SMS), las cuales impactan la seguridad, la trazabilidad y la confianza de los usuarios en este canal de comunicación.

La primera temática se centra en la ausencia de mecanismos para la identificación visual del remitente en los mensajes SMS A2P, dado que actualmente se originan principalmente desde códigos cortos numéricos compartidos entre múltiples marcas y campañas. Esta condición impide que el usuario distinga fácilmente quién envía el mensaje, lo que incrementa el riesgo de suplantación, *phishing* y *smishing*, y afecta la transparencia en las comunicaciones mediante SMS.

La segunda temática aborda la dificultad para garantizar trazabilidad en las comunicaciones A2P, derivada de la ausencia de controles sobre los originadores de contenido y la falta de mecanismos que permitan prevenir el fraude, o en caso de que ocurra, asignar responsabilidades claras en la cadena de valor. Las alternativas planteadas para abordar esta problemática se formulan en forma de paquete de medidas, las cuales se enfocan en aportar elementos de prevención y control desde diferentes perspectivas, pero que juntas constituyen una estrategia para mitigar este flagelo. Este tipo de paquetes de medidas ha facilitado en otros países la proliferación de prácticas ilícitas y la recuperación de la confianza en el canal de SMS.

Finalmente, la tercera temática analiza la ausencia de control sobre el tráfico SMS P2P, especialmente en planes que incluyen mensajes ilimitados. Esta situación abre la posibilidad de un mercado secundario en el que usuarios comercializan su tráfico con fines fraudulentos, o se llevan a cabo implementaciones de múltiples tarjetas sim (conocidas como *sim farms*) por parte de personas con fines fraudulentos, generando de este modo vulnerabilidades que comprometen la integridad del servicio y la protección del usuario.

Cada una de estas temáticas se desarrolla con alternativas regulatorias que buscan mitigar los riesgos identificados, mejorar la trazabilidad y fortalecer la confianza en el ecosistema de comunicaciones móviles.

7.1.1 TEMÁTICA 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.

En la actualidad, los mensajes de texto (SMS) llegan desde números genéricos o códigos cortos que no permiten al usuario saber con certeza quién los envía. Esta falta de información clara para el usuario facilita que los delincuentes suplanten a empresas o entidades públicas para cometer fraudes (smishing).

Las alternativas que se proponen para esta temática plantean dos alternativas de aplicación diferentes, distintas al statu quo, en las que los mensajes A2P deberían usar un código alfanumérico único, llamado Sender ID, el cual funcionaría como un nombre de dominio oficial y que sería visible en el encabezado del SMS. Por ejemplo, en lugar de recibir un mensaje desde «12345», el usuario vería que proviene de «BancoXYZ». El identificador alfanumérico abordado en esta temática se articula con las alternativas propuestas para la temática anterior (Temática 1).

7.1.1.1 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.

7.1.1.2 Alternativa 2: Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)

¿Qué es?
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.

¿Por qué 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 1)

¿Cuál es su efecto?
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.

7.1.1.3 Alternativa 3: Asignación y uso de código alfanumérico solo para tráfico transaccional

¿Qué es?
No todos los mensajes de texto tienen el mismo nivel de riesgo. Algunos, como los mensajes promocionales, pueden ser molestos para los usuarios, pero no necesariamente peligrosos. Otros, como los mensajes transaccionales (por ejemplo, códigos de verificación o alertas bancarias), son críticos y pueden ser usados para cometer fraudes si son suplantados.

Esta alternativa propone que solo los mensajes transaccionales usen Sender ID alfanuméricos exclusivos, mientras que los mensajes promocionales seguirían usando códigos cortos o números E.164, con la obligación de incluir el nombre del remitente dentro del texto del mensaje en virtud de la regulación vigente.

¿Por qué es útil?
Porque estos mensajes son los más sensibles y los más usados por los delincuentes para cometer fraudes, por lo que podría pensarse válidamente en implementar una identificación clara solamente para esta categoría.

¿Cuál es su efecto?
El efecto de esta medida es que se protege al usuario en los momentos más críticos, como cuando recibe un código para acceder a su cuenta bancaria.

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 las campañas publicitarias. Esto mejora la seguridad en mensajes sensibles y mantiene un esquema flexible para el tráfico promocional.

7.1.2 TEMÁTICA 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[23] para agregadores (verificación de legitimidad y contratos formales). • Medida 2: Validación centralizada con asignación de Entity_ID, 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 Entity_ID, 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.

7.1.2.1 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

[23] KYC por las siglas en inglés de Know Your Customer.

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.

7.1.2.2 Alternativa 2: Proceso de validación centralizado de originadores de contenido

El fraude por SMS, conocido como smishing, ocurre cuando delincuentes envían mensajes de texto haciéndose pasar por empresas, bancos o entidades públicas para engañar a los usuarios y obtener información personal o dinero. Para combatir este problema, mediante esta alternativa se propone un mecanismo centralizado de verificación que se encarga de validar, antes de enviar cualquier mensaje masivo, quién lo envía, qué empresa está detrás y si el contenido del mensaje tiene enlaces que pudieran llegar a tener propósitos fraudulentos. Así, se busca que solo mensajes legítimos lleguen a los usuarios, y que los fraudulentos sean bloqueados o claramente identificados para que el usuario voluntaria e informadamente decida acceder a ellos.

Medida 1: Conocimiento del cliente (KYC) obligatorio para agregadores

¿Qué es?
Los agregadores (empresas que envían SMS en nombre de otras) 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 agregador 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.

¿Por qué es útil?
Porque de esta forma se evita que empresas fantasma o delincuentes usen el canal de SMS para enviar mensajes fraudulentos.

¿Cuál es su efecto?
El efecto de esta medida se refleja 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 agregadores 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.

Medida 2: Proceso de validación centralizado (tercero)

¿Qué es?
Se trata de un mecanismo de validación en el que actúa un tercero autorizado (el «validador») que se encarga de revisar y aprobar la autenticidad de los agregadores, las marcas (empresas que envían los mensajes) y las campañas (la estructura del contenido de los mensajes). Luego del proceso, el validador le asigna un paquete de identificadores únicos a toda la cadena de envío del mensaje (agregador, marca

y plantilla del contenido) con el propósito de poder ejercer un control sobre los mensajes que se envían y poder actuar de manera oportuna frente a las posibles denuncias que se reciban.

¿Por qué es útil?
Porque permite saber de manera certificada quién envía cada mensaje, cuál es la cadena de empresas que actúan en el envío del mensaje, y qué tipo de contenido se está transmitiendo. De esta manera se logra tener una trazabilidad completa de la comunicación, una identificación clara de los responsables en el envío de cada mensaje, y se garantiza que se puedan detener de manera específica y a tiempo comunicaciones con fines fraudulentos.

¿Cuál es su efecto?
El efecto consiste en que, si un mensaje no tiene toda la validación requerida, representada en todos los identificadores válidos y aprobados por el validador, no puede ser enviado, lo que dificulta la labor de los delincuentes a la hora de pretender realizar una suplantación o de querer llevar a cabo el envío de mensajes engañosos.

En este contexto, de manera específica la medida propone la creación de un mecanismo centralizado de validación, administrado por un tercero autorizado, que permita verificar la identidad y legitimidad de los actores que intervienen en el envío de mensajes A2P antes de que el tráfico sea cursado por las redes. El objetivo es garantizar trazabilidad completa, prevenir la suplantación de identidad y asignar responsabilidades claras en la cadena de valor.

Como se mencionó, el proceso se basa en la asignación de identificadores únicos por parte del validador para cada nivel, así:

- Un **Entity_ID** para los agregadores validados.
- Un **Sender_ID** para las marcas validadas.
- Un **Template_ID** para las plantillas de contenido de campañas validadas y aprobadas.

Los roles que intervendrían en el proceso son los siguientes:

- **El validador central**: administra el registro, revisa documentación, aprueba solicitudes y asigna identificadores.
- **Los agregadores**: inscriben marcas y campañas, garantizando la veracidad de la información y cumpliendo con el conocimiento de su cliente (KYC).
- **Las marcas**: definen las plantillas con el contenido base y la clasificación de sus campañas.
- **PRSTM**: verifican en tiempo real que cada mensaje tenga identificadores válidos antes de cursarlo (obligación descrita en la medida 3).

El proceso de validación consistiría en la aplicación de los siguientes pasos:

Validación de agregadores. Cada agregador se inscribe ante el validador y remite la documentación requerida. El validador verifica la información oficial y, de ser conforme, asigna una identificación del agregador (Entity_ID), habilitándolo para operar dentro del sistema. En caso de no ser conforme, solicitará las aclaraciones que considere pertinentes hasta tener la verificación de la información oficial requerida, antes de asignar el Entity_ID.

