COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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

Documento de respuesta a comentarios

Diseño Regulatorio

Julio de 2026

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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

De conformidad con lo establecido en el Decreto 1078 del 26 de mayo de 2015[1], la Comisión de Regulación de Comunicaciones (CRC) presenta al sector las respuestas a las observaciones y comentarios realizados por los agentes interesados a la propuesta regulatoria del proyecto denominado «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles», publicada para conocimiento y participación sectorial entre el 5 de junio de 2026 y el 23 de junio de 2026 en el sitio web de la Comisión[2].

Esta propuesta estuvo acompañada de la publicación de los siguientes documentos:

- Documento soporte: «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles».

- Proyecto de resolución «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones».

Dentro del plazo antes mencionado se recibieron comentarios, observaciones o sugerencias por parte de los siguientes agentes:

REMITENTE	ABREVIATURA
AXESNET S.A.S	**ALDEAMO**
CÁMARA COLOMBO AMERICANA, AMCHAM COLOMBIA	**AMCHAM**
ASOCIACIÓN NACIONAL DE EMPRESAS DE SERVICIOS PÚBLICOS Y COMUNICACIONES EN COLOMBIA	**ANDESCO**
ASOCIACIÓN NACIONAL DE EMPRESARIOS DE COLOMBIA	**ANDI**
ASOCIACIÓN BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA	**ASOBANCARIA**
BLIPBLIP	**BLIPBLIP**
BLIP-BLIP, INALAMBRIA y NEXVIA S.A.S. (comentarios conjuntos en un solo archivo)	**BLIP-BLIP, INALAMBRIA y NEXVIA**
BYTECOL TECHNOLOGY SYSTEMS SAS	**BYTECOL**

[1] Decreto 1078 de 2015, «Por medio del cual se expide el Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones», Artículo 2.2.13.3.2. (Publicidad de proyectos de regulaciones) compilatorio del Artículo 9° del Decreto 2696 de 2004.
[2] https://www.crcom.gov.co/es/proyectos-regulatorios/2000-41-7-1

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES	**CCIT**
COLOMBIA MÓVIL S.A.S.	**TIGO**
COMUNICACIÓN CELULAR COMCEL S.A.	**CLARO**
CLEARTECH S.A.	**CLEARTECH**
ASOCIACIÓN COLOMBIANA DE EMPRESAS DE TECNOLOGÍA E INNOVACIÓN FINANCIERA	**COLOMBIA FINTECH**
CRISTIAN CAMILO CANTILLO	**CRISTIAN CANTILLO**
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. E.S.P.	**ETB**
EXPERIAN COLOMBIA S.A.	**EXPERIAN**
GERMÁN CRUZ	**GERMÁN CRUZ**
GMS	**GMS**
HABLAME COLOMBIA S.A. E.S.P.	**HABLAME**
INALAMBRIA INTERNACIONAL SAS.	**INALAMBRIA**
INETUM	**INETUM**
JULIO NULDEMAR	**JULIO NULDEMAR**
NEXVIA S.A.S.	**NEXVIA**
PARTNERS TELECOM COLOMBIA S.A.S.	**PTC**
SAEM COLOMBIA S.A.S.	**SAEM**
SANDRA RODRÍGUEZ GUERRERO	**SANDRA RODRÍGUEZ**
SCAMZERO	**SCAMZERO**
SEGUROS BOLIVAR	**SEGUROS BOLIVAR**
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO	**SIC**
SINCH COLOMBIA S.A.S	**SINCH**
SISTEMAS SATELITALES DE COLOMBIA S.A. E.S.P.	**SSC**
SUMA MÓVIL S.A.S.	**SUMA**
THE CAMPAIGN REGISTRY	**CAMPAIGN REGISTRY**
CIFIN S.A.S. - TRANSUNION	**TRANSUNION**

Con posterioridad al término establecido se recibieron comentarios de la CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO (**CCCE**) y de la SUPERINTENDENCIA FINANCIERA DE COLOMBIA (**SFC**), 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 la decisión final a ser adoptada en el marco de este proyecto regulatorio.

Para facilitar la comprensión de este documento, la CRC presenta exclusivamente los apartes de cada comentario en donde se hacen propuestas, observaciones y cuestionamientos puntuales al proyecto de regulación sometido a discusión, los cuales se responden agrupados por temas. Lo anterior, sin perjuicio de la posibilidad de consultar los textos completos de cada documento, que se encuentran publicados en la página web de la Comisión[3].

[3] Documentos disponibles en la interacción 3 del micrositio del proyecto que se puede consultar en el siguiente enlace: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-41-7-1

Por otro lado, la Comisión advierte que el artículo 2.2.2.30.5. del Decreto 1074 de 2015 dispone lo siguiente:

> «Artículo. 2.2.2.30.5. Evaluación que debe realizar la autoridad que proyecta expedir un acto. La autoridad que se proponga expedir un acto administrativo con fines regulatorios deberá evaluar su posible incidencia sobre la libre competencia con base en el cuestionario que adoptará la Superintendencia de Industria y Comercio mediante una resolución de carácter general. Esa evaluación deberá realizarla antes de someter a consideración de la Superintendencia de Industria y Comercio el proyecto de acto regulatorio.
>
> La resolución que expida la Superintendencia de Industria y Comercio establecerá las preguntas centrales que deberá formularse la autoridad que proyecta expedir un acto administrativo. Con el fin de facilitar la evaluación, las preguntas podrán complementarse con ejemplos o situaciones que sirvan para ilustrar el tipo de efectos de una regulación, perseguidos o no, que puedan restringir indebidamente la libre competencia».

De conformidad con lo establecido en el citado artículo 2.2.2.30.5. del Decreto 1074 de 2015, esta Comisión diligenció el cuestionario expedido por la Superintendencia de Industria y Comercio (SIC) mediante el artículo 5 de la Resolución SIC 44649 de 2010, con el fin de verificar si las disposiciones contempladas en la propuesta regulatoria publicada para comentarios del sector tienen efectos en la competencia.

En observancia de lo definido en el artículo 7 de la Ley 1340 de 2009, el artículo 2.2.2.30.8. del Decreto 1074 de 2015 y la Resolución SIC 44649 de 2010, el 24 de junio de 2026 la CRC envió a la SIC el proyecto regulatorio publicado con su respectivo documento soporte, y anexó el cuestionario dispuesto por tal entidad para proyectos regulatorios de carácter general, así como, los diferentes comentarios a la propuesta regulatoria que fueron recibidos durante el plazo establecido[4].

La Superintendencia, en sede del mencionado procedimiento de abogacía de la competencia, mediante comunicación identificada con el radicado SIC 26-259501- -1-0 del 9 de julio de 2026, emitió su concepto sobre la propuesta regulatoria publicada, a propósito de lo cual planteó las siguientes recomendaciones:

> «(…)
>
> **5. RECOMENDACIONES**
>
> Por las razones expuestas, se recomienda a la CRC, en relación con el proyecto:
>
> • Considerar la conveniencia de complementar la justificación técnica y económica en relación con los siguientes aspectos: (i) explicar cómo el análisis de costos permite valorar la proporcionalidad económica de las cargas previstas, tanto por subtemática como de manera agregada; (ii) precisar si la distribución

[4] Estos documentos fueron recibidos en la mencionada superintendencia bajo radicado con el No. 26-259501- -00000-000.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

de dichos costos entre los distintos agentes del ecosistema fue considerada en la selección de alternativas; (iii) procurar, en la medida en que la información disponible lo permita, una estimación cuantitativa de los beneficios esperados; y (iv) justificar la suficiencia del plazo de (6) meses previsto para la implementación del nuevo ecosistema A2P; en caso de que, a partir de dicho análisis, se identifique que el plazo podría no resultar suficiente para una implementación ordenada, se valore la conveniencia de ampliarlo.

• Procurar un tratamiento claro, sistemático y suficiente de las observaciones presentadas por terceros, especialmente de aquellas con posible incidencia en la libre competencia económica.

(…)»

Al respecto, debe decirse que, con fundamento en el artículo 7 de la Ley 1340 de 2009, la CRC se pronunció puntualmente frente a cada una de las recomendaciones en la parte motiva del acto administrativo por medio del cual se adopta la respectiva decisión.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

1. Comentarios generales 8

2. Sobre las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS) 34

2.1 Sender ID 34

2.2 Código Corto A2P 58

2.3 Validador centralizado: forma de selección, competencias y funciones 82

2.4 Bloqueo o etiquetado de mensajes 123

2.5 KYC 125

2.6 Plantillas (Template ID) 138

2.7 Obligación de constituir una sucursal en Colombia y cargas para sociedades internacionales 164

2.8 Tratamiento de mensajes OTP, autenticación, seguridad y comunicaciones críticas 168

2.9 Atribución de responsabilidad 179

2.10 Tráfico P2P 185

2.11 Reportes de información 205

2.12 Comité Técnico de Seguimiento y coordinación operativa 212

3 Sobre las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz 216

3.1 Bloqueo de llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano 216

3.2 Monitoreo de llamadas que derivan en la etiqueta de «Alerta de llamada sospechosa» 243

3.3 Etiquetado de llamadas con fines publicitarios 258

3.4 Lista de No Originación (DNO) 268

3.5 Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM 272

4 Sobre las temáticas enfocadas en la educación de la ciudadanía 280

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

5 Sobre las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación 288
5.1 Consecuencia para reincidentes 288
5.2 Oposición a la interconexión 294
6 Otras temáticas 299
6.1 Régimen de transición 299
6.2 Remuneración/fases del proyecto/AIN 306
6.3 Definiciones 318
6.4 Portabilidad 321
6.5 Sobre los OMV 323

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1. Comentarios generales

ALDEAMO

Advierte que las medidas no consideran la capacidad técnica y de adaptación de los grupos dedicados al fraude, quienes operan al margen de la regulación, evaden filtros, usan múltiples empresas y suplantan identidades, por lo que no se registrarían como PCA ni cumplirían controles formales. Sostiene que reducir el fraude exige una estrategia conjunta con controles dinámicos y actualización permanente, además de una revisión de la estructura de precios de los SMS. Cuestiona la falta de concertación previa y advierte efectos no deseados, como el aumento del fraude por SMS P2P, mayores barreras para las pymes usuarias de SMS y una reducción de integradores tecnológicos que concentraría el mercado en los operadores móviles y fortalecería el duopolio.

ANDESCO

Cuestiona el test de proporcionalidad: estima las medidas potencialmente idóneas para reducir el fraude en SMS y voz, pero afirma que la CRC no demuestra su eficacia ni cuantifica la reducción esperada, no acredita que sean la alternativa menos gravosa, no evalúa ex post las herramientas vigentes y no cuantifica los costos, lo que impide verificar que los beneficios los superen y podría hacer inviable la operación de agentes pequeños y medianos. Señala que el proyecto no analiza el efecto de sustitución del fraude hacia canales no cubiertos (OTT, correo, VoIP), por lo que las medidas podrían desplazar el fraude sin reducirlo. Propone una coordinación formal con el MinTIC, la SFC, la SIC y el COLCERT para extender las obligaciones antifraude a los canales OTT, y fortalecer las herramientas existentes (suspensión provisional de códigos cortos, recuperación de recursos, monitoreo de tráfico por los PRST y coordinación con COLCERT y la Fiscalía).

ANDI

Advierte que el proyecto podría producir efectos contrarios a su finalidad: impone cargas potencialmente desproporcionadas frente a alternativas menos restrictivas e igualmente eficaces, comprometiendo la neutralidad tecnológica, la continuidad de servicios críticos y la seguridad digital, y puede generar tensiones con la libertad de empresa y la libre competencia.

Señala riesgos no intencionados derivados del propio diseño (interrupción de controles antifraude críticos, nuevos puntos únicos de falla, mayor dependencia de infraestructuras de terceros e incentivos a la adaptación del fraude), por lo que recomienda una evaluación ex ante y ex post del riesgo sistémico y soportar las medidas en un Análisis de Impacto Normativo robusto e integral.

Solicita, además, un análisis específico de protección de datos que sujete las medidas a los principios de la Ley 1581 de 2012, defina el rol del validador en el tratamiento de datos, exija una evaluación de impacto previa, fije reglas de gobernanza, conservación y acceso, y limite la validación de plantillas a metadatos o elementos estructurales, evitando el acceso al contenido de las comunicaciones.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ASOBANCARIA

Advierte el riesgo de desplazamiento del fraude hacia canales no contemplados (OTT, mensajería instantánea, ingeniería social híbrida) y pide un diseño integral y dinámico con medidas que mitiguen esa migración. Propone un mandato expreso de articulación interinstitucional entre la CRC, la URF, la SFC y la SIC para reglas comunes de prevención, reporte, trazabilidad y atención al usuario, y evaluar un intercambio de información en tiempo real entre telecomunicaciones y sector financiero.

Solicita reforzar las garantías de finalidad, minimización, seguridad y reserva sobre la información de los asignatarios, en armonía con la Ley 1581 de 2012.

Considera desproporcionadas las cargas de los artículos 2, 6, 7, 12 y 19 (en especial la transición de seis meses), por lo que pide pruebas piloto y etapas escalonadas. Reclama definir con precisión quién clasifica una línea o identificador como fraudulento y bajo qué criterios, con plazos de reclasificación y canales para reportar falsos positivos; precisar la periodicidad, responsables y estándares de actualización de las bases de información (listas DNO, etiquetado, validadores, registros de originadores); e incorporar trazabilidad técnicamente verificable, interoperable y auditable, indicadores de desempeño (falsos positivos, disponibilidad, tiempos de entrega), protocolos de comunicación al usuario ante fallas y mesas intersectoriales permanentes.

Finaliza su intervención realizando unas recomendaciones adicionales. Concretamente, **ASOBANCARIA** dice que, con el fin de mitigar los riesgos identificados, se recomienda complementar el Proyecto con medidas que fortalezcan el enfoque preventivo, sin afectar la continuidad operativa ni la efectividad de los controles antifraude existentes. En particular, considera positiva la incorporación de medidas como las siguientes:

• Mecanismos de redundancia y validación alternativa frente a fallas de los componentes centralizados.

• Protocolos de comunicación al usuario en escenarios de falla o de inconsistencias en el etiquetado.

• Mesas intersectoriales permanentes para la gestión coordinada de incidentes de fraude.

• La adopción, por parte de la CRC, de un enfoque de evaluación ex ante y ex post del riesgo sistémico asociado a las medidas, que asegure que los beneficios esperados superen los impactos potenciales sobre la estabilidad, la continuidad y la seguridad del ecosistema.

BLIPBLIP

Solicita no expedir el proyecto en su estructura actual y reformularlo por completo para analizar sus impactos económicos, operativos y funcionales sobre los ecosistemas de A2P y voz. Advierte que, aunque atiende una problemática real, las medidas podrían generar cargas burocráticas, barreras de acceso y pérdida de volumen de mensajes A2P sin atacar directamente el fraude. Pide mantener el

enfoque regulatorio, pero promoviendo la coordinación entre actores y procesos estandarizados, eficientes y uniformes que permitan cumplir sin obstaculizar el acceso al ecosistema.

CLARO

Indica que, si bien comparte la necesidad de adoptar medidas orientadas a proteger a los usuarios frente a las distintas modalidades de fraude cibernético, el documento soporte no presenta evidencia suficiente que permita concluir que las medidas propuestas generarán una reducción efectiva y sostenible del fraude que afecta a los usuarios de los servicios de comunicaciones.

En efecto, señala que la propuesta parte de la premisa según la cual el fortalecimiento de los mecanismos de validación, autenticación y trazabilidad asociados a los servicios de voz y SMS reducirá significativamente la ocurrencia de eventos fraudulentos. No obstante, indica que el documento no incorpora análisis cuantitativos que permitan demostrar que las medidas planteadas tendrán como resultado una disminución real de las conductas fraudulentas y no se traduzcan simplemente en una modificación del canal utilizado para ejecutarlas.

Esta distinción resulta particularmente relevante para **CLARO** si se considera que el fraude cibernético es un fenómeno dinámico que evoluciona permanentemente en función de los costos, riesgos y barreras que enfrentan los actores maliciosos. En consecuencia, es esperable para ese operador que las actividades fraudulentas migren hacia otros canales que presenten menores restricciones regulatorias o menores costos de operación, luego de realizar estas cuantiosas inversiones.

Señala que, precisamente, diversos actores del sector han advertido que una parte creciente de los eventos de fraude actualmente se desarrolla a través de plataformas OTT, aplicaciones de mensajería instantánea, redes sociales, aplicaciones de comercio electrónico, servicios de mensajería empresarial y otros entornos digitales que no se encuentran cubiertos por las medidas propuestas en el presente proyecto regulatorio. Sin embargo, resalta que el documento soporte no contiene un análisis de sustitución o desplazamiento del fraude entre canales de comunicación.

En consecuencia, es necesario para **CLARO** que antes de adoptar nuevas obligaciones, se complemente el análisis de impacto normativo con una evaluación específica de los efectos de sustitución entre canales, así como con evidencia que permita estimar la reducción efectiva del fraude esperada, diferenciándola de una simple migración de las actividades fraudulentas hacia plataformas no sujetas al ámbito de aplicación de la presente regulación.

La ausencia de este análisis impide concluir, para **CLARO**, que las medidas propuestas resultan efectivas, necesarias y proporcionales para alcanzar el objetivo perseguido, especialmente cuando los costos regulatorios asociados a su implementación son significativos y recaen exclusivamente sobre un subconjunto de los actores que participan en el ecosistema digital.

La regulación propuesta parece partir del supuesto de que el fraude es inherente al canal SMS o voz, cuando en realidad el fraude es un fenómeno transversal al ecosistema digital que se adapta continuamente a los mecanismos de control implementados por los distintos actores.

Asimismo, indica que el documento soporte no presenta información que permita determinar aspectos fundamentales para la evaluación de la política pública, tales como:

- El número de suspensiones provisionales decretadas.
- Los tipos de conductas que dieron lugar a dichas medidas.
- El volumen de tráfico involucrado.
- La reducción efectiva de eventos fraudulentos atribuible a estas actuaciones.
- El tiempo promedio de reacción frente a reportes de fraude.
- Los resultados obtenidos en términos de protección de usuarios.

La ausencia de esta información impide determinar si las herramientas actualmente disponibles han resultado efectivas, si requieren ajustes regulatorios o si, por el contrario, existen oportunidades para fortalecer su aplicación antes de introducir nuevos mecanismos regulatorios de carácter estructural.

Menciona que el documento tampoco demuestra que medidas como el validador centralizado, los mecanismos de Sender ID o las nuevas obligaciones tecnológicas propuestas generen resultados superiores a los obtenidos mediante el fortalecimiento de los esquemas de monitoreo, detección temprana, bloqueo de tráfico irregular y suspensión provisional actualmente disponibles.

COLOMBIA FINTECH

Observa que, conforme al artículo 20, las medidas de voz y P2P entran en vigor con la publicación, mientras el ecosistema A2P queda sujeto a la Fase II, y que el numeral 19.1.4.3 dispone que los códigos cortos no consolidados al vencer la transición pasarán a estado «no implementado» e iniciarán recuperación, sin excepción para entidades financieras con comunicaciones críticas activas.

Advierte que interrumpir OTP, alertas de seguridad y notificaciones transaccionales impactaría la seguridad de las operaciones, por lo que solicita una cláusula explícita de continuidad operativa que garantice la mensajería crítica del sector financiero durante toda la transición, con prórroga automática para las entidades que acrediten migración en curso.

ETB

Sostiene que el papel del regulador no se limita a reforzar obligaciones sobre los operadores, sino a promover un marco integral con participación coordinada de todos los actores (PCA, OTT, integradores, carriers).

Pide que el análisis de impacto garantice necesidad, proporcionalidad, eficiencia, sostenibilidad y mínima carga, evaluando los efectos sobre la competencia, la inversión, el mercado y agentes como los OMV, y evitando incentivos de migración del riesgo.

Critica que el proyecto concentre las cargas regulatorias, económicas y sancionatorias en los PRSTM pese a que el fraude se origina en un ecosistema más amplio (OTT, mensajería, agregadores, integradores internacionales), cuando los PRST no controlan el contenido ni el origen de las campañas, configurando una asimetría regulatoria.

Propone un modelo de corresponsabilidad funcional basado en el control efectivo, ampliando progresivamente el alcance a PCA, integradores tecnológicos, OTT, agregadores y carriers internacionales (ejecutando las medidas prioritariamente en el punto de originación) y fortalecer la coordinación con el MinTIC, la SFC, la SIC y el COLCERT para abordar los canales OTT.

GMS

Propone complementar el proyecto con recomendaciones técnicas por capas: en red y señalización, firewalls de SMS con inteligencia artificial y aprendizaje automático sobre tráfico SMPP y SS7, y firewalls de señalización SS7 y Diameter en los puntos de interconexión; un firewall de voz contra modalidades como CLI spoofing, Wangiri y bypass internacional; un gateway centralizado de mensajería A2P (infraestructura SMSC) que dé visibilidad al regulador sobre el tráfico A2P internacional; un firewall de datos que asegure la entrega de OTP internacionales por canales legítimos; API de red para servicios como verificación de número o detección de cambio de SIM; y un canal estandarizado de reporte ciudadano de SMS fraudulentos, integrado con el firewall, que alimente las reglas de detección y las listas negras compartidas entre operadores.

Resalta que la efectividad aumenta con mecanismos de intercambio de inteligencia sobre amenazas, complementando el Comité Técnico propuesto.

GERMÁN CRUZ

Propone herramientas de transparencia y control para los usuarios: una consulta pública que, al ingresar un código corto, identifique las empresas que lo usan y los tipos de mensajes, y mecanismos para que se reporten las asignaciones y exista trazabilidad sobre los responsables del envío.

Plantea controles preventivos previos al envío masivo, mediante análisis de las plantillas con inteligencia artificial para detectar spam, phishing, amenazas o incumplimientos, con alertas al remitente, bloqueo de campañas recurrentes y reporte a la CRC; el almacenamiento temporal de los mensajes masivos para facilitar investigaciones; y un mecanismo sencillo de recepción de quejas asociado al código corto que permita verificar la fecha y hora del envío y determinar su legitimidad.

En general, aboga por un modelo más preventivo y activo basado en controles tecnológicos y análisis automático de contenido antes de la transmisión.

INALAMBRIA

Sostiene que el proyecto trata el canal SMS como un factor de riesgo en sí mismo y propone diferenciar las categorías de mensajes según su nivel de riesgo (siendo los que contienen URLs los de mayor riesgo), pues no resulta proporcional someter a idénticos controles un aviso transaccional, una alerta de autoridad, una confirmación de cita médica o un OTP.

Advierte que, aunque su motivación es el fraude financiero, la regulación afecta otros derechos constitucionales (información —art. 20—, salud —art. 49—, vida e integridad —arts. 11 y 12— y acceso a servicios públicos —art. 365—) y recae sobre todos los usuarios del ecosistema, por lo que pide un análisis de proporcionalidad que valore beneficios, afectaciones a otros derechos y alternativas menos restrictivas.

Señala que las exigencias de registro, códigos cortos y SENDER ID pueden constituir una barrera económica y administrativa para las pymes, contraria a la inclusión digital, y solicita un régimen simplificado para pequeños remitentes que permita compartir recursos de identificación agrupados de forma controlada por los integradores y procedimientos abreviados con menores cargas documentales.

NEXVIA

Plantea lo que considera una paradoja regulatoria: las facultades de suspensión, recuperación, bloqueo y desconexión que se conceden a los PRST y al validador afectarían de manera masiva, automática e indiscriminada comunicaciones esenciales para el consumidor, sacrificando los derechos de los mismos usuarios que se busca proteger.

Fundamenta su observación en los artículos 78 y 365 de la Constitución, la Ley 1341 de 2009 (arts. 2 y 53), la Ley 2300 de 2023 y la Ley 1581 de 2012, y advierte que por el SMS circulan claves OTP, alertas de fraude, confirmaciones de comercio electrónico, recordatorios médicos y notificaciones de autoridades, de modo que cada suspensión repercute sobre usuarios ajenos a la conducta investigada. Sostiene que la continuidad del servicio es una garantía exigible (art. 365) que las facultades de suspensión instantánea, sin transición ni régimen de continuidad para comunicaciones críticas, contrarían; que la afectación es especialmente grave y discriminatoria (art. 13) para la población sin internet móvil que depende del SMS para acceder a su banco, su EPS y las autoridades; y que el consumidor no fue informado ni consultado.

Solicita que la resolución definitiva incorpore salvaguardas mínimas en favor del usuario final (**aunque no las determina de manera particular más allá de los comentarios incorporados a lo largo del texto recibido**), advirtiendo que «Mientras subsista la posibilidad de que las comunicaciones esenciales de millones de usuarios sean interrumpidas como consecuencia automática de una medida

dirigida contra un intermediario, y por decisión de un operador que es a la vez juez y parte, la invocación de la protección al usuario operará como un fundamento meramente nominal, desmentido por los efectos reales de la regulación».

SAEM

Manifiesta un interés directo como integrador tecnológico de SMS A2P, ya que es asignatario del código corto A2P (art. 6.4.1.3) y sujeto, además, a las medidas de voz (art. 2.1.10.7.2.2) y a la ampliación del RNE al correo (art. 2.1.18.1), con obligaciones de financiar el validador (art. 6.13.1.2), adelantar KYC (art. 6.13.3.1), integrarse con el validador (art. 6.13.4.5.2), participar en el CTLFSM (art. 2.1.10.7.3) y el CTS (art. 6.13.5.1) y consolidar sus códigos cortos (art. 19).

Sostiene que la cadena A2P formal opera bajo contratos, debida diligencia y trazabilidad, mientras que el fraude se origina mayoritariamente por fuera del perímetro regulado —SMS spoofing, numeración ilegal y rutas grises internacionales, plataformas y agregadores clandestinos del exterior, SIM farms, simboxes y «SMS blasters», y suplantación mediante inteligencia artificial—, citando cifras de la Global Anti-Scam Alliance y de la GSMA que atribuyen el crecimiento del fraude a la suplantación y la IA y no a los actores regulados.

Alega la afectación de la libertad económica (art. 333), la confianza legítima, la proporcionalidad y necesidad, y la libre competencia (Ley 1340 de 2009), y pide que la SIC examine en abogacía de la competencia el diseño del validador (selección por los PRSTM, financiación por los integradores y monopolio de hecho) y las facultades de suspensión unilateral del PRST.

Solicita concentrar la estrategia en las verdaderas fuentes del fraude, mediante auditoría a las plataformas que transaccionan desde el exterior y cooperación con operadores, autoridades y organismos como la GSMA.

SANDRA RODRÍGUEZ

Señala que las empresas integradoras contratan con personas jurídicas constituidas (entidades financieras, de cobranza y demás PCA) sometidas a debida diligencia y verificación, y que la Ley 2300 de 2023 ya redujo su capacidad de contacto y su tráfico, deteriorando su situación económica.

Sostiene que las nuevas cargas se imponen sin evidencia de que el origen principal del fraude esté en los códigos y numeraciones asignados conforme al marco colombiano, cuando la experiencia y los estudios muestran que el fraude proviene de numeraciones ilícitas, spoofing, plataformas clandestinas y herramientas de inteligencia artificial, y que el bloqueo tradicional tiene efectividad limitada frente a modalidades como el smishing y los números desechables.

Considera que restringir aún más a quienes actúan dentro del marco legal no ataca las verdaderas fuentes del fraude y puede afectar la sostenibilidad de un sector de empresas emergentes y medianas, por lo que pide aplicar los principios de necesidad y proporcionalidad y un análisis costo-beneficio.

SCAMZERO

Propone complementar los controles de red con mecanismos de protección para el usuario final y establecer un estándar homogéneo de monitoreo entre los actores, unificando variables y criterios de detección, con el fin de superar las limitaciones de los controles actuales (principalmente reactivos y no predictivos) y cerrar la brecha de protección que se produce cuando los mensajes y llamadas fraudulentas superan los filtros de red y llegan al usuario final sin una capa adicional de defensa.

SINCH

Valora positivamente el enfoque de corresponsabilidad y gestión integral de la cadena de valor por su carácter sistémico, pero advierte la complejidad de supervisar a múltiples actores y el riesgo de que la responsabilidad se diluya si las reglas no son suficientemente claras ante una filtración de tráfico fraudulento.

Sostiene que endurecer la regulación del SMS hará que la delincuencia migre hacia canales IP como WhatsApp, por lo que se requiere una visión convergente que involucre a las plataformas OTT; y que, desde una perspectiva comercial, la sobrerregulación del SMS dificulta su operatividad frente a competidores como WhatsApp, con una reducción crítica del volumen que afectaría la rentabilidad de operadores y agregadores y comprometería la viabilidad de largo plazo del canal.

TIGO

Considera positiva la diferenciación de roles (integrador tecnológico, PCA, código corto A2P único por agente y SENDER ID por marca) y formula dos precisiones en mensajería: (a) que se aclare la extensión del régimen de trazabilidad, KYC y control a la numeración no geográfica E.164 (numeración larga) usada para SMS (sustituible con los códigos cortos para fines de fraude) o se disponga su devolución y la restricción de su uso para A2P, a fin de evitar que los agentes migren a ese canal menos regulado; y (b) que se preserve expresamente la facultad de los PRST de ofrecer y cobrar servicios de dimensionamiento y capacidad adicional que hoy permite negociar la Resolución CRC 6522 de 2022, de manera independiente a los recursos destinados a la validación centralizada.