Validación de marcas. Una vez inscritos y validados, los agregadores proceden con la inscripción de las marcas registradas que originarán contenido. El validador revisa la documentación de la marca y el contrato suscrito con el agregador. Si todo es conforme, asigna una identificación de la marca (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 la marca tiene su correspondiente validación en el sistema, define el contenido base de cada campaña, con posibilidad de etiquetas variables, y asigna una clasificación conforme al catálogo regulatorio. El agregador registra la plantilla ante el validador, quien corrobora la clasificación, y la aprueba o rechaza. Si aprueba, emite 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.

Medida 3: Bloqueo o marcado por parte del PRSTM de tráfico no autorizado

¿Qué es?
Para que la medida 2 pueda ser efectiva, los proveedores de redes y servicios de telecomunicaciones móviles (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» o «probable estafa», enviándolo de esta manera con una alerta expresa para el usuario.

¿Por qué es 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.

¿Cuál es su efecto?
El efecto esperado 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 Entity_ID, 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.

Medida 4: Categorización del contenido y consentimiento del usuario (articulación con RNE)

¿Qué es?

Con el fin de generar una clasificación de los mensajes acorde con el contenido remitido, y con ello aportar más información y control a los usuarios sobre las comunicaciones recibidas 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 envían si el usuario no está inscrito en el Registro de Números Excluidos (RNE) de la CRC.

¿Por qué 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.

¿Cuál es su efecto?
El efecto de esta medida es que el usuario tiene control sobre qué tipo de mensajes recibe, y se protege así su privacidad y sus derechos de una manera más efectiva.

Teniendo en cuenta el anterior contexto, de manera específica esta medida adopta una clasificación estándar del contenido y su relación con el consentimiento del usuario, integrada con el RNE, así:

- **Contenido transaccional**: exclusivo para bancos y entidades financieras (OTP y validaciones). Tendría un consentimiento implícito del usuario por la relación contractual. Tendría una disponibilidad 24/7, incluso para números inscritos en RNE.
- **Contenido promocional**: referente a publicidad y marketing. Requiere consentimiento explícito previo (opt-in) del usuario y está prohibido su envío a números inscritos en el RNE. Aplican restricciones horarias según estipula actualmente la regulación para usuarios que otorgan el consentimiento explícito.
- **Contenido de servicio implícito**: información relacionada con un servicio contratado por el usuario (p. ej., facturación, autenticación, etc). Aplica un consentimiento implícito dada la relación existente entre el usuario y la marca que envía el mensaje. Tendría una disponibilidad 24/7, incluso para números inscritos en RNE.
- **Contenido de servicio explícito**: comunicaciones de servicio que requieren consentimiento explícito del usuario (opt-in) y registro documental (p. ej., recordatorios de citas).
- **Contenido de gobierno y emergencias**: comunicaciones en interés público como alertas críticas y de seguridad pública. Alta prioridad, exentas de restricciones horarias e independientes del RNE por su naturaleza.

Medida 5: Definición de reglas de monitoreo de tráfico por agregadores

¿Qué es?
Los agregadores deben usar herramientas de monitoreo que analicen en tiempo real el 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 violación alguna a la privacidad de la información de los usuarios o a la obtención de sus datos personales.

¿Por qué es útil?
Porque permite detectar y detener campañas fraudulentas antes de que puedan llegar a los usuarios.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

¿Cuál es su efecto?
El efecto es que se crea una red de vigilancia por parte de toda la cadena, 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 agregadores 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, de manera que se articulen los eslabones de la cadena de actores que intervienen en el envío de SMS en contra del fraude.

Las características y parámetros mínimos que debería tener en cuenta el monitoreo por parte de los agregadores son:

- **Filtrado de enlaces:** Análisis en tiempo real de las URL 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 (Entity_ID, 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:** Los agregadores deberán exponer APIs seguras para compartir señales de riesgo con los PRSTM, permitiendo la activación de bloqueos coordinados en red.

¿Por qué la acción conjunta de las 5 medidas es integral y efectiva?

Cada medida por sí sola aporta una capa de protección a toda la cadena de envío de SMS, pero juntas forman un sistema robusto que cubre varios frentes del fraude por este canal:

- **Prevención:** Solo empresas legítimas pueden enviar mensajes.
- **Trazabilidad:** Se sabe quién envía cada mensaje y qué estructura de contenido tiene.
- **Bloqueo y alerta:** Los mensajes sospechosos no llegan al usuario, o son claramente identificados para alertarlo.
- **Respeto al usuario:** Solo se envían mensajes permitidos y relevantes para el usuario.
- **Vigilancia continua:** Se detectan y detienen nuevas formas de fraude en tiempo real.

Tal como se evidencia en el numeral 6 de este documento, enfoques integrales similares al propuesto en esta alternativa han sido implementados en países como Australia, España, Singapur y Reino Unido, donde la implementación de registros centralizados, validación de remitentes, clasificación del contenido y monitoreo proactivo de tráfico ha reducido significativamente el fraude por SMS y han aportado con la recuperación de la confianza de los usuarios en este canal.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.1.2.3 Alternativa 3: Proceso de validación distribuido (DLT)

Esta alternativa propone 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 (como operadores y agregadores) 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.

Medida 1: Conocimiento del cliente (KYC) obligatorio para agregadores
De la misma manera que se describe en la medida 1 de la alternativa 2, los agregadores deberán verificar la legitimidad de sus clientes (marcas) y formalizar contratos que definan responsabilidades, alcances, uso permitido de recursos de identificación y obligaciones de cumplimiento. De esta forma, el KYC previo se integra como requisito para acceder al sistema de validación y constituye la primera barrera contra el uso indebido de la red.

Medida 2: Validación distribuida en DLT

¿Qué es?
Se trata de un mecanismo de validación en el que intervienen varios validadores autorizados o nodos que se encargan de revisar y aprobar la autenticidad de los agregadores, las marcas (empresas que envían los mensajes) y las campañas (la estructura del contenido de los mensajes). Luego del proceso, el sistema le asigna un paquete de identificadores únicos a toda la cadena de envío del mensaje (agregador, marca y plantilla del contenido) con el propósito de poder ejercer un control sobre los mensajes que se envían y poder actuar de manera oportuna frente a las posibles denuncias que se reciban.

¿Por qué es útil?
Porque le permite acceder de manera certificada a todos los participantes (operadores, agregadores, autoridades) a la misma información validada, sin depender de un único punto de control, pudiendo saber quién envía cada mensaje, cuál es la cadena de empresas que actúan en el envío del mensaje, y qué tipo de contenido se está transmitiendo. De esta manera se logra tener una trazabilidad completa de la comunicación, una identificación clara de los responsables en el envío de cada mensaje, y se garantiza que se puedan detener de manera específica y a tiempo comunicaciones con fines fraudulentos.

¿Cuál es su efecto?
El efecto consiste en que, si un mensaje no tiene toda la validación requerida, representada en todos los identificadores válidos y aprobados por la red de validadores, no puede ser enviado, lo que dificulta la labor de los delincuentes a la hora de pretender realizar una suplantación o de querer llevar a cabo el envío de mensajes engañosos

En este contexto, de manera específica la medida propone la creación de un mecanismo distribuido de validación, garantizando inmutabilidad y resiliencia, en el que intervienen varios validadores autorizados o nodos, que permita verificar la identidad y legitimidad de los actores que intervienen en el envío de mensajes A2P antes de que el tráfico sea cursado por las redes. El objetivo es garantizar trazabilidad completa, prevenir la suplantación de identidad y asignar responsabilidades claras en la cadena de valor.

El proceso se basa en la asignación de identificadores únicos por parte de la red de validadores para cada nivel:

- Un **Entity_ID** para los agregadores validados.
- Un **Sender_ID** para las marcas validadas.
- Un **Template_ID** para las plantillas de contenido de campañas validadas y aprobadas.

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.
- **Agregadores**: inscriben marcas y campañas, garantizando la veracidad de la información y cumpliendo con KYC.
- **Marcas**: definen el contenido base y la clasificación de sus campañas.
- **PRSTM**: verifican en tiempo real que cada mensaje tenga identificadores válidos antes de cursarlo (obligación descrita en la medida 3).

En este contexto, el proceso de validación consistiría en la aplicación de los siguientes pasos:

Validación de agregadores. Cada agregador se inscribe ante cualquier nodo validador y remite la documentación requerida. El nodo validador verifica la información oficial y, de ser conforme, asigna una identificación del agregador (Entity_ID), habilitándolo dentro del sistema DLT.

Validación de marcas. Los agregadores inscriben las marcas registradas que originarán contenido. El nodo validador revisa la documentación de la marca y el contrato suscrito con el agregador; si todo es conforme, asigna una identificación de la marca (Sender_ID) y la incluye dentro del sistema DLT. 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. La marca define el contenido base de cada campaña, con posibilidad de tener etiquetas variables, y asigna una clasificación conforme al catálogo regulatorio. El agregador 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.

Medida 3: Bloqueo o marcado por parte del PRSTM del tráfico no autorizado

De la misma manera que se describe en la medida 3 de la alternativa 2, Los PRSTM deberán verificar, previo al enrutamiento, que cada mensaje cuente con Entity_ID, Sender_ID y Template_ID válidos y habilitados. En ausencia de alguno de estos identificadores, o de la inhabilitación por parte de algún nodo validador, el mensaje debe bloquearse, o alternativamente marcarse 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 similar al spam en el teléfono del usuario, alertándolo de este modo.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Medida 4: Categorización del contenido y consentimiento del usuario (articulación con RNE)

De la misma manera que se describe en la medida 4 de la alternativa 2, se adopta una clasificación estándar del contenido y su relación con el consentimiento del usuario, integrada con el Registro de Números Excluidos (RNE), considerando contenido transaccional exclusivo para bancos y entidades financieras, contenido promocional enfocado en publicidad y marketing, contenido de servicio implícito en el que se le envía al usuario información relacionada con un servicio contratado, contenido de servicio explícito enfocado en comunicaciones de servicio que requieren consentimiento explícito, y contenido de gobierno y emergencias mediante el cual se envían comunicaciones en interés público, alertas críticas y seguridad pública.

Medida 5: Monitoreo de tráfico colaborativo por los agregadores

De la misma manera que se describe en la medida 5 de la alternativa 2, en el marco del sistema de validación distribuida, esta medida establece la obligación para los agregadores de implementar mecanismos avanzados de monitoreo de tráfico, integrados con la infraestructura DLT, para garantizar trazabilidad, interoperabilidad y respuesta coordinada ante riesgos. Es importante aclarar que este monitoreo de ninguna manera implica la violación de la privacidad de la información de los usuarios o la obtención de sus datos personales por parte del agregador.

El objetivo es que todos los actores de la cadena implementen mecanismos proactivos de monitoreo de tráfico para detectar y compartir patrones anómalos de los mensajes en tiempo real, y de esta manera poder prevenir fraudes de manera colaborativa. En esta línea, frente a la identificación y reporte de un mensaje con fines fraudulentos por parte de uno de los actores de la cadena, los demás actores deberán proceder también con la integración de esa identificación en su propio sistema.

Parámetros mínimos del monitoreo en el entorno DLT serían los siguientes:

- **Filtrado inteligente de enlaces:** Análisis en tiempo real de las URL incluidas en los mensajes, comparándolas con listas negras dinámicas y reputación de dominios compartida en la red distribuida.
- **Etiquetado y marcado de riesgo:** Mensajes que no cumplan con los requisitos de validación (Entity_ID, Sender_ID, Template_ID) o que presenten indicadores de fraude deberán ser marcados con etiquetas visibles para el usuario (**«sin verificar»** o **«probable estafa»**).
- **Sincronización descentralizada:** Actualización automática de listas blancas y negras entre nodos del DLT, evitando dependencias de un punto único y reduciendo falsos positivos.
- **Análisis de comportamiento distribuido:** Correlación de datos entre múltiples agregadores y operadores para identificar patrones globales de fraude (volumen, frecuencia, velocidad, repetición de URL).
- **Auditoría inmutable:** Registro de eventos de validación, bloqueos y alertas en el libro distribuido, garantizando trazabilidad y evidencia para investigaciones judiciales.
- **Interoperabilidad con PRSTM:** Disposición de APIs seguras para compartir señales de riesgo y activar bloqueos coordinados en red, con validación en cadena de las reglas aplicadas.

¿Por qué esta alternativa es una solución integral?

La validación distribuida con DLT no solo protege al usuario, sino que también fortalece todo el ecosistema de mensajería A2P, teniendo en cuenta lo siguiente:

- **Descentralización:** No depende de un único actor, lo que mejora la resiliencia y reduce riesgos de corrupción o fallos únicos.
- **Trazabilidad total:** Cada mensaje puede ser rastreado hasta su origen, lo que facilita la identificación de responsables en caso de fraude.
- **Colaboración entre actores:** Operadores, agregadores y autoridades comparten información en tiempo real, lo que permite una respuesta más rápida y coordinada ante el fraude.
- **Protección al usuario:** Se bloquean o etiquetan los mensajes sospechosos, y se respeta el consentimiento del usuario.
- **Prevención proactiva:** Las herramientas de monitoreo permiten anticiparse a los ataques y evitar que lleguen a los usuarios.

Tal como se indicó en el numeral 6 de este documento, India implementó un sistema para registrar y validar remitentes y campañas basado en tecnología DLT y ha sido pionero en el uso de esta tecnología para combatir el smishing. Reino Unido, por su parte, utiliza herramientas avanzadas de monitoreo y análisis de tráfico para detectar y bloquear mensajes sospechosos en tiempo real. Enfoques integrales similares al propuesto en esta alternativa han demostrado ser exitosos en la reducción significativa del fraude por SMS, y ha recuperado la confianza de los usuarios en este canal.

7.1.2.4 Alternativa 4: Identificación exclusiva mediante códigos cortos y numeración E.164, o códigos alfanuméricos

Uno de los principales problemas del fraude por SMS es que los usuarios no pueden identificar fácilmente o de manera exclusiva quién les está escribiendo. En la actualidad, los mensajes llegan desde números genéricos o compartidos entre varias empresas, lo que facilita la suplantación de identidad. Esta alternativa propone que cada empresa tenga un identificador exclusivo y visible, ya sea un código corto o un número E.164 (formato internacional), o un código alfanumérico, con el fin de que los usuarios puedan reconocer con claridad al remitente del mensaje desde el encabezado. Aunque esta alternativa no constituye un mecanismo preventivo por sí solo, sí mejora la identificación visual del remitente y facilita la trazabilidad en caso de fraude.

Esta alternativa asigna a cada marca un código corto, un número E.164 (NDC 940), o un código alfanumérico de uso exclusivo, de forma que el usuario pueda asociar de manera exclusiva el identificador del remitente con la marca.

Medida 1: Asignación de un recurso de identificación exclusivo por marca

¿Qué es?
Esta medida consiste en que cada empresa que quiera enviar SMS a su nombre debe tener su propio identificador exclusivo, ya sea un código corto (como 123-456), un número E.164 (como +57 940 2345678) o un código alfanumérico en forma de nombre de dominio que, mediante texto legible, le permita al usuario saber la procedencia de la comunicación.

¿Por qué es útil?
Porque en la actualidad, las empresas que originan contenido a través de SMS, comparten el mismo código corto para enviar mensajes. Esta situación no le aporta información específica a los usuarios, e

incluso puede pasar que mediante un mismo código corto se mezclen comunicaciones legítimas y comunicaciones con fines fraudulentos. Con esta medida, cada originador de contenido tiene su identidad única en el sistema y es responsable por las comunicaciones que se realicen en su nombre.

¿Cuál es su efecto?
El efecto esperado de esta medida es que el usuario pueda tener certeza de quién envía el SMS mediante el identificador único, lo que reduce la posibilidad de caer en fraudes por suplantación.

En este contexto, la CRC, o aquel que delegue la entidad, asigna a cada marca un recurso exclusivo (un código corto, un número E.164 en el NDC 940 o un código alfanumérico) para su identificación inequívoca ante los usuarios.

Medida 2: Categorización del contenido y consentimiento del usuario (articulación con RNE)

De la misma manera que se describe en la medida 4 de la alternativa 2, se adopta una clasificación estándar del contenido y su relación con el consentimiento del usuario, integrada con el Registro de Números Excluidos (RNE), considerando contenido transaccional exclusivo para bancos y entidades financieras, contenido promocional enfocado en publicidad y marketing, contenido de servicio implícito en el que se le envía al usuario información relacionada con un servicio contratado, contenido de servicio explícito enfocado en comunicaciones de servicio que requieren consentimiento explícito, y contenido de gobierno y emergencias mediante el cual se envían comunicaciones en interés público, alertas críticas y seguridad pública.