En voz, sostiene que el declive del mercado es estructural y acelerado, por lo que obligar a cuantiosas inversiones de CAPEX y OPEX sobre un canal en desuso configura ineficiencia económica; que los PRSTM ya operan capacidades antifraude en voz y que el modelo les exige inversiones adicionales (validación en línea frente al RNE, ampliación de patrones, etiquetado y verificación de identidad CLI) con costos elevados y sin impacto proporcional, pues el fraude se origina y controla en buena medida fuera del PRST terminante.

Solicita trasladar al cliente corporativo u originador el deber de consultar el RNE y abstenerse de contactar a los inscritos (con un llamado a la SIC para fijar reglas generales aplicables a las empresas), eliminando la obligación de validación y bloqueo del RNE en tiempo real a cargo del PRST en el tráfico de voz.

TRANSUNION

Sugiere que la CRC promueva, bajo su supervisión y en coordinación con el ecosistema, una hoja de ruta de autorregulación sectorial para recuperar la confianza.

Reconoce que las medidas de voz (suplantación de CLI, etiquetado, monitoreo y no originación) son avances importantes, pero plantea que el diseño de mecanismos de confianza en voz puede requerir una evolución gradual, flexible y coordinada que incorpore verificación de identidad de organizaciones legítimas, etiquetas positivas, información contextual sobre la finalidad de la llamada, controles anti-suplantación y métricas de reducción de fraude y falsos positivos.

Pide preservar flexibilidad para una convergencia futura entre validación de identidad empresarial, KYC, SENDER ID, validación de marcas, gobierno de plantillas, identidad de llamadas, inteligencia antifraude y educación, evitando silos rígidos entre voz y mensajería, y resalta que los beneficios son mayores cuando las soluciones se ofrecen nativamente en la red y no mediante aplicaciones OTT, sin que ello implique adoptar una única tecnología. Cita como referentes internacionales las experiencias de Brasil (ANATEL y ABR Telecom), Estados Unidos (FCC y ATIS) y Canadá (CRTC).

PTC

Recuerda que el artículo 19 de la Ley 1341 de 2009, modificado por el artículo 15 de la Ley 1978 de 2019, exige que la regulación de la CRC promueva la simplificación regulatoria en igual jerarquía que la inversión y la protección de los usuarios. Comparte el propósito antifraude, pero advierte que algunos puntos del diseño —en particular la creación del validador centralizado— suponen costos adicionales y excesivos para los PRST cuando estos no son los responsables de la generación del tráfico. En la misma línea, aunque está de acuerdo con la creación del SENDER ID y con dos instancias de coordinación de objeto parcialmente coincidente (CTLFSM y CTS), considera que no deberían implicar la contratación de terceros, sino la asunción de esas funciones por la propia CRC.

Reafirma que los PCA e Integradores Tecnológicos que son asignatarios de numeración sí están sometidos a las obligaciones legales y regulatorias derivadas de la asignación y uso de los códigos cortos y de la gestión del tráfico A2P, pues la Resolución CRC 5050 de 2016 establece deberes exigibles a todos los asignatarios; por ello no resulta jurídicamente procedente que pretendan sustraerse de tales deberes alegando no ser sujetos regulados de manera integral, ya que la asignación de un recurso escaso es fuente de obligaciones y no una simple habilitación. En consecuencia, esos agentes asumen

responsabilidades directas, e incluso solidarias cuando corresponda, sin que las cargas recaigan exclusivamente sobre los PRST.

Indica que los PRST ya están sometidos a un régimen integral de prevención del fraude (artículo 2.1.10.7 de la Resolución CRC 5050 de 2016) anterior a este proyecto, y que el proyecto les adiciona un extenso catálogo de obligaciones (monitoreo P2P, respuesta escalonada, bloqueo de CLI, listas DNO, etiquetado, participación en el CTLFSM y el CTS, integración con el validador), mientras que las obligaciones equivalentes de los PCA e IT se concentran en el KYC y el uso correcto de las plantillas. Como el PRST carece de visibilidad sobre el contenido, la campaña, la relación comercial y el originador real —que sí controla el PCA y, de manera derivada, el IT—, solicita que en el artículo 6.13.4.4 se incorpore una presunción según la cual, salvo prueba en contrario, la responsabilidad primaria por el contenido fraudulento, engañoso o no autorizado recae en el asignatario del SENDER ID y, de manera subsidiaria, en el asignatario del código corto A2P cuando se acredite que facilitó o permitió el tráfico irregular con conocimiento de la irregularidad. Sostiene que esa precisión es consistente con las causales de recuperación ya diferenciadas del SENDER ID (artículo 6.12.3.2) y del código corto A2P (artículo 6.4.3.2) y evita trasladar al PRST cargas de verificación que no puede asumir.

BLIPBLIP, NEXVIA E INALAMBRIA

Como petición central solicitan no expedir el proyecto en su forma actual y reformularlo de manera integral, pues el número de incongruencias, contradicciones internas y efectos colaterales es de tal magnitud que las correcciones parciales resultan insuficientes; el proyecto debería reconstruirse desde sus premisas, a partir de la realidad operativa del negocio A2P, de un análisis de impacto que cuantifique sus efectos y de un diálogo técnico con todos los actores.

Los agentes exponen una premisa compartida: comparten el fin y objetan los medios. Afirman operar la primera línea de detección (filtran contenidos, bloquean cuentas, identifican suplantación, SIM boxing y SMS pumping) y sostienen que el tráfico fraudulento es una fracción menor del total, por lo que el reto es atacar esa fracción sin poner en riesgo el tráfico legítimo. Consideran que el proyecto invierte esa lógica: en lugar de fortalecer la inteligencia compartida y las herramientas tecnológicas (incluida la inteligencia artificial), opta por una arquitectura de control previo, validadores privados, autorización de contenidos y sanciones de desconexión que recaen sobre los agentes formales y no sobre los defraudadores, con el resultado previsible de que el fraude no se reduce y el canal legítimo se encarece, se ralentiza y se contrae.

Alegan un error de diagnóstico en el sentido de sostener que se combate con burocracia (nuevos comités, procesos, aprobaciones previas y entidades) un problema que es tecnológico y de precios, lo que disminuiría el volumen de mensajería A2P legítima; que quien vive del fraude nunca se registrará ante el validador ni someterá plantillas; y que la «recuperación de códigos», reconocida como ineficaz, se convierte en el eje de toda la regulación.

Afirman que, al exigir conexión directa e infraestructura propia, prohibir el tráfico en nombre de terceros, negar el SENDER ID a los proveedores de infraestructura y limitar a los IT a un único código, el proyecto vuelve obsoleta la figura del IT, fuerza la desintermediación, concentra el mercado en los operadores (cada recuperación operaría como transferencia forzosa de clientela al PRST integrado) y elimina un eslabón que ha permitido masificar el SMS.

Señalan que el proyecto asume que los PRST son infraestructura neutral, cuando también son asignatarios masivos de códigos cortos, compiten en contenidos y han sido objeto de recuperación por las mismas causales que el proyecto agrava solo para los PCA e IT independientes, de modo que la consecuencia agravada opera en una sola dirección; agregan que, tras la integración Tigo–Movistar, la red móvil es una instalación esencial cuya facultad de exclusión opera como barrera de entrada definitiva.

Indican que existen unos efectos colaterales sistémicos: (i) migración del fraude de A2P a P2P, al concentrar los controles en el A2P; (ii) desconexión de Colombia, pues la exigencia de NIT o sucursal, sumada a la prohibición de cursar tráfico de terceros, clausuraría las comunicaciones transaccionales globales de agregadores internacionales (mencionan a Microsoft, SAP, Salesforce, Google, Meta, Uber, Didi, Temu y Siigo), que dejarían de entregar OTP, confirmaciones y alertas; (iii) migración a canales OTT no regulados (WhatsApp), fuera de la jurisdicción y los instrumentos de la CRC, desconociendo que el SMS llega a todo usuario con cobertura 2G a 5G sin datos ni aplicación; (iv) exclusión de las pequeñas y medianas empresas y de los negocios en territorios apartados; y (v) afectación de las comunicaciones críticas y del usuario final, pues el encadenamiento entre código corto, SENDER ID y plantilla, junto con la unicidad y el arrastre de la recuperación, haría recaer las consecuencias sobre terceros inocentes (financieras, salud, plataformas), con un plazo de treinta días hábiles insuficiente para migrar y una interrupción de OTP y alertas que amplificaría el riesgo en lugar de mitigarlo.

Advierten la existencia de incongruencias normativas y contradicciones internas: (1) contradicción con la propia estrategia de simplificación de la CRC; (2) contradicción con la doctrina de corrección de asimetrías de la Resolución CRC 8144 de 2026, que cita en el sentido de «preservar o restablecer el equilibrio que debe existir entre aquellos actores que abrigan intereses legítimos contrapuestos»; (3) asimetría en los plazos de transición (la Resolución 8144 concedió meses con pruebas técnicas a los operadores, mientras el proyecto otorga plazos de diez y quince días hábiles para decisiones estructurales y treinta días hábiles a terceros inocentes); (4) contradicción entre la unicidad del código corto y el régimen de reincidencia, pues si cada agente solo puede tener un código, la recuperación lo desconecta desde el primer instante y la suspensión por segunda y la terminación por tercera presuponen una pluralidad prohibida; (5) contradicción entre el documento soporte y el articulado, ya que el soporte ilustra el SENDER ID con formatos diferenciados por propósito («Banco XX – Citas», «Banco XX – Transacciones», «Banco XX – Mercadeo»), granularidad que el articulado imposibilita al limitar la asignación a un único SENDER ID por NIT; y (6) ausencia de análisis de impacto que cuantifique las migraciones masivas, la devolución de recursos en operación y la consolidación de códigos con usuarios activos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Proponen un modelo alternativo propuesto: reserva estatal de la coerción (que las suspensiones, bloqueos, recuperaciones y desconexiones las ordene solo la CRC mediante acto motivado y con derecho de defensa, limitando a los PRST y al validador a detectar y reportar); continuidad del servicio como principio (portabilidad operativa inmediata del SENDER ID, continuidad transitoria del tráfico de terceros inocentes y pluralidad de códigos como redundancia); identificación sobre recursos existentes (aprovechar la Ley 2300 sin crear recursos paralelos); e inteligencia compartida e inclusiva (CTLFSM con membresía plena de PCA e IT y una plataforma de alertas en tiempo real).

Formulan las siguientes solicitudes concretas: (1) reformular integralmente el proyecto; (2) reformular o eliminar el régimen del validador centralizado, o sustituirlo por un esquema de detección distribuida con decisión estatal; (3) eliminar la unicidad del código corto A2P y la consolidación forzosa (artículos 6.4.1.4, 6.4.2.2.2 y 19.1.5); (4) eliminar la suspensión y desconexión unilateral por el PRST (Parágrafo 4 del artículo 6.1.1.8) y reservar toda medida restrictiva a la CRC; (5) sustituir la autorización previa de plantillas por un esquema de etiquetado y eliminar la renovación mensual obligatoria; (6) preservar la figura del Integrador Tecnológico y el modelo de agregación, permitiendo el tráfico en nombre de terceros y la identificación de remitentes internacionales a través del agente local, sin exigir sucursal; (7) incorporar a los PCA e IT al CTLFSM con voz y voto; (8) publicar un análisis de impacto normativo antes de expedir la resolución; y (9) convocar una mesa técnica con PCA e IT.

Respuesta CRC:

En esta sección fueron agrupados los comentarios generales presentados por **ALDEAMO**, **ANDESCO**, **ANDI**, **ASOBANCARIA**, **BLIPBLIP**, **CLARO**, **COLOMBIA FINTECH**, **ETB**, **GMS**, **GERMÁN CRUZ**, **INALAMBRIA**, **NEXVIA**, **SAEM**, **SANDRA RODRÍGUEZ**, **SCAMZERO**, **SINCH**, **TIGO**, **TRANSUNION**, **PTC**, así como los comentarios generales que se desprenden del escrito conjunto presentado por **BLIPBLIP**, **NEXVIA** e **INALAMBRIA**. Revisadas dichas intervenciones, la Comisión identifica tendencias coincidentes que agrupa en los ejes temáticos que se desarrollan a continuación. Los comentarios que, además de las consideraciones generales, versan sobre medidas específicas del proyecto serán abordados en el capítulo temático correspondiente de este documento, según se indica en cada caso, en aras de evitar repeticiones y así garantizar una respuesta integral y motivada a la totalidad de las observaciones recibidas.

1. Sobre el riesgo de sustitución o migración del fraude hacia canales no cubiertos por el proyecto (OTT) y el alcance del ámbito de aplicación

ALDEAMO, **ANDESCO**, **ASOBANCARIA**, **CLARO**, **ETB**, **SINCH** y el escrito conjunto de **BLIPBLIP**, **NEXVIA** e **INALAMBRIA** coinciden en advertir que el fortalecimiento de los controles sobre los servicios tradicionales de SMS y voz podría inducir la migración del fraude, e incluso del tráfico legítimo, hacia plataformas OTT, aplicaciones de mensajería instantánea, redes sociales, correo electrónico y llamadas VoIP, entornos que no se encuentran cubiertos por las medidas propuestas. A partir de esta premisa, algunos de estos agentes sostienen que el documento soporte carece de un análisis de sustitución entre canales y que, en ausencia de dicho análisis, no sería posible concluir que las medidas

propuestas resultan idóneas, necesarias y proporcionales. **ASOBANCARIA** y **ETB**, en la misma línea, solicitan que el diseño regulatorio adopte un enfoque integral y dinámico que contemple la evolución de las tipologías de fraude y que se fortalezca la coordinación con otras autoridades para extender la estrategia a los entornos digitales no regulados.

Al respecto, la Comisión recuerda que la dinámica evolutiva del fraude cibernético y la capacidad de adaptación de los actores maliciosos frente a los controles regulatorios y tecnológicos no son circunstancias ajenas al presente proyecto. Por el contrario, desde el documento de formulación del problema y el documento de alternativas regulatorias, este fenómeno fue identificado expresamente dentro de la causa denominada «Dificultad en la identificación y rastreo de los ataques cibernéticos», en la cual se reconoce que el internet actúa como habilitador transversal de la cadena del fraude y que los defraudadores migran hacia los canales con menores costos y controles. Precisamente por ello, el documento soporte no afirma que el fraude sea un fenómeno exclusivo o inherente a los canales SMS y voz; lo que acredita, con soporte empírico, es que estos canales concentran una afectación creciente, verificable y cuantificada para los usuarios colombianos: de acuerdo con la información remitida por la Superintendencia Financiera de Colombia, el valor de las reclamaciones por smishing y vishing pasó de $30.622 millones en 2022 a $92.235 millones en 2024, con una tendencia creciente y sostenida sin señales de estabilización, tal como se expuso en el numeral 6.2 del documento soporte publicado.