Medida 3: KYC obligatorio para agregadores

De la misma manera que se describe en la medida 1 de la alternativa 2, los agregadores deberán verificar la legitimidad de sus clientes (marcas) y formalizar contratos que definan responsabilidades, alcances, uso permitido de recursos de identificación y obligaciones de cumplimiento. De esta forma, el KYC previo constituye la primera barrera contra el uso indebido de la red.

Medida 4: Monitoreo de tráfico colaborativo por los agregadores

De la misma manera que se describe en la medida 5 de las alternativas 2 y 3, esta medida establece la obligación para los agregadores de implementar mecanismos avanzados de monitoreo de tráfico, para garantizar una respuesta coordinada ante riesgos identificados. El objetivo es detectar patrones anómalos en tiempo real, prevenir fraudes y generar señales de riesgo verificables. Es importante aclarar que este monitoreo de ninguna manera implica violación alguna a la privacidad de la información de los usuarios o a la obtención de sus datos personales, por parte del agregador.

Los parámetros mínimos que debería tener en cuenta el monitoreo son los siguientes:

- **Filtrado inteligente de enlaces:** Análisis en tiempo real de las URLs incluidas en los mensajes, con listas negras dinámicas y reputación de dominios.
- **Etiquetado y marcado de riesgo:** Mensajes que no cumplan con parámetros mínimos de seguridad o que presenten indicadores verificables de fraude, deberán ser marcados con etiquetas visibles para el usuario («sin verificar» o «probable estafa»).

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- **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:** Los agregadores deberán exponer APIs seguras para compartir señales de riesgo con los PRSTM y otros agregadores, permitiendo la activación de bloqueos coordinados en red.

Medida 5: Bloqueo o marcado por parte del PRSTM de mensajes sospechosos

¿Qué es?
De la misma manera que se describe en la medida 3 de las alternativas 2 y 3, Los PRSTM deberán tener en cuenta la información del monitoreo de tráfico colaborativo realizado por los agregadores, para verificar, previo al enrutamiento, que cada mensaje no tenga una alerta de fraude. En caso de tener una alerta, el mensaje debe bloquearse, o alternativamente marcarse 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 similar al spam en el teléfono del usuario, alertándolo de este modo.

¿Por qué es útil?
Porque se ejercerán controles colaborativos entre los agregadores y las redes de los PRSTM, que permitirán que los usuarios puedan identificar fácilmente comunicaciones sospechosas y evitar caer en el fraude.

¿Cuál es su efecto?
El efecto esperado es que se reduzca la llegada de mensajes con fines fraudulentos, y que se alerte al usuario sobre posibles riesgos.

En este contexto, por efecto de esta medida se impone a los PRSTM la obligación de bloquear los mensajes identificados como sospechosos por reglas de red o señales de riesgo, y alternativamente podrá permitirse su paso con marcado obligatorio como «sin verificar» o «probable estafa», encausándolos a un buzón similar al de spam de los correos electrónicos para alertar al usuario sin restringir el tráfico por completo.

¿Por qué esta alternativa es una solución integral?

Aunque esta alternativa no incluye mecanismos de validación de los originadores del contenido, sí aporta valor en varios frentes:

- **Identificación clara:** Cada marca tiene un número exclusivo, lo que facilita al usuario reconocer al remitente del contenido.
- **Bloqueo y alerta:** Los mensajes sospechosos no llegan al usuario, o son claramente identificados para alertarlo.
- **Trazabilidad:** En caso de fraude, podría resultar más fácil rastrear el origen del mensaje.
- **Protección del usuario:** Se clasifica el contenido para respetar su consentimiento y se le alerta sobre mensajes sospechosos.

Tal como se evidencia en la revisión internacional descrita en el numeral 6 de este documento, países como India utilizan códigos cortos y números E.164 diferenciados para tráfico transaccional y promocional, y los mensajes transaccionales deben provenir de códigos alfanuméricos exclusivos. España en su consulta pública sobre el Registro de Alias, discute la posibilidad de limitar el uso de alias genéricos y exigir identificadores únicos por empresa. Australia y Singapur aplican reglas estrictas sobre el uso de identificadores de remitente, incluyendo la validación de alias y la prohibición de nombres genéricos o engañosos.

7.1.3 TEMÁTICA 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	Implementación de mecanismos de detección y bloqueo para identificar comportamientos anómalos en el tráfico SMS P2P, como envíos masivos a números desconocidos o fuera del patrón habitual. Incluye 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.

Los mensajes SMS entre personas (P2P por las siglas en inglés de Person to Person) tradicionalmente han sido considerados seguros. Sin embargo, con la aparición de planes ilimitados para este servicio, se ha evidenciado la existencia de aplicaciones en internet que compran la capacidad de envío de mensajes que no utilizan los usuarios, y algunos usuarios han comenzado a revender su capacidad de envío de mensajes a terceros, los cuales podrían llegar a ser actores maliciosos. Adicionalmente, las implementaciones conocidas como *SIM farms*[24] representan una de las principales amenazas en el tráfico P2P, al convertir líneas móviles personales en plataformas masivas de envío de mensajes, muchas veces con fines fraudulentos.

Estas implementaciones de tarjetas SIM operan mediante la instalación de decenas o cientos de SIMs en dispositivos automatizados, aprovechando los planes ilimitados para enviar grandes cantidades de SMS por hora, sin pasar por los controles que aplican o podrían aplicar al tráfico A2P. Esta práctica no

[24] Las SIM farms son sistemas que usan varias tarjetas SIM para enviar mensajes masivos o hacer llamadas con las tarifas P2P.

solo distorsiona el uso legítimo del canal P2P, sino que facilita el smishing, la suplantación de identidad y la evasión de mecanismos de trazabilidad.

7.1.3.1 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.

7.1.3.2 Alternativa 2: Control de patrones de tráfico atípicos

¿Qué es?
Esta alternativa propone que los operadores implementen sistemas de monitoreo inteligente para detectar comportamientos anómalos en el tráfico P2P. Se trata de identificar patrones que no corresponden al uso personal típico, como el envío masivo de mensajes similares, alta frecuencia de envío o destinatarios secuenciales.

¿Por qué es útil?
Porque permite diferenciar entre el uso legítimo y el uso abusivo del canal P2P. Al detectar estos patrones, los operadores pueden actuar antes de que se materialice un fraude, evitando que las SIM farms y otros esquemas ilegales se aprovechen de los planes ilimitados ofrecidos por los proveedores.

¿Cuál es su efecto?
Se espera una reducción significativa del tráfico fraudulento en el canal P2P, una mejora en la trazabilidad de los mensajes, y una mayor protección para los usuarios frente a campañas de smishing y suplantación que usan de manera ilegítima los canales de comunicación P2P.

Con el anterior contexto, esta alternativa propone de manera específica la adopción de mecanismos de detección y control de comportamientos anómalos en el tráfico SMS P2P. El objetivo es poder identificar a tiempo, y mitigar el uso fraudulento de planes con SMS ilimitados, mediante el uso de las denominadas *SIM farms* o también mediante las conocidas «rutas grises»[25], evitando que se conviertan en un canal para el envío masivo de mensajes con fines ilícitos. El control se basaría en el análisis de patrones de uso, incluyendo volumen, frecuencia y distribución de los mensajes enviados por cada usuario.

Cuando se detecten desviaciones significativas respecto del comportamiento normal —por ejemplo, envíos masivos a números desconocidos o fuera del rango habitual— se activarían alertas automáticas y bloqueos temporales. Este enfoque permite actuar de manera preventiva sin afectar el uso legítimo del servicio, reduciendo el riesgo de que surja un mercado secundario para la comercialización de tráfico P2P.

7.1.3.3 Alternativa 3: Límite de SMS P2P por usuario

¿Qué es?

[25] Práctica por la cual los mensajes A2P se envían través de canales diseñados para el tráfico P2P que no están supervisados por un operador de red móvil.

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.

¿Por qué es 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.

¿Cuál es su efecto?
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 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.

7.2 Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

En este apartado se abordan las cuatro situaciones principales identificadas que afectan la seguridad, trazabilidad y confianza de los usuarios en el canal de voz, así como las correspondientes alternativas regulatorias propuestas para su mitigación. Cada temática se desarrolla con alternativas excluyentes, estructuradas para facilitar su estudio independiente y posterior evaluación.

7.2.1 TEMÁTICA 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)[26] (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

[26] 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.

	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.
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, pero exige que sean identificadas y marcadas como «No verificada» o «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.

7.2.1.1 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).

Bajo este escenario, las llamadas internacionales podrían seguir presentándose ante el usuario como si fueran colombianas, sin que el PRST tenga la capacidad o la obligación de validar la autenticidad del número mostrado o la identidad de la línea llamante.

7.2.1.2 Alternativa 2: Prohibición total del enmascaramiento de la identidad de la 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). El objetivo 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.

En términos operativos, los operadores de red 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 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.

7.2.1.3 Alternativa 3: Permitir enmascaramiento con obligación de identificación y etiquetado de llamadas para el usuario

Esta alternativa propone permitir que las llamadas internacionales entrantes utilicen números colombianos como identificador de llamada (CLI), pero exige que dichas llamadas sean marcadas en el dispositivo del usuario como «No verificada» o «Probable fraude». El objetivo es alertar al usuario sobre el posible riesgo de suplantación, sin bloquear el tráfico legítimo, y facilitar la transición hacia esquemas más robustos de autenticación y trazabilidad.

Para ello los PRST deben usar sistemas que permitan identificar llamadas internacionales entrantes con identidad de línea llamante (CLI) nacional, y al detectar este tipo de llamadas, añadir una etiqueta visible («No verificada» o «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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.2.1.4 Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional

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)[27] 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.

[27] 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.

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.

7.2.2 TEMÁTICA 2: Falta de aplicación coordinada de métodos preventivos de filtrado de tráfico de voz

Situación identificada:	En Colombia no existe un esquema uniforme que permita a los operadores a aplicar métodos preventivos de filtrado estandarizado en tráfico de voz, lo que dificulta la detección temprana de patrones anómalos asociados a fraude (*vishing*, llamadas masivas ilegítimas, *spoofing*). Esta falta de coordinación genera vulnerabilidades y limita 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	Cada operador aplica controles internos sin lineamientos regulatorios comunes; no existe monitoreo ni filtrado coordinado del tráfico de voz.
Alternativa 2: Lineamientos regulatorios para monitoreo de tráfico	Esta alternativa propone que la CRC establezca lineamientos regulatorios obligatorios para que todos los operadores implementen mecanismos de monitoreo en tiempo real del tráfico de voz. El objetivo es detectar, filtrar y prevenir actividades fraudulentas, como el enmascaramiento de la identidad de la línea llamante (CLI), vishing y suplantación de identidad, mediante la identificación de patrones sospechosos y/o comportamientos anómalos.
Alternativa 3: Creación de una plataforma de articulación e intercambio de alertas	Esta alternativa propone la creación de una plataforma nacional centralizada, 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, facilitando la coordinación entre operadores, la trazabilidad de eventos y la respuesta rápida ante campañas fraudulentas.
Alternativa 4: Implementación de STIR/SHAKEN/RCD	Esta alternativa propone exigir que todas las llamadas nacionales e internacionales entrantes estén firmadas digitalmente mediante el protocolo STIR/SHAKEN, garantizando la autenticidad del número mostrado al usuario. Además, se incorpora la posibilidad de incluir información enriquecida de la llamada (RCD por sus siglas en inglés Rich Call Data) 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.

7.2.2.1 Alternativa 1: Statu quo

Cada operador aplica controles internos sin lineamientos regulatorios comunes; no existe monitoreo ni filtrado coordinado del tráfico de voz.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.2.2.2 Alternativa 2: Lineamientos regulatorios para monitoreo de tráfico

Esta alternativa propone que la CRC establezca lineamientos regulatorios obligatorios para que todos los operadores implementen mecanismos de monitoreo en tiempo real del tráfico de voz. El objetivo es detectar, filtrar y prevenir actividades fraudulentas, como el enmascaramiento de la identificación de línea llamante (CLI), *vishing* y suplantación de identidad, mediante la identificación de patrones sospechosos o comportamientos anómalos. Los lineamientos incluirían parámetros mínimos de monitoreo, técnicas de screening, correlación con listas negras y reportes de fraude, y la obligación de tomar medidas preventivas ante la detección de anomalías asociadas al tráfico.

En este orden de ideas, se definen los parámetros técnicos mínimos que deben cumplir los sistemas de monitoreo de tráfico de voz, incluyendo como mínimo los siguientes:

- **Detección de volumen inusual de llamadas por origen/destino.**

  Ejemplo: Un número o rango de numeración inicia más de 100 llamadas por minuto a distintos destinos, superando los umbrales normales definidos por el operador.
  Se activa una alerta de "tráfico anómalo por tasa de establecimiento" (Call Setup Rate – CSR).
  El sistema puede suspender temporalmente la numeración o enrutar las llamadas a un entorno de inspección.

- **Identificación de patrones repetitivos (llamadas cortas, secuenciales, típicas de robocall).**

  Ejemplo: Se detectan llamadas consecutivas de 2–3 segundos hacia múltiples destinos, con tiempos de conversación mínimos o nulos.
  El motor de análisis agrupa las llamadas por origen, destino y hora, y calcula indicadores como Average Call Duration (ACD) o Answer-Seizure Ratio (ASR), se analiza el comportamiento basado en métricas de desempeño de red.

- **Correlación automática con listas negras y reportes de fraude.**

  Ejemplo: Un número detectado en la red coincide con registros de listas negras de la GSMA o de bases nacionales de spam telefónico. El sistema correlaciona eventos de tráfico con repositorios externos o nacionales mediante API seguras (por ejemplo, GSMA Fraud Intelligence Database). En consecuencia, el sistema asigna una clasificación de riesgo alto y aplica políticas de mitigación automática, como: bloqueo temporal de la numeración sospechosa, enrutamiento hacia una pasarela de inspección, o generación de alerta a los equipos de cumplimiento y seguridad de red.

- **Técnicas de screening para clasificar y filtrar llamadas sospechosas en tiempo real.**

  Ejemplo: Antes de que la llamada sea completada, un sistema de análisis en tiempo real ejecuta un modelo de puntuación de riesgo (*Call Scoring Engine*) basado en el nivel de autenticación STIR/SHAKEN, patrones de tráfico recientes, reputación del número, y comportamiento histórico del abonado.
  Si el puntaje excede un umbral, la llamada se etiqueta como "No verificada" o "Probable fraude" en el dispositivo del usuario.

En este sentido, los PRST deben actualizar sus plataformas de gestión de tráfico para integrar estas herramientas, y ante la identificación de anomalías, estarán obligados a bloquear el tráfico sospechoso o, alternativamente, etiquetar las llamadas como «No verificada» o «Probable fraude» en el dispositivo del usuario.

7.2.2.3 Alternativa 3: Creación de una plataforma de articulación e intercambio de alertas

Esta alternativa propone la creación de una plataforma nacional centralizada, 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* de intercambio de alertas y señales de riesgo, 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 reacción coordinada frente a amenazas, mejorando la protección del usuario y la eficacia de las investigaciones.

La administración de la plataforma nacional de alertas sería implementada mediante un sistema centralizado o distribuido, según se considere más conveniente en términos técnicos y económicos, y podría ser accesible a todos los PRST y entidades relevantes. 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.

De esta manera, la plataforma recibiría, procesaría y correlacionaría las alertas, generando notificaciones en tiempo real para todos los PRST y entidades conectadas. 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).

Las entidades competentes podrían emitir alertas prioritarias, coordinar bloqueos preventivos y publicar listas negras temporales basadas en la información recibida y los PRST deberían actualizar sus procedimientos internos para responder a las alertas recibidas, bloqueando o etiquetando llamadas según los protocolos definidos.

7.2.2.4 Alternativa 4: Implementación de STIR/SHAKEN/RCD

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. Además, se incorpora la posibilidad de incluir información enriquecida de la llamada (RCD por sus siglas en ingles Rich Call Data) 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, reducir el *spoofing* y mejorar la trazabilidad y confianza en el canal de voz.

A diferencia de las alternativas basadas en monitoreo, filtrado y articulación de alertas, esta alternativa no depende de la detección reactiva de patrones sospechosos ni del análisis de tráfico para identificar posibles fraudes. Por su parte, establece un mecanismo técnico de autenticación en la raíz del proceso

del origen de la llamada, asegurando que solo las llamadas con identidad verificada puedan cursarse y presentarse como confiables al usuario.

Por su naturaleza, sustituye los métodos de screening y monitoreo teniendo en cuenta que, si la autenticidad del originador se valida criptográficamente en el momento de la originación, no es necesario depender de la detección de anomalías en el tráfico ni de la correlación de alertas entre operadores. Es decir, al validar criptográficamente la identidad del originador de la llamada desde el inicio, se reemplazan los métodos de detección y monitoreo de tráfico, pues la autenticidad se garantiza directamente en el origen de la llamada.

Por lo tanto, esta alternativa es excluyente respecto a las demás tenidas en cuenta en esta temática, ya que representa un cambio de paradigma: pasa de la prevención reactiva (filtrado y monitoreo) a la prevención proactiva y técnica (autenticación y verificación en origen).