Frente a esta evidencia, el argumento según el cual la eventual migración del fraude hacia otros canales privaría de idoneidad a las medidas no puede ser acogido por tres razones. Primero, desde el punto de vista jurídico, las competencias de la CRC, conferidas en particular por los numerales 1, 3, 12 y 13 del artículo 22 de la Ley 1341 de 2009, se circunscriben a la regulación de las redes y los servicios de telecomunicaciones y a la administración de los recursos de identificación utilizados en su provisión. Las plataformas y aplicaciones que operan sobre internet exceden el objeto definido en este proyecto regulatorio, de manera que la ausencia de medidas sobre esos entornos no constituye una omisión del análisis, sino el respeto del principio de legalidad que gobierna el objeto de este proyecto. Segundo, desde el punto de vista de la técnica de regulación, y en línea con la primera razón, el objeto de este proyecto de regulación está enfocado, desde su concepción, en el fortalecimiento de los controles sobre los servicios tradicionales de SMS y voz. Tercero, aceptar la tesis de los agentes referenciado a una parálisis regulatoria ya que, bajo esa lógica, ninguna autoridad podría intervenir su propio sector mientras subsistan canales alternativos no regulados, lo que dejaría a los usuarios desprotegidos precisamente en los canales donde hoy se acredita la mayor afectación.

Nótese, además, que, en relación con el objeto de este proyecto, la Comisión no está creando un régimen de habilitación para la prestación de servicios digitales. Por el contrario, con base en las competencias mencionadas que fueron asignadas por la ley a la CRC, esta Comisión está creando una serie de reglas en materia de recursos de identificación que son administrados por la CRC y, naturalmente, esas cargas u obligaciones les aplicarán a aquellos agentes que pretendan ser asignatarios de esos recursos y utilizarlos en el marco del desarrollo de su objeto social.

Ahora bien, la Comisión comparte con los agentes mencionados la necesidad de una aproximación integral e interinstitucional al fenómeno. En esa medida, el proyecto contempla instancias permanentes de coordinación, por ejemplo el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles (CTLFSM) y el Comité Técnico de Seguimiento (CTS), comités que se fusionarán por las razones que se exponen en capítulos posteriores, que permiten la articulación con las autoridades competentes y el intercambio de inteligencia sobre las modalidades emergentes de fraude, así como una dimensión pedagógica transversal orientada a que los usuarios identifiquen intentos de fraude con independencia del canal por el que se materialicen. Adicionalmente, la CRC continuará monitoreando la evolución del fenómeno en el marco de sus competencias y de su agenda regulatoria, de modo que, si la evidencia ex post da cuenta de desplazamientos relevantes del fraude, la Comisión podrá evaluar los ajustes o las gestiones interinstitucionales a que haya lugar.

En consecuencia, no se acepta la solicitud de condicionar la expedición de la resolución a la elaboración previa de un análisis de sustitución entre canales ni la de extender el ámbito de aplicación del proyecto a plataformas OTT, sin perjuicio de lo cual los comentarios asociados a la coordinación interinstitucional serán retomados en el capítulo denominado «Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM» y los asociados a la dimensión pedagógica en el capítulo denominado «Sobre las temáticas enfocadas en la educación de la ciudadanía».

2. Sobre la suficiencia del Análisis de Impacto Normativo, la proporcionalidad de las medidas y la evaluación de las herramientas regulatorias vigentes

ANDESCO, **ANDI**, **CLARO**, **ETB**, **SANDRA RODRÍGUEZ**, **PTC** y el escrito conjunto de **BLIPBLIP**, **NEXVIA** e **INALAMBRIA** formulan, con distintos énfasis, cuestionamientos sobre la suficiencia del análisis que soporta el proyecto: la ausencia de cuantificación de la reducción de fraude esperada y de los costos de implementación (**ANDESCO**, **CLARO**), la necesidad de un enfoque de evaluación ex ante y ex post del riesgo sistémico (**ANDI**, **ASOBANCARIA**), la falta de evaluación ex post de herramientas vigentes como la suspensión provisional de códigos cortos, el monitoreo y el bloqueo de tráfico (**ANDESCO**, **CLARO**), la carencia de información sobre las actuaciones administrativas adelantadas por la Comisión (**CLARO**) y, en general, la supuesta insuficiencia del análisis costo-beneficio para acreditar la necesidad, idoneidad y proporcionalidad de las medidas (**SANDRA RODRÍGUEZ**, **PTC**).

Sobre el particular, la Comisión precisa que el presente proyecto regulatorio ha surtido de manera rigurosa todas las etapas de la metodología de Análisis de Impacto Normativo (AIN) adoptada por la entidad: (i) la realización de un diagnóstico de la problemática, contenido en el denominado documento de formulación del problema, publicado para comentarios del sector, en el que se identificó el árbol del problema, sus causas y consecuencias; (ii) el diseño de las alternativas regulatorias, contenido en el documento de identificación de alternativas regulatorias, igualmente publicado y sometido a participación; y finalmente (iii) la construcción de una propuesta regulatoria derivada del resultado de la evaluación de las alternativas regulatorias, contenido en el documento soporte de la propuesta regulatoria, cuyo capítulo 9 contiene la evaluación comparativa de las alternativas para cada una de las temáticas, incluyendo el análisis de los beneficios esperados, los costos regulatorios y la

proporcionalidad de cada intervención. En dicho análisis, el beneficio económico de las medidas se estimó a partir de una línea base observable —el valor de las reclamaciones por smishing y vishing reportado por la Superintendencia Financiera de Colombia—, proyectada bajo un escenario sin intervención regulatoria, y la efectividad esperada de cada alternativa se aproximó a partir de experiencias internacionales, estudios sectoriales, literatura académica y documentación de autoridades regulatorias y organismos especializados, precisamente porque no existe información estadística nacional que permita medir ex ante el impacto específico de cada medida. Esta aproximación metodológica es la técnicamente disponible y razonable frente a un fenómeno delictivo cuya cifra real de afectación, como lo reconoce el propio documento soporte, es probablemente incluso superior a la reportada, en la medida en que varias entidades financieras no logran desagregar los eventos de smishing y vishing de categorías más amplias.

En cuanto a la evaluación de las herramientas regulatorias vigentes, la Comisión aclara que el proyecto no parte de desconocerlas ni de sustituirlas, sino de fortalecerlas: la facultad de suspensión provisional del tráfico en el marco de actuaciones administrativas de recuperación, el régimen de recuperación de recursos de identificación y las obligaciones de prevención del fraude ya previstas en el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016 se mantienen y se complementan, y buena parte del articulado propuesto tiene por objeto, justamente, corregir las limitaciones que la aplicación práctica de esas herramientas ha evidenciado, tal como se expone en el capítulo del documento soporte relativo a las temáticas objeto de revisión bajo el enfoque de simplificación. La experiencia de la Comisión en las actuaciones administrativas de recuperación de códigos cortos —cuya utilidad reconoce expresamente **CLARO** en otros apartes de su intervención— constituye insumo directo del diagnóstico del proyecto. Los comentarios puntuales sobre estas herramientas serán abordados en el capítulo denominado «Sobre las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación».

De otra parte, en relación con las observaciones sobre la ausencia de análisis económico de la remuneración del ecosistema SMS A2P y la fragmentación del proyecto en fases (**ANDESCO**, **ALDEAMO**, **TIGO**), la Comisión advierte que dicha temática fue clasificada de manera autónoma y será abordada en el capítulo denominado «Remuneración/fases del proyecto/AIN», en el cual se explican las razones del diseño por fases y la articulación de las presentes medidas con las que se expidan en materia de remuneración de la Fase II.

Finalmente, la Comisión coincide con la **ANDI** y **ASOBANCARIA** en la conveniencia de hacer seguimiento a la efectividad de las medidas una vez implementadas. Para ello, el proyecto contempla instancias y obligaciones de reporte que permitirán la evaluación ex post: el CTS y el CTLFSM (comités que se fusionan en la versión final de la resolución que será publicada) tienen dentro de su objeto el seguimiento a la implementación y la revisión periódica de los parámetros técnicos, y los reportes de información previstos en el articulado alimentarán el monitoreo del fenómeno. Los comentarios sobre indicadores específicos de desempeño (tasas de falsos positivos, disponibilidad, tiempos de entrega) serán retomados en los capítulos denominados «Validador centralizado: forma de selección, competencias y funciones», «Monitoreo de llamadas que derivan en la etiqueta de Alerta de llamada

sospechosa» y «Reportes de información». En consecuencia, no se acoge la solicitud de rehacer o complementar el AIN como condición previa a la expedición de la resolución, por cuanto el análisis exigido por la metodología fue efectivamente realizado y publicado para consideración del público; y se acepta parcialmente la solicitud de incorporar mecanismos de evaluación y seguimiento, en los términos ya previstos en el proyecto y con los ajustes que se explican en los capítulos específicos mencionados.

3. Sobre la competencia de la CRC para imponer obligaciones a los Proveedores de Contenidos y Aplicaciones y a los Integradores Tecnológicos

Sobre este punto asociado a la imposición de obligaciones sustantivas a los PCA, tales como registro, KYC, aprobación previa de contenidos, validación anual y sometimiento a un validador centralizado, actores que no son PRST, vale anotar, en primera medida, que los PCA hoy en día ya están sometidos al cumplimiento de las obligaciones derivadas de la asignación y uso de dichos recursos, y que, como lo afirma **PTC**, resulta razonable que asuman responsabilidades directas frente a la mitigación del fraude, sin que las cargas recaigan exclusivamente sobre los PRST.

En segundo lugar, se debe recordar que los numerales 12 y 13 del artículo 22 de la Ley 1341 de 2009 —el primero modificado por el artículo 19 de la Ley 1978 de 2019— atribuyen a la CRC la competencia para regular y administrar los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones y cualquier otro recurso que actualmente o en el futuro identifique redes y usuarios, así como para administrar el uso de los recursos de numeración y demás recursos escasos utilizados en las telecomunicaciones. En ejercicio de esa competencia, materializada en el Régimen de Administración de Recursos de Identificación compilado en el Título VI de la Resolución CRC 5050 de 2016, la Comisión define desde hace años los requisitos de asignación, las obligaciones de los asignatarios, las condiciones de uso y las causales de recuperación de los códigos cortos, obligaciones que son exigibles a todos los asignatarios con independencia de su naturaleza, sea PRST, PCA o IT, pues derivan precisamente de su condición de asignatarios de recursos escasos administrados por el Estado. La asignación de un recurso de identificación no es únicamente una habilitación para su uso. Por el contrario, es también una fuente de deberes cuyo incumplimiento acarrea consecuencias administrativas, como lo ha sostenido de manera reiterada esta Comisión y como lo recuerda **PTC** en su intervención.

Bajo esa arquitectura competencial, las medidas del proyecto no configuran una regulación general de la actividad económica de los PCA ni un régimen de habilitación previa para el ejercicio de su objeto social. Las obligaciones de identificación, verificación (KYC), registro de plantillas y relacionamiento con el validador se predican de los agentes en cuanto solicitantes o asignatarios de los recursos de identificación que administra la CRC, código corto A2P y SENDER ID, y en cuanto usuarios de las redes de telecomunicaciones para cursar tráfico masivo A2P, ámbito en el cual el numeral 1 del artículo 22 de la Ley 1341 de 2009 habilita a la Comisión para expedir la regulación asociada al acceso y uso de las redes. Quien no pretenda originar tráfico A2P mediante los recursos de identificación administrados por la CRC no queda sujeto al régimen propuesto. Adicionalmente, el numeral 3 del artículo 2 de la misma ley impone al Estado el deber de promover el óptimo aprovechamiento de los recursos escasos, finalidad

a la que sirven directamente las condiciones de asignación y uso propuestas, en tanto previenen que dichos recursos sean instrumentalizados para el fraude.

En consecuencia, no resulta viable suprimir o recortar las obligaciones aplicables a los PCA por una supuesta falta de competencia de esta Comisión. Por su parte, la solicitud de **PTC** de incorporar en el artículo 6.13.4.4 una presunción de responsabilidad primaria en cabeza del asignatario del SENDER ID será resuelta en el capítulo denominado «Atribución de responsabilidad».

4. Sobre la distribución de cargas entre los agentes de la cadena de valor y la focalización de las medidas en los agentes formales

En esta materia concurren dos tendencias opuestas. De un lado, **ETB** y **TIGO** advierten que el proyecto concentraría la mayor parte de las obligaciones regulatorias, operativas, tecnológicas y económicas en los PRSTM, pese a que estos no controlan el contenido de las comunicaciones ni el origen de las campañas fraudulentas, y solicitan ampliar las obligaciones hacia los PCA, los IT y demás originadores de tráfico masivo, bajo un principio de control efectivo y corresponsabilidad. De otro lado, **SAEM**, **SANDRA RODRÍGUEZ**, **ALDEAMO** y el escrito conjunto de **BLIPBLIP**, **NEXVIA** e **INALAMBRIA** sostienen que las medidas recaen injustificadamente sobre los agentes formales del ecosistema, quienes ya operan bajo contratos, debida diligencia y trazabilidad, mientras que las verdaderas fuentes del fraude serían factores ajenos al perímetro regulado: SMS spoofing, numeración ilegal o no atribuida, rutas grises internacionales, plataformas clandestinas, SIM farms, simboxes, estaciones base falsas y suplantación potenciada por inteligencia artificial; por lo que concluyen que registrar y controlar al agente formal no reduce el fraude que se origina por fuera de ese perímetro.

La coexistencia de ambas críticas, esto es que el proyecto carga demasiado a los PRST y, simultáneamente, que carga demasiado a los PCA e IT, ilustra, en criterio de la Comisión, que el diseño propuesto distribuye las obligaciones a lo largo de toda la cadena de valor en función del control efectivo que cada eslabón ejerce, que es exactamente el principio que **ETB** reclama. En efecto, los PRSTM asumen las obligaciones asociadas a la infraestructura de red que administran (monitoreo de tráfico, bloqueo de CLI, gestión de listas DNO, etiquetado de llamadas); los asignatarios de código corto A2P, en su condición de agentes con conexión directa a las redes, asumen las obligaciones de verificación de sus clientes (KYC) y de integración con el validador; y los asignatarios de SENDER ID, en su condición de responsables de la producción del contenido, asumen las obligaciones asociadas a las plantillas y al uso legítimo del recurso. El control de la infraestructura de red no implica, por sí solo, la responsabilidad exclusiva sobre el origen de las conductas fraudulentas, razón por la cual las medidas guardan un enfoque de corresponsabilidad entre los distintos eslabones de la cadena de valor, tal como se explicó en el documento soporte.