Así las cosas, en línea con lo descrito en la temática anterior, los PRST deberían hacer las adecuaciones necesarias en sus plataformas de señalización y enrutamiento para soportar la autenticación criptográfica de llamadas mediante 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 operador 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 no presentan la verificación completa (nivel B o C) pueden ser bloqueadas, marcadas como «No verificada» o «Probable fraude», o bien ser sujetas a procesos adicionales de revisión, el cual puede incluir análisis de tráfico, correlación con reportes de fraude o monitoreo de patrones inusuales antes de su terminación al usuario final.

Por otra parte, si la llamada incluye Rich Call Data (RCD), el receptor debería estar en capacidad de mostrar el nombre, logo y motivo de la llamada definidos por el originador de la llamada en el dispositivo del usuario.

7.2.3 TEMÁTICA 3: Ausencia de diferenciación en rangos de numeración para comunicaciones personales, comerciales y publicitarias

Situación identificada:	En Colombia no existe una diferenciación entre los rangos de numeración asignados a comunicaciones personales y aquellos utilizados para fines comerciales (atención al cliente) y/o publicitarios. Esta condición dificulta que los usuarios identifiquen el propósito de la llamada, incrementa el riesgo

	de suplantación y fraude, y limita la capacidad del regulador para aplicar controles específicos que garanticen la trazabilidad del tráfico de voz comercial y publicitario.
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 marco regulatorio y operativo vigente, en el cual no existe distinción entre los rangos de numeración asignados para comunicaciones personales y aquellos utilizados para fines comerciales o publicitarios.
Alternativa 2: 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 3: Etiquetado obligatorio en el identificador de llamadas para contactos comerciales, usando la numeración actual	Esta alternativa propone mantener el uso de la numeración actual, pero exige que todas las llamadas comerciales y publicitarias incluyan un indicador visible en el identificador de llamada (Caller ID), que permita al usuario distinguir el propósito de la comunicación. El etiquetado consistiría en un descriptor textual («Comercial», «Publicidad», «Atención al cliente», etc.) o, cuando la tecnología lo permita, en la implementación de Rich Call Data (RCD) o Branded Caller ID bajo la implementación del esquema de STIR/SHAKEN/RCD, mostrando el nombre, logo y motivo de la llamada.

7.2.3.1 Alternativa 1: Statu quo

La alternativa statu quo consiste en mantener el marco regulatorio y operativo vigente, en el cual no existe distinción entre los rangos de numeración asignados para comunicaciones personales y aquellos utilizados para fines comerciales o publicitarios. Bajo este esquema, los operadores gestionan sin ningún tipo de diferenciación la numeración E.164, permitiendo que cualquier tipo de llamada, independientemente de su propósito, utilice cualquier número disponible en el plan nacional de numeración. Esta ausencia de diferenciación limita la capacidad de los usuarios para identificar el propósito de la llamada y restringe las posibilidades de trazabilidad y control por parte del regulador.

No se requieren modificaciones en los sistemas de administración y gestión de numeración ni en los procedimientos de asignación y enrutamiento de llamadas, por lo tanto, los PRST continúan aplicando los procesos actuales de administración de recursos de identificación, sin establecer controles adicionales ni mecanismos de clasificación para el tráfico comercial o publicitario.

La CRC mantiene su función de supervisión sobre el uso eficiente de la numeración, sin introducir obligaciones específicas para la identificación y/o registro de llamadas comerciales.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.2.3.2 Alternativa 2: 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.

7.2.3.3 Alternativa 3: Etiquetado obligatorio en el identificador de llamadas para contactos comerciales, usando la numeración actual

Esta alternativa propone mantener el uso de la numeración actual, pero exige que todas las llamadas comerciales y publicitarias incluyan un indicador visible en el identificador de llamada (Caller ID), que permita al usuario distinguir el propósito de la comunicación al momento que recibe la llamada.

El etiquetado consistiría en un descriptor textual («Comercial», «Publicidad», «Atención al cliente», etc.) o, cuando la tecnología lo permita, en la implementación de Rich Call Data (RCD) o Branded Caller ID bajo la implementación del esquema de STIR /SHAKEN/RCD, mostrando el nombre, logo y motivo de la llamada. Este mecanismo busca incrementar la transparencia y la protección del usuario frente a intentos de suplantación y fraude.

La CRC establecería las especificaciones técnicas y normativas para el etiquetado obligatorio, definiendo los formatos, textos permitidos y reglas de consistencia. Los PRST adaptarían sus sistemas de señalización y gestión de llamadas para insertar y propagar el indicador en el Caller ID, asegurando la interoperabilidad entre redes y dispositivos.

Bajo esta alternativa, se harían campañas de divulgación de la medida para los usuarios incentivando la denuncia ante las autoridades competentes de llamadas comerciales realizadas desde números sin

etiquetado, y al mismo tiempo se establecería la obligación de bloqueo de los números denunciados por parte de los PRST cuando dicha conducta se corrobore.

Las empresas originadoras de llamadas comerciales y/o publicitarias tendrían la obligación de declarar la naturaleza de la llamada en el proceso de originación, permitiendo que el operador aplique el etiquetado correspondiente.

7.2.4 TEMÁTICA 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 decide si administra o no 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: Registro DNO Nacional Único administrado por la CRC	Esta alternativa propone la creación y administración, por parte de la CRC, de un registro nacional único de números de no originación (DNO). Este repositorio centralizado funcionaría como la fuente oficial de números que no pueden ser utilizados para originar llamadas en ninguna red del país. El objetivo es eliminar la fragmentación de criterios entre PRST, garantizar la actualización y consulta en tiempo real, y asegurar que todos los proveedores apliquen de manera uniforme las medidas de bloqueo y control sobre los números incluidos en la lista DNO.
Alternativa 3: 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 de solo recibo de llamadas, etc.
Alternativa 4: Sustitución funcional de DNO por autenticación del CLI y reglas	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

anti-spoofing internacional STIR/SHAKEN/RCD	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.

7.2.4.1 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.

7.2.4.2 Alternativa 2: Registro DNO nacional único administrado por la CRC

Esta alternativa propone la creación y administración, por parte de la CRC, de un registro nacional único de números de no originación (DNO). Este repositorio centralizado funcionaría como la fuente oficial de números que no pueden ser utilizados para originar llamadas en ninguna red del país. El objetivo es eliminar la fragmentación de criterios entre PRST, garantizar la actualización y consulta en tiempo real, y asegurar que todos los proveedores apliquen de manera uniforme las medidas de bloqueo y control sobre los números incluidos en la lista DNO.

La CRC desarrollaría y operaría el registro DNO nacional, integrándolo con los estados que reposan en el Sistema de Información y Gestión de Recursos de Identificación (SIGRI) así como los estados de adjudicación por parte del operador y el usuario final que hace uso de ese número. Todos los PRST tendrían la obligación de integrar la lista del registro en su red, de actualizarla con una frecuencia establecida, y de consultarla antes de cursar llamadas, bloqueando aquellas que utilicen números allí incluidos.

La consulta se realizaría mediante una API segura y estandarizada, con ventanas de actualización definidas (por ejemplo, sincronización completa cada 4 horas y pushes críticos en menos de 1 hora). El registro incluiría procedimientos para la inscripción, actualización y baja de números, así como para la trazabilidad de consultas y bloqueos.

7.2.4.3 Alternativa 3: 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 de solo recibo de llamadas, etc. 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.

La CRC definiría el estándar mínimo obligatorio para la gestión de estas listas, especificando las categorías de números, los formatos de intercambio de información entre proveedores y los plazos de

actualización. 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.

7.2.4.4 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 llamada (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. El objetivo es trasladar la estandarización desde lo que se debe bloquear (listas) a cómo se debe autenticar (firma del CLI y políticas técnicas), eliminando la discrecionalidad y homogeneizando la decisión operativa.

En esta línea, la CRC establecería la obligación de implementar STIR/SHAKEN/RCD para la firma y verificación del CLI en tráfico IP, clasificando las llamadas según el nivel de verificación (A/B/C tal como se explicó en la alternativa 4 de la temática 2 – numeral 7.2.2.4). Para el tráfico internacional, se definirían políticas de bloqueo o supresión del CLI nacional en llamadas entrantes sospechosas, con excepciones para casos de roaming legítimo.

Por su parte, los PRST deberían adaptar sus plataformas de señalización y gestión de llamadas para cumplir con los requisitos técnicos, y las autoridades competentes supervisarían la interoperabilidad, la actualización de reglas y la efectividad de la medida mediante auditorías y análisis de métricas.