En cuanto al argumento según el cual el fraude se origina mayoritariamente por fuera del perímetro regulado, la Comisión formula dos precisiones. La primera es que el proyecto sí contiene medidas dirigidas de manera directa contra los vectores señalados por los agentes: el bloqueo de llamadas internacionales entrantes que presenten como CLI numeración del Plan Nacional de Numeración ataca

el spoofing de identificador de llamada; las listas de no originación (DNO) atacan la suplantación de numeración que no debe originar tráfico; el monitoreo de patrones y el esquema de respuesta frente al tráfico P2P con fines A2P atacan la inyección de tráfico mediante SIM farms y simboxes; y las obligaciones de trazabilidad del tráfico A2P atacan las rutas grises y las plataformas no establecidas. La segunda precisión es de orden lógico: la identificación confiable del tráfico legítimo es condición necesaria para aislar y combatir el tráfico ilegítimo. Un ecosistema en el que todo originador formal está identificado, verificado y es trazable permite a los PRST, al validador y a las autoridades concentrar la capacidad de detección y bloqueo sobre el tráfico que carece de esos atributos. Lejos de ser una carga inútil sobre quien ya cumple, la formalización del perímetro es el instrumento que hace operativa la persecución de quien opera por fuera de él. Por lo demás, la premisa de que el cumplimiento actual de los agentes formales es homogéneo no se compadece con la experiencia de esta Comisión en las actuaciones administrativas de recuperación de códigos cortos, en las que se ha constatado el uso de recursos formalmente asignados en campañas potencialmente fraudulentas.

En consecuencia, no se aceptan las solicitudes generales de reorientar el proyecto exclusivamente hacia las fuentes informales del fraude ni las de descargar a los PRST de las obligaciones de red propuestas. Los comentarios específicos de **TIGO** sobre la extensión del régimen de trazabilidad y KYC a la numeración E.164 no geográfica utilizada para SMS serán abordados en el capítulo denominado «Tráfico P2P», en el que se analiza el tratamiento del tráfico cursado por canales distintos al código corto A2P; su solicitud sobre la preservación de la facultad de negociar capacidad y servicios adicionales de red será abordada en el capítulo denominado «Remuneración/fases del proyecto/AIN»; y su solicitud de trasladar al originador la validación del Registro de Números Excluidos en el tráfico de voz será abordada en el capítulo denominado «Etiquetado de llamadas con fines publicitarios».

5. Sobre la protección de datos personales y la seguridad de la información

ANDI y **ASOBANCARIA** solicitan que el proyecto establezca de manera expresa su sujeción a los principios de la Ley 1581 de 2012 (finalidad, necesidad, proporcionalidad, minimización, seguridad y confidencialidad); que se defina el rol del validador centralizado en el tratamiento de datos personales y se exija una evaluación de impacto previa; que se establezcan reglas de gobernanza, límites de conservación y acceso, restricciones al uso ulterior de la información intercambiada, garantías frente a decisiones automatizadas y requisitos mínimos de seguridad de la información; y que se prohíba el almacenamiento de datos sensibles como los códigos OTP.

La Comisión comparte plenamente la relevancia de estas garantías y precisa que el régimen de protección de datos personales contenido en la Ley 1581 de 2012 y sus normas reglamentarias es de aplicación imperativa y directa a todos los agentes que, en el marco de la resolución, efectúen tratamiento de datos personales, incluido el validador centralizado, sin que sea necesario, ni técnicamente procedente, que la regulación sectorial reproduzca o reitere un régimen legal que rige por sí mismo y cuya vigilancia corresponde a la Superintendencia de Industria y Comercio. La resolución expedida delimita las finalidades de los flujos de información que ordena (la prevención, detección y mitigación del fraude), de modo que cualquier tratamiento ulterior incompatible con esas finalidades

quedaría por fuera de la habilitación regulatoria y estaría sujeto al régimen sancionatorio de protección de datos. Hecha esta precisión general, la Comisión advierte que las observaciones puntuales sobre la información que recopila y gestiona el validador, sobre los soportes del proceso de KYC y su conservación, y sobre el contenido y periodicidad de los reportes serán abordadas, respectivamente, en los capítulos denominados «Validador centralizado: forma de selección, competencias y funciones», «KYC» y «Reportes de información». La preocupación específica sobre el tratamiento de los códigos OTP y la improcedencia de su almacenamiento será abordada en el capítulo denominado «Plantillas (Template ID)».».

En consecuencia, se acoge parcialmente el comentario, en el sentido de que las garantías invocadas rigen plenamente el proyecto por ministerio de la Ley 1581 de 2012, y las precisiones puntuales que resulten procedentes sobre flujos de información específicos se resolverán en los capítulos indicados.

6. Sobre la coordinación interinstitucional y el intercambio de información con el sector financiero

ASOBANCARIA propone incorporar un mandato expreso de articulación interinstitucional entre la CRC, la URF, la Superintendencia Financiera de Colombia y la Superintendencia de Industria y Comercio, así como un esquema de intercambio de información en tiempo real entre operadores de telecomunicaciones y entidades financieras, incluyendo la posibilidad de compartir, sin cobro o a costo mínimo, la información de los procesos de debida diligencia y validación reforzada de los operadores móviles. **ETB**, **ANDESCO** y la **ANDI** formulan solicitudes análogas de coordinación con el MinTIC, la SIC, la SFC y el COLCERT.

La Comisión comparte el diagnóstico según el cual la lucha contra el fraude exige articulación entre autoridades y sectores, y precisamente por ello el proyecto institucionaliza una instancia permanentes de coordinación: el CTLFSM, para las temáticas de voz y SMS, y, de conformidad con lo que se expondrá en capítulos posteriores, se unificarán las funciones que se le habían concedido al CTS para el seguimiento del ecosistema A2P, instancias a las cuales pueden ser invitadas las autoridades y los actores cuya participación resulte pertinente, incluyendo a las entidades del sector financiero que, como lo señala **ASOBANCARIA**, con frecuencia identifican tempranamente las campañas de fraude. Ahora bien, la Comisión no puede acoger la solicitud de incorporar en la resolución un mandato de actuación dirigido a la URF, a la SFC o a la SIC, por cuanto la CRC carece de competencia para imponer obligaciones a dichas autoridades públicas en el sentido propuesto; sin embargo, la articulación con dichas entidades sí se canaliza a través de los instrumentos de coordinación administrativa disponibles y de las instancias creadas por el proyecto. En cuanto al esquema de intercambio de información entre operadores y entidades financieras, la Comisión advierte que su diseño de detalle (alcance, condiciones, seguridad y eventual remuneración) involucra relaciones entre agentes de sectores con regímenes de supervisión distintos, y será abordado en el capítulo denominado «Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM».

En consecuencia, se acepta parcialmente el comentario, en cuanto la finalidad de articulación que persiguen los agentes ya se encuentra recogida en las instancias de coordinación del proyecto, y no se acepta la incorporación de mandatos dirigidos a otras autoridades, por falta de competencia de esta Comisión.

7. Sobre la continuidad de las comunicaciones críticas (OTP, alertas transaccionales y de seguridad) y los plazos de implementación

COLOMBIA FINTECH solicita una cláusula explícita de continuidad operativa que garantice la prestación ininterrumpida de la mensajería crítica del sector financiero durante la transición, con prórroga automática para las entidades que acrediten procesos de migración en curso. **ASOBANCARIA** advierte que los artículos 6, 7, 12 y 19 del proyecto imponen cargas cuya aplicación simultánea, sin fases progresivas ni pruebas piloto, podría comprometer la continuidad del servicio, y que el plazo de seis meses de transición resulta insuficiente. **NEXVIA** y el escrito conjunto sostienen que las facultades de suspensión y desconexión previstas en el proyecto pueden interrumpir comunicaciones esenciales de usuarios ajenos a la conducta investigada (OTP, alertas de seguridad, notificaciones de salud y de autoridades), con especial afectación de la población sin acceso a internet móvil, e invocan los artículos 13, 78 y 365 de la Constitución Política, la Ley 1341 de 2009, la Ley 2300 de 2023 y la Ley 1581 de 2012.

La Comisión reconoce la centralidad de este asunto ya que la protección de las comunicaciones de autenticación y seguridad es, precisamente, una de las finalidades del proyecto, en tanto dichas comunicaciones constituyen la primera línea de defensa del usuario contra el fraude. Por esa razón, el diseño propuesto diferencia las modalidades de contenido del SENDER ID, entre ellas la de autenticación y seguridad, y les otorga un tratamiento acorde con su naturaleza. Ahora bien, dado que las preocupaciones expresadas se proyectan sobre disposiciones específicas del articulado, su análisis de fondo, incluyendo las salvaguardas de continuidad, los plazos de la transición, las garantías de debido proceso frente a medidas de suspensión y el tratamiento especial de los OTP, será desarrollado en el capítulo denominado «Tratamiento de mensajes OTP, autenticación, seguridad y comunicaciones críticas» al cual se remite la respuesta puntual de estos comentarios. Basta señalar en este punto que la premisa según la cual el proyecto habilita interrupciones «automáticas e indiscriminadas» de comunicaciones esenciales no corresponde al diseño propuesto, en el que las medidas restrictivas están asociadas a supuestos definidos, a la actuación de la autoridad y a la finalidad de excluir del ecosistema el tráfico fraudulento, y en el que la continuidad de las comunicaciones legítimas de terceros es objeto de reglas específicas cuyo alcance se examina en los capítulos mencionados.

8. Sobre el impacto en las micro, pequeñas y medianas empresas y las barreras de acceso al canal SMS

INALAMBRIA, **ALDEAMO**, **BLIP BLIP** y el escrito conjunto advierten que el nuevo régimen (registro, asignación de recursos de identificación, plantillas, financiación del validador) podría resultar excesivamente oneroso para pequeños y medianos remitentes, generando barreras de entrada

contrarias a las políticas de inclusión digital y de fortalecimiento de las MIPYMES, y solicitan un régimen simplificado que permita compartir recursos de identificación de manera controlada a través de los integradores y procedimientos abreviados con menores cargas documentales. **INALAMBRIA** solicita adicionalmente que el proyecto diferencie los controles según el nivel de riesgo de los mensajes, distinguiendo, por ejemplo, los mensajes con URL de las notificaciones transaccionales, las alertas de autoridades o los OTP, y que se incorpore un análisis de proporcionalidad que pondere los derechos de los usuarios de otros sectores (salud, servicios públicos, seguridad social) que dependen del canal.

La Comisión precisa, en primer lugar, que la premisa según la cual toda empresa originadora de mensajes debe obtener conexión directa e infraestructura propia no corresponde al diseño del proyecto. Por el contrario, los PCA sin conexión directa acceden al canal a través de los asignatarios de código corto A2P, quienes proveen la infraestructura de conexión, de modo que la agregación subsiste como vía de acceso para los remitentes de menor escala, y el SENDER ID cumple la función de identificar al responsable del contenido sin exigirle el despliegue de infraestructura. En segundo lugar, el proyecto sí diferencia los contenidos según su naturaleza mediante las modalidades del SENDER ID (autenticación y seguridad; transaccionales e informativos; comerciales o publicitarios; y regulatorios o de interés público), diferenciación que recoge, en lo sustancial, la segmentación por niveles de riesgo que propone **INALAMBRIA**. En cuanto a la ponderación de los derechos de usuarios de otros sectores, la Comisión reitera que la finalidad del proyecto es precisamente preservar la confiabilidad del canal SMS como medio universal de comunicación (incluyendo las citas médicas, las alertas de autoridades y las notificaciones de servicios) frente a su instrumentalización fraudulenta, y que el test de proporcionalidad desarrollado en el AIN ponderó los beneficios esperados frente a los costos regulatorios de cada alternativa. Los ajustes puntuales solicitados en materia de requisitos, cargas documentales y condiciones de asignación serán analizados en los capítulos denominados «Sender ID» y «Código Corto A2P», a los cuales se remite la respuesta específica.

En consecuencia, no se acepta la creación de un régimen simplificado paralelo en los términos solicitados, sin perjuicio de las precisiones que sobre requisitos y cargas se adopten en los capítulos indicados, y se precisa que la diferenciación por naturaleza del contenido ya se encuentra incorporada en el diseño de las modalidades del SENDER ID.

9. Sobre las recomendaciones técnicas y operativas complementarias

GMS recomienda complementar el proyecto con medidas técnicas en las capas de red y señalización (firewalls de SMS con clasificación mediante inteligencia artificial, firewalls de señalización SS7 y Diameter, firewalls de voz y de datos), en la capa de aplicación (gateway centralizado de mensajería A2P con infraestructura SMSC en las instalaciones del regulador, APIs de red) y en la capa de inteligencia (canal ciudadano de reporte integrado con los firewalls). **SCAMZERO** propone complementar los controles de red con mecanismos de protección para el usuario final y establecer un estándar homogéneo de monitoreo mediante la unificación de variables y criterios de detección. **GERMÁN CRUZ** propone una consulta pública que permita identificar las empresas asociadas a cada código corto,

controles preventivos de plantillas mediante inteligencia artificial, el almacenamiento temporal de los mensajes masivos enviados y un mecanismo sencillo de recepción de quejas asociado al código corto.

La Comisión valora positivamente estas contribuciones y advierte que varias de ellas coinciden con el diseño del proyecto o encuentran cauce natural en sus instancias. En cuanto a las medidas propuestas por **GMS**, se debe resaltar en primera instancia, que el proyecto se fundamenta en el principio de neutralidad tecnológica, conforme al cual se garantiza la libre adopción de tecnologías sin perjuicio del cumplimiento de las obligaciones y resultados establecidos en la regulación; en consecuencia, el proyecto establece objetivos dirigidos al monitoreo, detección, bloqueo y trazabilidad del tráfico en los servicios de voz y mensajería, pero no determina la arquitectura interna de las redes de los PRST, ni prescribe la implementación de equipos, plataformas, protocolos, proveedores o soluciones tecnológicas específicas. De otro lado, es preciso aclarar que a la CRC en su condición de autoridad de regulación, no cuenta con la función de operar infraestructura de telecomunicaciones o cursar directamente tráfico de los PRST, y por tanto corresponde a estos últimos, de acuerdo con las características y evolución de sus redes, el tráfico gestionado, los riesgos identificados y sus políticas de seguridad, seleccionar, implementar y configurar los mecanismos técnicos necesarios para cumplir las obligaciones regulatorias y gestionar los riesgos de fraude.