7.3 Temáticas enfocadas en la educación de la ciudadanía

7.3.1 TEMÁTICA 1: Acciones educativas 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.
Consecuencia relacionada:	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.
Alternativa 1: Statu quo.	Mantener la provisión de redes y servicios de telecomunicaciones, así como la provisión 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: Pedagogía y lista de campañas más denunciadas	Incluir una obligación de divulgación de información con objetivos pedagógicos y de prevención a los usuarios de servicios móviles, en cabeza de los PRST, PCA e IT. Adicionalmente, la CRC creará y administrará un portal que incluya una **lista** con las campañas más denunciadas ante la CRC e identificadas por esta autoridad de oficio que sean utilizados para contactar usuarios con fines presuntamente fraudulentos.
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 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, así como con la información periódica que reporten los PRST, PCA e IT. Adicionalmente, se definiría una estrategia educativa y de prevención de manera conjunta entre los agentes regulados y la CRC, a la cual se invitaría también a otras entidades competentes en estos asuntos.

7.3.1.1 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.

7.3.1.2 Alternativa 2: Pedagogía y lista de campañas más denunciadas

De acuerdo con los comentarios recibidos por los agentes interesados frente al Documento de Formulación del Problema, así como de la respuesta a las preguntas formuladas en relación con las temáticas a abordar en las alternativas del presente proyecto regulatorio, esta Comisión evidencia la pertinencia de formular como alternativa obligaciones de divulgación pedagógica en cabeza de los proveedores de redes y servicios de telecomunicaciones móviles, de los Proveedores de Contenidos y Aplicaciones y de los Integradores Tecnológicos, dado que estos agentes ostentan una posición privilegiada, al ser el primer contacto con el usuario.

Es así como, de acuerdo con esta alternativa, dichos agentes deberán, de acuerdo con los lineamientos que establezca la CRC, implementar campañas pedagógicas de los derechos que le asisten a sus usuarios frente a sus datos personales, así como respecto de las modalidades de fraude existentes a través de mensajes de texto y llamadas de voz, de las técnicas de ingeniería social que los ciberdelincuentes utilizan para engañarlos y así obtener su información confidencial, y de las acciones que pueden tomar para prevenir o mitigar ser víctimas de las mismas. Estas acciones educativas serán diferenciales tratándose de usuarios en condición de vulnerabilidad.

Lo anterior estaría acompañado de una lista administrada por la CRC, en la cual se publiquen las campañas más denunciadas y las de más impacto ante esta entidad o identificadas de oficio, que sean utilizadas para contactar usuarios con fines presuntamente fraudulentos a través de mensajes de texto o llamadas de voz. Tal y como algunos agentes[28] manifestaron en la respuesta a la consulta formulada por esta Entidad, respecto de las temáticas objeto de consideración en las alternativas, se evidencia que esta lista puede ser una herramienta de información complementaria que haga las veces de una alerta temprana con efecto disuasivo y que visibilice patrones delictivos, facilitando así la implementación de acciones preventivas y correctivas.

7.3.1.3 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 fraudes a través de mensajes de texto o llamadas telefónicas. Tal y como algunos agentes[29] expusieron en la consulta publicada por esta entidad respecto las temáticas a abordar en las alternativas del presente proyecto regulatorio, este tipo de sistema puede resultar útil, en el sentido de contribuir en 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 el intento o comisión de fraudes a través de llamadas de voz y mensajes de texto, lo cual permitirá conocer a todos los agentes interesados las modalidades empleadas por los delincuentes; lo cual podría llegar a ser una herramienta de divulgación, prevención y mitigación de este tipo de conductas.

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.

[28] Asobancaria, Aval, Colcert, Cristóbal Fuentes, Plintron, Superintendencia de Industria y Comercio y Universidad Externado. Comentarios disponibles en el siguiente enlace: https://www.crcom.gov.co/es/noticias/proyectos-regulatorios/comentarios-documento-formulacion-proyecto-identificacion-medidas-fraude-cibernetico-servicios-moviles

[29] Andi, Asobancaria, Aval, Colcert, Cristobal Fuentes, MDK, Superintendencia de Industria y Comercio y Universidad Externado. Comentarios disponibles en el siguiente enlace: https://www.crcom.gov.co/es/noticias/proyectos-regulatorios/comentarios-documento-formulacion-proyecto-identificacion-medidas-fraude-cibernetico-servicios-moviles

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[30].

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.

En esta estrategia se invitaría a su vez a participar a otras autoridades cuyas competencias se encuentran relacionadas con estos asuntos. Estas acciones educativas serán diferenciales tratándose de usuarios en condición de vulnerabilidad.

7.4 Temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

Finalmente, la CRC informa que, de acuerdo con los objetivos específicos trazados para este proyecto regulatorio, indicados en la sección **Error! Reference source not found.**, y teniendo en consideración los comentarios y sugerencias planteados en el marco del proyecto regulatorio *Simplificación del marco regulatorio 2024* y en la *Hoja de ruta de iniciativas regulatorias*, se efectuará una revisión integral del Régimen de Administración de Recursos de Identificación bajo un enfoque de simplificación, con el fin de identificar oportunidades de mejora tanto en los procedimientos de asignación como de recuperación de los recursos, desde una perspectiva de prevención del contacto a usuarios con fines fraudulentos.

En este sentido, en la revisión de este régimen se tendrá en cuenta si las disposiciones vigentes cumplen con alguno de los supuestos de evolución de mercado, evolución tecnológica, duplicidad normativa, transitoriedad, cambios en normas de rango superior, posibilidad de optimización normativa o reducción de costos de cumplimiento. En este contexto, la aplicación del enfoque de simplificación busca contribuir con la adecuación del régimen y garantizar que la efectividad de las medidas que se determinen sea la pertinente, como resultado de la aplicación del AIN, bajo el propósito de prevenir y mitigar prácticas fraudulentas mediante el uso indebido de la numeración E.164 y los códigos cortos.

Cabe señalar que, mientras se define, publica e implementa la propuesta regulatoria derivada del presente proyecto regulatorio, en particular sobre las alternativas propuestas en las temáticas anteriores, las disposiciones y alternativas propuestas bajo la presente temática se aplicarán de manera transitoria. Esto permitirá contar con herramientas regulatorias de manera inmediata, aunque de carácter reactivo, mientras se puede llevar a cabo la implementación de medidas preventivas, garantizando así la continuidad regulatoria y operativa para los distintos agentes involucrados en la mitigación del fraude a través de los canales tradicionales de voz y mensajes de texto (SMS).

Así mismo, la aplicación del enfoque de simplificación responde a las observaciones allegadas al documento de formulación del problema que indican la modernización de los modelos de negocio y su posible impacto en la cadena de valor del flujo de las comunicaciones, en donde los recursos de

[30] Tal y como fue propuesto por algunos agentes (entre los que se encuentran Alianza Lationamericana de Telecomunicaciones, Hablame y Tigo) en la respuesta a la consulta formulada por la CRC, respecto de las temáticas objeto de consideración en las alternativas. Comentarios disponibles en el siguiente enlace: https://www.crcom.gov.co/es/noticias/proyectos-regulatorios/comentarios-documento-formulacion-proyecto-identificacion-medidas-fraude-cibernetico-servicios-moviles

identificación juegan un papel fundamental. En este sentido, resulta necesario considerar si las disposiciones contenidas en el régimen vigente reflejan de buena manera las dinámicas actuales de los diferentes agentes que usan los recursos de identificación objeto del análisis.

7.4.1 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, de las causales del artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, sin obligaciones adicionales para nuevos procesos de asignación y/o recuperación.
Alternativa 2: Establecer obligaciones y consecuencias ante reincidencia	Incorporar al régimen normativo obligaciones y consecuencias específicas relacionadas para los asignatarios reincidentes por recuperación de códigos cortos.

7.4.1.1 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.

7.4.1.2 Alternativa 2: Establecer obligaciones y concecuencias ante reincidencia

Esta alternativa propone ajustar el régimen de administración de los recursos de identificación mediante la incorporación de obligaciones específicas para los asignatarios reincidentes en el uso indebido de códigos cortos o de cualquier recurso de identificación administrado por la CRC. En particular, los asignatarios que hayan sido objeto de recuperación por algunas de las causales identificadas en 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, deben ser evaluados para acceder a nuevos recursos de identificación.

La implementación de esta alternativa requiere la inclusión de definiciones de reincidencia o conductas indebidas en el uso de códigos cortos, así como las condiciones bajo las cuales se identificaría un asignatario como reincidente. Además, dadas estas definiciones, deben revisarse las causales de recuperación y evaluar la inclusión de la reincidencia como causal de recuperación. Finalmente, deben identificarse las condiciones, si las hay, en las cuales un reincidente podría o no ser asignatario de un nuevo recurso de identificación, lo cual implicaría una revisión de los requisitos y procedimientos de asignación de estos recursos.