En este sentido, las recomendaciones formuladas por **GMS** relacionadas a la incorporación de firewalls específicos, soluciones basadas en inteligencia artificial, gateways centralizados, infraestructura SMSC o componentes determinados de señalización, no se acogen en la medida en que ello implicaría que esta Comisión ordenara de forma específica la utilización una determinada solución tecnológica para la implementación de las medidas de intervención planteadas, lo que de plano no solo contravendría el principio de neutralidad tecnológica sino que, además, podría incluso considerarse una injerencia desmedida por parte del regulador en la administración de las redes, sistemas y, a la postre, el negocio de los operadores, desdibujándose así la finalidad primigenia de la función regulatoria en cabeza de la CRC. Sin perjuicio de lo anterior, es claro que los PRST puedan adoptar voluntariamente dichas soluciones como parte de sus estrategias internas de seguridad y prevención del fraude. Las propuestas relativas al intercambio de inteligencia sobre amenazas y a los canales de reporte encuentran desarrollo en el CTLFSM y serán retomadas en el capítulo correspondiente. La propuesta de **SCAMZERO** sobre unificación de variables y criterios de detección coincide con las funciones de coordinación del CTLFSM y con el esquema de monitoreo propuesto, y será abordada en los capítulos denominados «Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM» y «Monitoreo de llamadas que derivan en la etiqueta de Alerta de llamada sospechosa».

Frente a las propuestas de **GERMÁN CRUZ**, la Comisión debe precisar lo siguiente: (i) la información sobre los recursos de identificación asignados y su estado es pública y puede ser consultada por cualquier ciudadano a través de los sistemas de información de la CRC, de manera que la finalidad de verificación de legitimidad del remitente que persigue el comentario se encuentra satisfecha en la regulación vigente, y será reforzada con las medidas de identificación del originador (SENDER ID) propuestas en el proyecto; (ii) el control preventivo del contenido mediante plantillas registradas y validadas coincide con el mecanismo de plantillas del proyecto, cuyos detalles se abordan en el capítulo

denominado «Plantillas (Template ID)»; (iii) la propuesta de almacenamiento temporal del contenido de los mensajes masivos no se acoge, por cuanto el contenido de las comunicaciones se encuentra amparado por la garantía de inviolabilidad prevista en el artículo 15 de la Constitución Política, y una obligación general de retención de contenidos excedería la finalidad del proyecto y el juicio de proporcionalidad; la trazabilidad que el proyecto ordena recae sobre los metadatos y los recursos de identificación empleados, no sobre el contenido de las comunicaciones de los usuarios; y (iv) los usuarios ya cuentan con los mecanismos de PQR ante su proveedor y ante las autoridades de vigilancia, y la dimensión pedagógica del proyecto contempla la divulgación de los canales de reporte, aspecto que será retomado en el capítulo denominado «Sobre las temáticas enfocadas en la educación de la ciudadanía».

10. Sobre la hoja de ruta de autorregulación, la flexibilidad evolutiva del marco y las experiencias internacionales

TRANSUNION propone que la CRC promueva una hoja de ruta de autorregulación sectorial orientada a recuperar la confianza en los canales de voz y mensajería; solicita que el diseño regulatorio preserve flexibilidad para una convergencia futura entre los mecanismos de validación de identidad empresarial, KYC, SENDER ID, gobierno de plantillas, identidad de llamadas e inteligencia antifraude, evitando silos rígidos entre voz y mensajería; y aporta referencias internacionales (Brasil, Estados Unidos, Canadá, India y las iniciativas de la GSMA) de las cuales deriva lecciones sobre validación de identidad empresarial, gobernanza, soluciones nativas de red y sostenibilidad económica. **SINCH**, por su parte, valora el enfoque sistémico de corresponsabilidad del proyecto, aunque advierte sobre la complejidad de supervisar a múltiples actores y el riesgo de dilución de responsabilidades si las reglas no son suficientemente claras.

La Comisión acoge favorablemente el espíritu de estos comentarios, que en lo sustancial convergen con el diseño del proyecto. Las experiencias internacionales fueron insumo expreso del análisis de alternativas desarrollado en el documento soporte, en el que se examinaron los modelos de autenticación de llamadas, registro de remitentes y gobernanza adoptados en otras jurisdicciones para aproximar la efectividad esperada de las medidas. El marco propuesto es tecnológicamente neutro y no impone una plataforma común ni una tecnología única, de modo que no obstruye la evolución futura hacia arquitecturas interoperables y modulares como las que describe **TRANSUNION**; y las instancias de coordinación creadas (CTLFSM y CTS que se fusionan) constituyen precisamente el espacio institucional para la revisión periódica de parámetros, la adaptación de estándares y el desarrollo de iniciativas colaborativas del ecosistema, funciones que absorben la finalidad de la hoja de ruta de autorregulación propuesta, bajo la supervisión del regulador. En cuanto a la observación de **SINCH** sobre la claridad en la asignación de responsabilidades entre eslabones, la Comisión remite al capítulo denominado «Atribución de responsabilidad», en el que se examinan las reglas de imputación propuestas. En consecuencia, se acepta parcialmente el comentario, en los términos expuestos, sin que resulte necesario introducir modificaciones adicionales al articulado por razón de esta temática.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

11. Sobre la solicitud de reformulación integral del proyecto y las peticiones del escrito conjunto de BLIPBLIP, NEXVIA e INALAMBRIA

El escrito conjunto de **BLIPBLIP**, **NEXVIA** e **INALAMBRIA**, cuyos planteamientos coinciden con la intervención individual de **BLIP BLIP**, solicita a la Comisión abstenerse de expedir el proyecto en su forma actual y reformularlo integralmente, por considerar que este adolece de un error de diagnóstico (combatir con burocracia un problema tecnológico y de precios), que desdibuja la figura del Integrador Tecnológico, que configura una asimetría regulatoria a favor de los PRSTM en un mercado concentrado, que genera efectos colaterales sistémicos (migración del fraude al P2P y a canales OTT, desconexión de las comunicaciones transaccionales internacionales, exclusión de las MIPYMES y afectación de comunicaciones críticas) y que contiene incongruencias normativas y contradicciones internas. Como modelo alternativo, proponen la reserva estatal de la coerción, la continuidad del servicio como principio, la identificación sobre recursos existentes y un esquema de inteligencia compartida e inclusiva; y concretan nueve solicitudes.

Frente a la petición central, la Comisión no accede a la reformulación integral del proyecto. El diseño propuesto es el resultado de un proceso de AIN que surtió todas sus etapas con participación del sector (formulación del problema, identificación y evaluación de alternativas y propuesta regulatoria), y las objeciones estructurales del escrito reproducen, en lo esencial, las tendencias ya analizadas en los ejes precedentes de esta respuesta: el eje 1 en cuanto a la migración del fraude hacia canales OTT y P2P; el eje 2 en cuanto a la suficiencia del AIN y la cuantificación de impactos; el eje 4 en cuanto a la focalización en los agentes formales y la distribución de cargas; el eje 7 en cuanto a la continuidad de las comunicaciones críticas; y el eje 8 en cuanto al impacto sobre las MIPYMES, a cuyas consideraciones se remite la CRC. La Comisión destaca, además, que los agentes comparten expresamente la finalidad del proyecto y reconocen la realidad y gravedad del problema; la discrepancia versa sobre los medios, y es precisamente en los capítulos temáticos específicos de este documento donde cada medida cuestionada se examina de fondo, con indicación expresa de los ajustes que la Comisión acoge como resultado del proceso participativo. Este proceder (responder motivadamente cada comentario y ajustar el articulado donde la evidencia y los argumentos lo ameritan) materializa el diálogo técnico que los firmantes reclaman, sin que sea necesario retrotraer la actuación administrativa a sus etapas iniciales.

En cuanto a las nueve solicitudes concretas, la Comisión responde así: la solicitud PRIMERA (reformulación integral) no se acepta, por las razones expuestas en el párrafo anterior. La solicitud SEGUNDA (reformulación o eliminación del régimen del validador centralizado) será abordada en el capítulo denominado «Validador centralizado: forma de selección, competencias y funciones». La solicitud TERCERA (eliminación de la unicidad del código corto A2P y de la consolidación forzosa) será abordada en los capítulos denominados «Código Corto A2P» y «Régimen de transición». La solicitud CUARTA (eliminación de la suspensión y desconexión unilateral por el PRST y reserva de toda medida restrictiva a la CRC) será abordada en los capítulos denominados «Consecuencia para reincidentes» y «Oposición a la interconexión». La solicitud QUINTA (sustitución de la autorización previa de plantillas por un esquema de etiquetado y eliminación de la renovación mensual) será abordada en el capítulo denominado «Plantillas (Template ID)». La solicitud SEXTA (preservación de la figura del Integrador

Tecnológico, tráfico en nombre de terceros y supresión de la exigencia de sucursal) será abordada en los capítulos denominados «Código Corto A2P», «Sender ID» y «Obligación de constituir una sucursal en Colombia y cargas para sociedades internacionales». La solicitud SÉPTIMA (incorporación de los PCA e IT al comité técnico con voz y voto) será abordada en los capítulos denominados «Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM» y «Comité Técnico de Seguimiento y coordinación operativa». La solicitud OCTAVA (publicación de un análisis de impacto normativo previo a la expedición, con respuesta motivada a los comentarios) no se acepta en cuanto supone la inexistencia del AIN, pues este fue efectivamente elaborado y publicado en las etapas del proyecto, incluyendo el análisis costo-beneficio contenido en el capítulo 9 del documento soporte y se encuentra satisfecha en cuanto a la respuesta motivada, que se materializa en el presente documento, publicado junto con el texto definitivo de la resolución. Finalmente, frente a la solicitud NOVENA (convocatoria de una mesa técnica con participación de PCA e IT), la Comisión valora la disposición manifestada por los firmantes y precisa que los espacios de participación del proyecto se han garantizado en todas sus etapas; adicionalmente, las instancias permanentes creadas por la resolución constituyen el escenario institucional idóneo para el diálogo técnico continuo sobre la implementación de las medidas, sin perjuicio de las mesas de trabajo que la Comisión estime pertinente convocar durante el período de transición, en ejercicio de sus funciones.

Por último, en relación con las incongruencias normativas y contradicciones internas alegadas (unicidad frente a régimen de reincidencia, granularidad del SENDER ID frente al ejemplo del documento soporte, plazos de transición, coherencia con la estrategia de simplificación y con la doctrina de corrección de asimetrías), la Comisión advierte que cada una de ellas se predica de disposiciones específicas del articulado y será resuelta, con el análisis de consistencia correspondiente, en los capítulos denominados «Código Corto A2P», «Sender ID», «Consecuencia para reincidentes», «Régimen de transición» y «Sobre las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación».

12. Sobre los comentarios individuales restantes

Además de las tendencias ya respondidas en los ejes 1, 2 y 4 (adaptabilidad de los grupos delictivos, necesidad de estrategia conjunta y de controles dinámicos, y riesgo de concentración del mercado), **ALDEAMO** cuestiona la falta de concertación previa de las medidas y solicita una revisión de la estructura de precios de los SMS. Frente a lo primero, la Comisión reitera que el proyecto ha surtido todas las instancias de participación previstas en la metodología de AIN y en el régimen de publicidad de proyectos regulatorios, incluyendo la publicación para comentarios del documento de formulación del problema, del documento de alternativas y del proyecto de resolución con su documento soporte, proceso del cual la presente respuesta hace parte; en consecuencia, no se acepta la premisa de ausencia de concertación. Frente a lo segundo, la revisión de las condiciones económicas del ecosistema SMS A2P será abordada en el capítulo denominado «Remuneración/fases del proyecto/AIN». El riesgo de migración del fraude hacia el tráfico P2P será abordado en el capítulo denominado «Tráfico P2P».

Frente a la intervención individual de **NEXVIA** es menester indicar que los planteamientos sobre la afectación de usuarios finales ajenos a las conductas investigadas, la continuidad del servicio como garantía constitucional, la situación de la población sin acceso a internet móvil y el derecho a la información del consumidor fueron respondidos en el eje 7, y su desarrollo de fondo se remite a los capítulos allí indicados. La Comisión precisa, en todo caso, que comparte la premisa constitucional invocada (la protección del usuario y la continuidad de los servicios públicos como mandatos de los artículos 78 y 365 de la Constitución) y que es justamente esa premisa la que fundamenta la intervención regulatoria: el statu quo, en el que las reclamaciones por smishing y vishing se triplicaron entre 2022 y 2024, es el escenario que compromete los derechos de los usuarios que la regulación busca proteger.

De otra parte, la caracterización que **SAEM** efectúa de su posición en la cadena de valor y de las obligaciones que le resultarían aplicables es correcta en lo sustancial y da cuenta de un interés directo y cualificado en el proyecto. Sus planteamientos sobre el origen del fraude por fuera del perímetro regulado y sobre los principios constitucionales comprometidos (libertad económica, confianza legítima, proporcionalidad y libre competencia) fueron respondidos en los ejes 2 y 4 de esta sección. En cuanto a su observación sobre el examen del diseño del validador en sede de abogacía de la competencia, la Comisión informa que el proyecto fue remitido a la Superintendencia de Industria y Comercio para el trámite previsto en el artículo 9 de la Ley 1340 de 2009, cuyo resultado se refleja en la parte considerativa de la resolución. Sus solicitudes específicas sobre el validador, el KYC, la consolidación de códigos y las medidas de voz serán abordadas en los capítulos temáticos correspondientes, donde se responden sus comentarios particulares.

Los planteamientos de **SANDRA RODRÍGUEZ** sobre la focalización de las medidas en los agentes formales y sobre la aplicación de los principios de necesidad, proporcionalidad y análisis de impacto económico fueron respondidos en los ejes 2 y 4. En cuanto a la referencia al impacto de la Ley 2300 de 2023 sobre la actividad de cobranza y el modelo económico de los integradores, la Comisión advierte que las restricciones de contacto establecidas por dicha ley son de rango legal y su conveniencia escapa al ámbito de este proyecto regulatorio; la solicitud de privilegiar mecanismos de identificación de numeraciones ilegales, intercambio de información y trazabilidad sobre plataformas no autorizadas coincide con medidas que el proyecto efectivamente contempla, según se explicó en el eje 4.

La solicitud de **COLOMBIA FINTECH** correspondiente a una cláusula de continuidad operativa para la mensajería crítica del sector financiero durante la transición, con prórroga para entidades que acrediten migración en curso, será abordada en el capítulo denominado «Régimen de transición», conforme se indicó en el eje 7.

La posición de **PTC** sobre las obligaciones de los PCA e IT en su condición de asignatarios fue acogida en el eje 3. Su observación sobre la creación del validador centralizado y su propuesta de que las funciones de este y de las instancias de coordinación sean asumidas directamente por la CRC serán abordadas en el capítulo denominado «Validador centralizado: forma de selección, competencias y funciones». Su solicitud de incorporar una presunción de responsabilidad primaria en cabeza del

asignatario del SENDER ID en el artículo 6.13.4.4 será abordada en el capítulo denominado «Atribución de responsabilidad».

Finalmente, la solicitud de **BLIP BLIP** de no expedir el proyecto y reformularlo integralmente coincide con la petición central del escrito conjunto y se responde en los términos del eje 11.

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

2.1 Sender ID

ANDI

Sostiene que el artículo 1 del Proyecto de Resolución define el SENDER ID como un recurso de identificación administrado por la CRC, destinado a identificar al responsable del contenido enviado por SMS y USSD. A su vez, el Capítulo 12 (artículos 6.12.1.1 y siguientes) regula su asignación y condiciona la posibilidad de cursar tráfico A2P a la tenencia de un SENDER ID.

A juicio de la **ANDI**, resulta preocupante que esta figura se utilice como mecanismo para imponer un régimen de habilitación previa a los generadores de contenido, condicionando su posibilidad de comunicarse con los usuarios. Si bien reconoce que la CRC administra legítimamente determinados recursos de identificación, considera que dicha competencia debe ejercerse dentro de los límites propios de su gestión técnica, eficiente y segura, sin convertirlos en instrumentos de autorización previa para el desarrollo de actividades económicas o el envío de comunicaciones legítimas.

La **ANDI** reconoce la importancia del SENDER ID como herramienta para identificar con mayor claridad al originador de las comunicaciones A2P, reducir la suplantación y fortalecer la confianza del usuario. No obstante advierte que su configuración como requisito administrativo previo, con asignación única por entidad, exigencias de validación, causales de recuperación y dependencia del validador centralizado, podría convertirse en una barrera de acceso y permanencia en el mercado.

Añade que un régimen de asignación previa, sujeto a tiempos administrativos y causales de recuperación, resulta incompatible con la velocidad operativa de los servicios digitales y con la incorporación ágil de nuevos remitentes legítimos. En su opinión, ello podría generar barreras de entrada para startups, comercios digitales y desarrolladores, así como demoras para proveedores de mayor escala, con el riesgo de que determinados servicios de seguridad no puedan operar en Colombia.

ASOBANCARIA

Señala que la obligatoriedad de contar con un SENDER ID único, realizar una validación previa, surtir un proceso de KYC y obtener la aprobación de plantillas, introduce cargas operativas y tiempos adicionales que podrían afectar la agilidad en el envío de comunicaciones críticas, especialmente aquellas relacionadas con autenticación, seguridad o alertas de fraude. Por lo anterior, surgiere incorporar un régimen diferencial o expedito para los asignatarios de SENDER ID que requieran enviar mensajes de naturaleza crítica, garantizando: i) La aprobación automática o mediante un procedimiento fast-track de las plantillas asociadas a prevención del fraude, autenticación de clientes, envío de códigos OTP (One Time Password), alertas de seguridad y notificaciones transaccionales; y ii) La definición expresa de los términos máximos y niveles de servicio aplicables a los procesos de validación y aprobación del validador centralizado, así como de los mecanismos de contingencia que deberán activarse ante indisponibilidad, fallas operativas o demoras en la respuesta.

Respecto de la clasificación prevista en el artículo 6.12.1.3.3 (MENSAJES COMERCIALES O PUBLICITARIOS), **ASOBANCARIA** sostiene que la norma obliga a los operadores a implementar monitoreo en tiempo real mediante algoritmos de analítica de datos, por lo cual se sugiere exigir que las comunicaciones de cobranza, recuperación de cartera y comerciales estén debidamente parametrizadas e inscritas ante los operadores móviles con el fin de evitar que sean clasificadas erróneamente como «sospechosas». Asimismo sugiere evaluar un esquema de registro o identificación de las numeraciones utilizadas por las entidades vigiladas en procesos de cobranza, atención al cliente, autenticación y gestión operativa. Este mecanismo debería permitir acreditar la finalidad legítima de las comunicaciones y garantizar que las numeraciones registradas no sean etiquetadas automáticamente como sospechosas, sino que reciban un tratamiento diferencial basado en el análisis de riesgo. Finalmente, recomienda considerar la implementación de un sandbox regulatorio que permita validar, en entornos controlados, las medidas propuestas (en especial las relacionadas con identificación de remitentes, el monitoreo de tráfico y el etiquetado de comunicaciones) antes de su despliegue a nivel nacional.

ANDESCO

Afirma que el proyecto establece que a cada persona natural o jurídica se le asignará un único Sender ID (Art. 6.12.1.2, Parágrafo 2) y que la solicitud deberá ser presentada por el asignatario del código corto A2P en nombre del solicitante (Art. 6.12.2.1), y no directamente por el creador del contenido. A su juicio, ambas restricciones generan problemas operativos.

Respecto del Sender ID único por empresa señala que: (i) Las grandes corporaciones (bancos, aseguradoras, retailers con múltiples marcas) requieren Sender ID diferenciados por categoría de mensaje, de manera que el usuario pueda reconocer y priorizar el tipo de comunicación. Un banco con un único Sender ID mezclaría OTP de autenticación, avisos de transacciones, comunicaciones comerciales y alertas de seguridad, dificultando la distinción entre mensajes críticos y no críticos. (ii) Los grupos empresariales con varias personas jurídicas deberán registrar Sender ID separados por NIT, multiplicando los trámites administrativos sin mejorar la trazabilidad del fraude. (iii) Aunque el parágrafo del artículo 6.12.1.1 prohíbe identificadores que 'imiten nombres de entidades públicas, financieras u

operadores de telecomunicaciones', no establece una verificación cruzada con el registro de marcas de la SIC ni con el RUES, lo que permitiría solicitar Sender ID similares a marcas reconocidas (homoglifos, variaciones ortográficas).

Añade que un único Sender ID por empresa genera mayores costos de gestión documental para corporaciones con múltiples marcas, afecta la experiencia del usuario al impedirle identificar visualmente el tipo de mensaje e incentiva la fragmentación societaria para eludir la restricción.

En cuanto a la asignación, considera necesario modificar la obligación impuesta al PCA de solicitar ante la CRC la asignación del SENDER ID a nombre del creador del contenido. En su criterio, esta obligación debe recaer directamente sobre el creador o responsable del contenido y no sobre el Proveedor de Contenidos, dado que el SENDER ID está asociado a la identidad, actividad y responsabilidad del remitente final, quien conoce, controla y responde por el contenido de los mensajes enviados.

Finalmente, propone que la CRC administre directamente el registro de Sender ID mediante el SIGRI, con validación cruzada automática frente al registro de marcas de la SIC y el RUES. Considera que este modelo sería técnicamente más sencillo y menos costoso que el validador centralizado, además de eliminar el riesgo de un monopolio privado.

BLIPBLIP

Cuestiona la limitación de asignar un único código corto por PCA, al considerar que no está suficientemente justificada y desconoce el uso eficiente de los recursos de identificación para diferenciar tipos de contenido (gratuito, con cobro, entre otros).

- Garantía de Operación. Señala que un único código corto constituiría un punto único de falla, pues una desconexión asociada al código o al SenderID podría afectar tanto el contenido malicioso como los demás contenidos y dejar al PCA fuera de operación.

-Servicios SMS de doble vía (MO/MT). Indica que un único código corto impediría identificar clientes, industrias o unidades de negocio independientes y direccionar adecuadamente el tráfico correspondiente.

-Restricción al crecimiento y posible bloqueo. Advierte que exigir un SENDER ID por cada empresa o vertical generaría un volumen de solicitudes difícil de atender por los PRST y el centralizador, además de incrementar los procesos de configuración técnica.

-Relación PCA e IT. señala que impedir que un IT tenga su propio SENDER ID genera un desbalance, afecta el concepto conjunto de PCA e IT y podría permitir que el PCA prescinda del IT y traslade el negocio directamente al PRST. Añade que eliminar la figura del intermediador desconoce sus aportes a la masificación de los servicios y a la simplificación de las relaciones comerciales y técnicas entre los PCA y los PRST.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

-Uso del SenderID. Considera que este es un recurso adecuado que, pese a las restricciones de la norma técnica de conectividad SMPP, puede utilizarse como herramienta de confianza entre las marcas y sus usuarios. Señala que no debe condicionarse a un único código corto y que la identificación numérica, el SENDER ID y el código corto pueden coexistir.

-Justificación de la necesidad de código corto. Cuestiona la exigencia de justificar detalladamente su necesidad y propósito, al considerar que este recurso es esencial para la operación de los PCA e IT.

-Tiempos de implementación. Solicita precisar qué se entiende por implementación de un código corto, dado que los PRST podrían tardar más de seis meses en activarlo debido a la complejidad de la integración. Asimismo, pregunta si se establecerán obligaciones para hacer más eficientes estos tiempos.

- Asignación de SenderID. Solicita que se permita asignar múltiples identificadores y no uno único.

- Composición accionaria. Cuestiona la exigencia de publicar la composición accionaria de la sociedad como requisito para solicitar un código corto.

COLOMBIA FINTECH

Señala que la distinción entre mensajes transaccionales e informativos (artículo 6.12.1.3.2) y mensajes comerciales (artículo 6.12.1.3.3) no es clara en el contexto del crédito de consumo. Mensajes como «tiene cupo disponible», avisos de activación de productos o comunicaciones sobre beneficios de un contrato vigente podrían ubicarse en cualquiera de las dos categorías, con consecuencias distintas respecto del consentimiento requerido y el cumplimiento del RNE. Un ejemplo es el mensaje: «Tu pago fue exitoso. Aprovecha 20 % en tu próxima compra».

Considera que la clasificación entre mensajes de autenticación, transaccionales, comerciales y regulatorios determina reglas estrictas de consentimiento —opt-in y opt-out— y limita la administración y envío de mensajes comerciales. Por ello, solicita que la CRC publique, antes de que el validador comience a aprobar plantillas, una guía interpretativa con ejemplos concretos del sector financiero que permita diferenciar claramente los mensajes transaccionales de los comerciales.

Añade que, en la operación real, una proporción significativa de los mensajes A2P financieros combina elementos de varias modalidades. Por ejemplo, un recordatorio de pago puede incluir una invitación a refinanciar, o una confirmación de transacción puede mencionar un programa de beneficios. Aunque el parágrafo del artículo permite que un mismo SENDER ID curse plantillas de distintas modalidades, no regula los mensajes individuales de contenido híbrido.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Advierte que esta ambigüedad obliga a fragmentar comunicaciones legítimas, afectando la experiencia del usuario, o a clasificar como comercial todo mensaje con algún componente promocional, lo que podría impedir flujos transaccionales necesarios por falta de autorización previa.

En consecuencia, solicita adicionar al artículo 6.12.1.3 lineamientos para clasificar mensajes híbridos, estableciendo que la modalidad aplicable corresponda al componente principal, entendido como aquel que motiva principalmente el envío y ocupa la mayor parte del contenido. Asimismo, propone que el validador publique criterios objetivos para esta determinación y que el asignatario del SENDER ID justifique la clasificación al someter la plantilla a aprobación.

Por otra parte, señala que la norma no precisa si las comunicaciones relacionadas con acuerdos de pago, reestructuraciones o descuentos por pronto pago constituyen contenido transaccional o comercial. Esta distinción resulta crítica, pues su clasificación como comerciales exigiría autorización previa y expresa del cliente, lo que podría hacer inviable la gestión de cobranza de obligaciones derivadas de relaciones contractuales vigentes.

Por ello, solicita precisar en el artículo 6.12.1.3.2 que todo el ciclo de gestión de cartera vencida, incluidas las comunicaciones para negociar acuerdos sobre obligaciones vigentes, constituye contenido transaccional. Indica que la clasificación de estas plantillas como transaccionales por proveedores tecnológicos internacionales, como Twilio, respalda esta solicitud.

Respecto de la inscripción pública de SENDER ID y numeración, señala que los artículos 6.14.2.2 y 6.14.3.1 obligan a publicar en un portal de la CRC los SENDER ID del sector financiero y la numeración E.164 de voz. Aunque reconoce la finalidad de permitir al consumidor verificar la legitimidad del remitente, advierte que un catálogo abierto de identificadores legítimos podría facilitar ataques de suplantación en canales no regulados, como WhatsApp, correo electrónico o llamadas desde numeración internacional.

Considera que el efecto sobre el fraude dependerá de la capacidad técnica de los operadores para validar el SENDER ID al momento de la entrega, condición que no está garantizada en el régimen propuesto.

Además, advierte que la publicación de la numeración utilizada para cobranza podría deteriorar la contactabilidad, al permitir que los clientes en mora identifiquen y bloqueen sistemáticamente esos números, sin que se prevean mecanismos para detectar bloqueos masivos, rotar la numeración o habilitar líneas alternativas. En consecuencia, solicita:

(i) Modificar el artículo 6.14.2.2 para que la inscripción de SENDER ID y códigos cortos del sector financiero se realice mediante consultas puntuales y autenticadas, de forma que el ciudadano pueda verificar un identificador específico, en lugar de acceder a un catálogo público; o, subsidiariamente, condicionar su apertura a la implementación de una validación efectiva del SENDER ID al momento de la entrega; y

(ii) Establecer, para la numeración corporativa, mecanismos de monitoreo de bloqueos masivos, procedimientos expeditos de rotación o sustitución que no obliguen a reiniciar la inscripción y criterios objetivos para diferenciar el bloqueo individual legítimo del bloqueo sistemático inducido.

En relación con la asignación del SENDER ID, manifiesta que el parágrafo 2 prevé un único identificador por NIT, sin permitir su uso compartido entre personas jurídicas relacionadas. Señala que, en estructuras de financiamiento donde varias entidades de un mismo grupo intervienen en el flujo de un producto, los mensajes de autenticación o verificación pueden enviarse antes de determinar cuál entidad otorgará finalmente el servicio o crédito. En esa etapa no existiría un SENDER ID válido asociado a un NIT específico.

Por ello, solicita adicionar un parágrafo al artículo 6.12.2 que permita a los grupos económicos acreditados ante el validador contar con un SENDER ID compartido, asociado a una marca común y respaldado por los NIT de las entidades participantes, sujeto al cumplimiento individual del proceso de KYC. Como alternativa, propone reconocer un «SENDER ID de flujo previo a decisión», asignado a la entidad encargada del proceso de vinculación del grupo.

Finalmente, señala que la resolución no contempla la situación de los proveedores internacionales de comunicaciones en la nube que no son PRST ni integradores tecnológicos inscritos en Colombia, lo que genera incertidumbre sobre su articulación con el nuevo régimen y la asignación de responsabilidades.

En este sentido, solicita a la CRC emitir lineamientos que aclaren si estos proveedores pueden actuar como integradores tecnológicos bajo el régimen colombiano, si deben integrarse con el validador centralizado o si la responsabilidad regulatoria recae exclusivamente en la entidad local asignataria del SENDER ID.

CCIT

Indica que el artículo 1 del Proyecto de Resolución define el SENDER ID como un recurso de identificación administrado por la CRC, destinado a identificar al responsable del contenido enviado por SMS y USSD. Por su parte, el Capítulo 12 (artículos 6.12.1.1 y siguientes) regula su asignación y condiciona la posibilidad de cursar tráfico A2P a la tenencia de un SENDER ID.