7.4.2 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.

7.4.2.1 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 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.

7.4.2.2 Alternativa 2: Adopción de condiciones para la cesión o transferencia

Esta alternativa propone introducir condiciones específicas para la cesión o transferencia de recursos de identificación, como los códigos cortos. Para su implementación, se requeriría la revisión de las obligaciones generales de los asignatarios, así como de los principios para la administración e implementación de los recursos de identificación.

Entre las medidas sugeridas se incluye la evaluación del historial del asignatario, la prohibición de cesión de códigos cortos a asignatarios reincidentes en procesos de recuperación por uso indebido, la obligación explícita de mantener las condiciones de asignación, y la verificación de la vigencia de la razón social del nuevo asignatario en el Registro Mercantil, así como en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores tecnológicos (RPCAI) por parte de la CRC, como parte del proceso de validación.

Adicionalmente, se establecería de forma expresa que la cesión o transferencia de un recurso de identificación no implica modificación alguna sobre el uso, servicio o propósito para el cual fue originalmente asignado. Esta operación se entendería exclusivamente como un cambio de asignatario, manteniéndose inalteradas las condiciones técnicas y operativas del recurso previamente asignado.

Una vez asignado el recurso de identificación, no se admitirían solicitudes de modificación respecto de su uso, servicio o propósito. En consecuencia, el nuevo asignatario deberá mantener integralmente las condiciones bajo las cuales le fue otorgado el recurso, sin que proceda la modificación alguna de su finalidad, servicio a soportar y/o propósito.

7.4.3 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 presuntamente fraudulento 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 durante una actuación administrativa.	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, teniendo en cuenta las quejas y/o reportes de presunto fraude allegados a la Entidad.

7.4.3.1 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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7.4.3.2 Alternativa 2: Suspensión preventiva del tráfico durante una actuación administrativa

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, cuando existan presuntos indicios de uso indebido del recurso soportados en las quejas o reportes allegados a la Entidad. En este sentido, se deben evaluar y modificar las causales de recuperación con el fin de incorporar aquellos casos de uso indebido que de forma preliminar no se ajustan a una causa directa de recuperación; así como, definir las condiciones que en la actuación administrativa dan lugar a la suspensión de tráfico en cualquier etapa de su desarrollo.

En concreto, deben considerarse las condiciones que motivaron el inicio de la actuación administrativa, así como, la posterior existencia de evidencia que demuestre 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.

7.4.4 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 o en el RUES cuando se presentan novedades en términos de su existencia y representación legal, lo que dificulta el contacto por parte del Administrador de los recursos de identificación en ejercicio de sus funciones, y la trazabilidad de los requerimientos de información en casos de uso indebido.
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 Administración de Recursos de Identificación asociadas a una vigencia específica para la asignación del código corto, así como la obligación de actualizar la información del asignatario del código corto en el RPCAI y en el RUES de manera periódica.

7.4.4.1 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.

7.4.4.2 Alternativa 2: Vigencias y actualización de la asignación del código corto.

Esta alternativa propone incluir, dentro de los criterios de uso eficiente y de las causales de recuperación, la obligación de llevar a cabo la renovación de la asignación del código corto asignado, luego de pasado un tiempo determinado posterior a la asignación, para poder continuar con su uso en las condiciones inicialmente otorgadas.

En caso de no llevarse a cabo la renovación del recurso de identificación, constatando el cumplimiento de los requisitos inicialmente remitidos al Administrador, se incurriría en una causal de recuperación del código corto. Dicho criterio de uso eficiente y causal de recuperación se incorporaría en el Régimen de Administración de Recursos de Identificación establecido en el capítulo 4 del título VI de la Resolución CRC 5050 de 2016.

En este sentido, la asignación de un código corto tendría una vigencia específica, la cual se ve condicionada por el cumplimiento de la obligación de actualización de la información registrada en el RPCAI y en el Registro Único Empresarial y Social (RUES). Así mismo se establecería como obligación mantener actualizada la información básica en el RPCAI y el RUES en aspectos como:

- Existencia jurídica y representación legal vigente.
- Contactos administrativos y técnicos actualizados.

El incumplimiento de la actualización periódica conllevaría a la suspensión preventiva del tráfico del código corto asignado, y en caso de persistencia en la falta de actualización durante un tiempo determinado, la recuperación definitiva del recurso por parte de la CRC.

8. BIBLIOGRAFÍA

- CRC. Documento de formulación del problema del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles». Página 42. https://crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-formulacion-problema-identificacion-medidas-mitigar-fraude-cibernetico-servicios-moviles.pdf
- CRC. Documento del estudio sobre «El rol de los servicios OTT en el sector de las comunicaciones en Colombia - 2024». Página 203. Disponible en: https://www.crcom.gov.co/es/biblioteca-virtual/estudio-sobre-rol-servicios-over-top-ott-en-colombia-2024
- CRC. Proyecto regulatorio «Revisión de Medidas Aplicables a Servicios Móviles - Fase 2». Disponible en: https://crcom.gov.co/es/proyectos-regulatorios/2000-38-3-17-1
- CRC. Proyecto regulatorio «Revisión de los esquemas de remuneración móvil». Disponible en: https://crcom.gov.co/es/proyectos-regulatorios/2000-38-3-2
- CRC. «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». Disponible en: https://www.crcom.gov.co/sites/default/files/normatividad/00007285.pdf

- UIT. Recomendación UIT-T E.164 (11/2010). Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.164-201011-I!!PDF-S&type=items
- Asobancaria, Aval, Colcert, Cristóbal Fuentes, Plintron, Superintendencia de Industria y Comercio y Universidad Externado. Comentarios disponibles en el siguiente enlace: https://www.crcom.gov.co/es/noticias/proyectos-regulatorios/comentarios-documento-formulacion-proyecto-identificacion-medidas-fraude-cibernetico-servicios-moviles

9. CONSULTA

Teniendo en cuenta la metodología de Análisis de Impacto Normativo -AIN, con esta consulta la CRC se permite socializar con los agentes interesados las alternativas regulatorias identificadas para abordar las causas asociadas al problema definido en el marco del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles».

Con el objetivo de orientar esta consulta, se solicita a los agentes interesados contestar las siguientes preguntas al momento de realizar sus comentarios, los cuales se recibirán hasta el **22 de diciembre de 2025** mediante del correo electrónico medidasantifraude@crcom.gov.co:

9.1 Preguntas generales

- 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 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?

- ¿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?

- ¿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?

- ¿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?

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9.2 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?

- 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?

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

- ¿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?

- ¿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?

- ¿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?

- ¿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?

- ¿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?

- ¿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?

- ¿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?

- ¿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?

- ¿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?

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

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

- ¿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?

9.3 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?

- ¿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?

- ¿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?

- ¿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?

- ¿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)?

- ¿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?

- ¿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? ¿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?

- ¿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?

- ¿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?

- ¿Qué beneficios y riesgos identifica en la creación de un registro nacional único de números DNO? ¿Qué criterios deberían regir su actualización y acceso?

- ¿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?

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9.4 Frente a las temáticas enfocadas en la educación de la ciudadanía

- ¿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?

- ¿Qué cargas técnicas y económicas representaría para los PRST, los IT y los PCA implementar obligaciones de divulgación pedagógica frente al fraude cibernético?

- 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.)

- 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.)

- 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.)

- 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?

- 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?

- ¿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.

- ¿Qué variables o campos considera debería contener este sistema de trazabilidad para permitir análisis útiles?

- ¿Qué riesgos de seguridad o privacidad considera deben ser tenidos en cuenta al centralizar la información de PQR relacionadas con fraude?

- ¿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.)

9.5 Frente a las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

A partir de las temáticas identificadas en el presente documento, y en el marco del proceso de revisión del Régimen de Administración de Recursos de Identificación bajo un enfoque de simplificación regulatoria, resulta pertinente evaluar la pertinencia de ajustes adicionales. En este sentido, se plantean las siguientes preguntas orientadoras:

Reincidencia en el uso indebido de recursos de identificación para el envío de SMS.

- 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.

- 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.

- 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.

- 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.

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.

- 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.

- 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.

- 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.

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.

- 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.

- 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.

- 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.

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.

- ¿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.

- ¿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.

- ¿Qué consecuencias regulatorias adicionales considera adecuadas en caso de que los asignatarios no actualicen su información según lo estipulado? Por favor, justifique su respuesta.