Afirma que, aunque la CRC administra legítimamente ciertos recursos de identificación, esta competencia debe ejercerse dentro de los límites de su administración técnica, eficiente y segura, sin convertirlos en instrumentos de autorización previa para actividades económicas o comunicaciones legítimas.

CCIT reconoce la importancia del SENDER ID para identificar con mayor claridad al originador de comunicaciones A2P, reducir la suplantación y mejorar la confianza del usuario. Sin embargo, considera que convertirlo en un requisito administrativo previo, con asignación única por entidad, exigencias de

validación, causales de recuperación y dependencia del validador centralizado, podría transformarlo en una barrera de acceso y permanencia en el mercado.

Concluye que un régimen de asignación previa, sujeto a tiempos administrativos y causales de recuperación, resulta incompatible con la velocidad operativa de los servicios digitales y la incorporación ágil de nuevos remitentes legítimos. En la práctica, podría generar barreras de entrada para startups, comercios digitales y desarrolladores, así como demoras para proveedores de mayor escala, con el riesgo de que algunos servicios de seguridad no puedan operar en Colombia.

CRISTIAN CANTILLO

Formula las siguientes preguntas:

¿Cuál es el ámbito de aplicación de la resolución respecto de los canales propios y cerrados de mensajería del operador, como las notificaciones push integradas en su aplicación oficial, los servicios de mensajería mediante applets o STK en la tarjeta SIM y los protocolos RCS propios? Dado que estas comunicaciones no transitan por el canal tradicional de mensajería mayorista SMS A2P de interconexión, sino que se transmiten cifradas sobre la red de datos del operador hacia sus propios usuarios, ¿se encuentran excluidas de las obligaciones de validación previa, registro de SENDER ID y uso de plantillas?

De no estar excluidas, ¿con fundamento en qué facultad legal la CRC regularía el contenido y envío de notificaciones internas de aplicaciones privadas del operador? Asimismo, cuestiona si imponer la validación previa de plantillas a las notificaciones push o mensajes in-app podría vulnerar el principio de neutralidad tecnológica previsto en la Ley 1341 de 2009 y constituir una intervención desproporcionada en la libertad de empresa y el desarrollo de software propio.

CLARO

Señala que la viabilidad técnica del SENDER ID está limitada a los remitentes alfanuméricos de hasta 11 caracteres soportados nativamente por los estándares GSM/3GPP y el protocolo SMPP (Short Message Peer-to-Peer), utilizado para conectar a los Integradores Tecnológicos (IT) con los centros de mensajería (SMSC) de los operadores. Este límite comprendería el SENDER ID y el código corto.

Indica que el SENDER ID alfanumérico es compatible con los terminales de manera independiente del dispositivo, pues no requiere teléfonos inteligentes ni planes de datos. Puede visualizarse tanto en teléfonos básicos 2G como en terminales 4G y 5G, siempre que utilice hasta 11 caracteres en formato ASCII. Por ello, considera que presenta viabilidad técnica inmediata y cobertura universal sobre los terminales compatibles con estos estándares.

Respecto de la asignación, señala que el Proyecto establece que el PCA debe solicitar ante la CRC el SENDER ID a nombre del creador del contenido. Al respecto, propone que esta obligación recaiga directamente sobre el creador o responsable del contenido, dado que el identificador está asociado a la

identidad, actividad y responsabilidad del remitente final, quien conoce, controla y responde por los mensajes enviados.

Considera que la solicitud y administración directa por parte del responsable del contenido fortalece la trazabilidad, garantiza la correspondencia entre el identificador y el remitente, facilita la supervisión de las autoridades y reduce los riesgos de suplantación o uso indebido. Asimismo, permite que cada agente asuma las obligaciones relacionadas con la información y las actividades que controla.

Por otra parte, advierte que la limitación a un único SENDER ID por empresa genera problemas operativos, especialmente para grandes corporaciones que requieren identificadores diferenciados por marca, línea de negocio o tipo de comunicación. Por ejemplo, una entidad financiera podría necesitar SENDER ID distintos para mensajes de autenticación, alertas de seguridad, notificaciones transaccionales y comunicaciones comerciales. Concentrarlos en un solo identificador dificultaría que el usuario distinga y priorice los mensajes críticos.

Añade que, sin un mecanismo inmediato de validación cruzada, una empresa legalmente constituida podría solicitar identificadores similares a marcas reconocidas, como «AMAZ0N» o «DIAN_COL». Por ello, propone vincular la asignación del SENDER ID con la validación de las marcas registradas ante la SIC o de los nombres comerciales inscritos en el RUES.

También solicita excluir caracteres especiales y homógrafos que puedan utilizarse para engañar al usuario, como la sustitución de la letra «O» por el número «0» o el uso de caracteres cirílicos visualmente similares. En consecuencia, propone exigir que los SENDER ID utilicen exclusivamente caracteres alfanuméricos estándar en formato ASCII.

Frente a la limitación de un único código corto y un único SENDER ID por titular, considera que resulta excesiva y desconoce la realidad operativa de los modelos de negocio que utilizan servicios de mensajería. Una misma empresa puede administrar varias marcas, productos, servicios, unidades de negocio o procesos de comunicación, cada uno de los cuales puede requerir identificadores propios.

La restricción dificultaría la identificación del origen y propósito de las comunicaciones, reduciría la trazabilidad y generaría confusión respecto de la entidad, área o servicio que origina el mensaje. Asimismo, desconocería las estructuras corporativas complejas, integradas por diferentes unidades de negocio, filiales, marcas o plataformas tecnológicas que requieren identificadores independientes.

Desde la perspectiva de prevención del fraude, considera que el uso de múltiples identificadores debidamente registrados y asociados a un responsable no genera riesgos adicionales. Por el contrario, mejora la trazabilidad, facilita la identificación del origen de las comunicaciones y permite gestionar de manera diferenciada los incidentes, reportes y controles de seguridad.

Añade que el Proyecto no presenta evidencia de que limitar a un único código corto o SENDER ID por titular contribuya a mitigar el fraude, ni analiza los impactos operativos, comerciales y tecnológicos para los agentes que utilizan legítimamente varios identificadores.

Esta limitación también desconoce la diversidad de roles dentro del ecosistema de mensajería. Una empresa de telecomunicaciones puede actuar simultáneamente como PRST, PCA o IT y requerir identificadores para sus propias comunicaciones, así como para los servicios que presta a terceros. La imposición de un único identificador dificultaría separar las comunicaciones según su naturaleza y determinar claramente al responsable de cada mensaje.

Por lo anterior, solicita permitir que un mismo titular cuente con varios códigos cortos y SENDER ID cuando exista una justificación operativa, comercial o funcional, siempre que estén debidamente registrados, asociados a un responsable identificable y sujetos a las medidas de control y trazabilidad previstas en la regulación.

En consecuencia, solicita eliminar el artículo 6.4.2.2.2, según el cual se negará una nueva asignación cuando el solicitante ya tenga un código corto A2P registrado en el SIGRI, salvo que solicite simultáneamente la devolución del anterior.

Finalmente, señala que no se justifica la creación de un validador centralizado si su función se limita a administrar un único código corto y un único SENDER ID por empresa.

INETUM

Solicita aclarar si, dentro de la gestión del SENDER ID, se han contemplado los distintos actores que intervienen en la cadena de envío de mensajes SMS: el proveedor de origen, encargado de generar los mensajes y validar la autorización del alias; el proveedor de tránsito, que intermedia el tráfico y aplica validaciones sobre el origen y registro del SENDER ID; y el proveedor de terminación, responsable de entregar el mensaje al usuario final.

Asimismo, frente a la regla de asignar un único SENDER ID por NIT o documento de identificación, solicita precisar su aplicación para empresas con diferentes marcas, productos o denominaciones comerciales que podrían requerir múltiples identificadores para reconocer adecuadamente el origen de sus comunicaciones.

NEXVIA

Respecto de la cadena de valor del servicio SMS A2P, señala que el Proyecto invierte la arquitectura funcional definida por la CRC en la Resolución 6522. El Integrador Tecnológico es el agente que provee la infraestructura de conexión entre los PRST y los PCA sin conexión directa, mientras que el PCA es responsable de la producción y consolidación de contenidos y puede o no estar conectado directamente. En su criterio, exigir al PCA conexión directa e infraestructura propia, prohibir el tráfico en nombre de

terceros y restringir el SENDER ID a titulares con NIT colombiano rompe varios eslabones de la cadena de valor.

Afirma que la consecuencia práctica no sería la mitigación del fraude, sino una desintermediación forzosa. Las entidades financieras, plataformas globales y empresas sin sucursal en Colombia quedarían impedidas para enviar comunicaciones transaccionales, incluidos códigos OTP, salvo que contraten directamente con el PRST.

Asimismo, considera que la identificación unívoca de cada empresa frente al usuario ya cuenta con un recurso diseñado para ese fin: el NDC 940. A su juicio, bastaba ajustar su régimen para incorporar requisitos de verificación, como la titularidad de la marca o razón social, el soporte documental y las plantillas de contenido, sin crear un recurso alfanumérico paralelo, un validador privado, nuevas causales de recuperación y un régimen de transición que desmonta la numeración existente.

Frente al parágrafo 1 del artículo 6.12.1.2, sostiene que la prohibición desconoce que las calidades de PCA e IT concurren de manera habitual y legítima en un mismo agente inscrito en el RPCAI. Los Integradores Tecnológicos también requieren identificarse ante sus usuarios y clientes para remitir notificaciones de plataforma, alertas de servicio y comunicaciones operativas. Negarles el SENDER ID los excluye del mecanismo de identificación que el Proyecto pretende hacer universal y obligatorio..

Respecto del parágrafo 2 del mismo artículo, afirma que exigir sucursal en Colombia a toda empresa extranjera que pretenda identificarse ante usuarios colombianos impediría las comunicaciones transaccionales globales. Plataformas internacionales de redes sociales, comercio electrónico, transporte o servicios en la nube envían códigos OTP, confirmaciones y alertas derivados de relaciones contratadas por el usuario. Estas empresas difícilmente constituirían una sucursal local para terminar mensajes de bajo valor unitario, por lo que las comunicaciones podrían dejar de llegar o migrar a canales no regulados, deteriorando la seguridad del usuario.

Añade que este requisito no guarda relación directa con la finalidad antifraude, pues la trazabilidad del remitente internacional puede garantizarse mediante el PCA o IT local que cursa el tráfico y responde por él. Sin embargo, la prohibición de cursar tráfico de terceros prevista en el numeral 6.12.3.2.6 eliminaría también esta alternativa, dejando a las comunicaciones internacionales sin un canal lícito.

De igual forma, señala que la regla de un único SENDER ID por NIT desconoce la operación de grupos empresariales y entidades con múltiples marcas, líneas de negocio o unidades funcionales. Una misma entidad financiera, por ejemplo, puede operar banca personal, seguros y fiduciaria con identidades comerciales distintas, por lo que la restricción obligaría a mezclar comunicaciones que el recurso pretende diferenciar.

Advierte además que esta regla contradice el documento soporte del Proyecto, que presenta ejemplos diferenciados por propósito dentro de una misma entidad, como «Banco XX – Citas», «Banco XX – Transacciones» y «Banco XX – Mercadeo». La motivación ofrece una granularidad que el articulado

impide al limitar la asignación a un único SENDER ID por NIT, inconsistencia que, a su juicio, debe corregirse antes de la expedición del acto.

Respecto de los numerales 6.12.2.1.1, 6.12.2.1.5, 6.12.2.2.2 y 6.12.2.2.5, señala que corresponden a reglas operativas de las restricciones cuestionadas y, por tanto, deberían eliminarse junto con ellas, dado que:

(i) La exigencia de inscripción como PCA y de sucursal nacional excluye a titulares legítimos de marcas globales;
(ii) Vincular el SENDER ID a un código corto específico y a un contrato vigente con su asignatario genera un riesgo sistémico, pues la recuperación del código dejaría sin soporte los SENDER ID asociados y obligaría a rehacer contratos y registros, mientras los usuarios dejan de recibir comunicaciones; y,
(iii) La verificación de unicidad por NIT aplica la regla de un único SENDER ID cuya eliminación solicita.

Manifiesta que el Proyecto elimina en la práctica la figura del Integrador Tecnológico. Esta calidad exige inversión en infraestructura, contratos de acceso directo con los PRST y gestión administrativa frente a los operadores. Al exigir que los PCA acrediten conexión directa y contrato vigente con un PRST, el Proyecto equipara funcionalmente a PCA e IT y hace innecesario al intermediario especializado, alterando la estructura del mercado mediante requisitos propios de la función del IT.

En este contexto, propone que el SENDER ID se asigne con base en la titularidad legítima del identificador —marca, razón social o denominación oficial— y en la responsabilidad verificable de un agente local que curse el tráfico. Asimismo, solicita que no quede vinculado rígidamente a un código corto determinado y que se permita su portabilidad operativa inmediata entre asignatarios ante recuperación del código, terminación contractual o decisión comercial.

Frente al numeral 6.12.3.1.5, sostiene que la obligación de mantener vigencia contractual «en todo momento» convierte cualquier interrupción contractual ordinaria, como una terminación, renegociación o recuperación del código del proveedor, en causal automática de pérdida del recurso, sin periodo de gracia. Sumada al requisito de conexión directa operativa a un PRST, la regla traslada al titular del SENDER ID contingencias contractuales ajenas sobre las cuales no tiene control.

Finalmente, señala que, si la finalidad es asegurar la trazabilidad, bastaría con exigir que el SENDER ID curse tráfico únicamente a través de agentes inscritos y responsables, y que cualquier cambio de canal sea informado al Administrador, sin establecer la pérdida automática del recurso por circunstancias contractuales.

TIGO

El operador señala que la implementación del modelo de identificación basado en el SENDER ID debe resolver previamente aspectos técnicos aún indefinidos, con impacto directo en la operación y el dimensionamiento de la red: la interacción del validador con el flujo de mensajes y sus efectos sobre la señalización y los tiempos de establecimiento; la especificación de APIs seguras; el plan de contingencia ante la indisponibilidad del validador; el funcionamiento del tráfico bidireccional entre el PCA y el usuario final; y la capacidad (TPS) requerida para concentrar el tráfico de múltiples marcas en un único código corto por agente.

Considera que este último aspecto es crítico, pues actualmente la capacidad se asigna y dimensiona por relación de acceso. Por tanto, la consolidación del tráfico en un único código no debe generar cuellos de botella que retrasen o impidan la entrega oportuna de los mensajes, especialmente los de autenticación y transaccionales, cuya inmediatez es esencial.

SAEM

Sostiene que el Proyecto crea el SENDER ID alfanumérico de 3 a 11 caracteres, asigna uno por NIT o cédula (artículo 6.12.1.2, parágrafo 2) y exige que los solicitantes extranjeros establezcan una sucursal en Colombia. Asimismo, dispone que el SENDER ID corresponda a la razón social, nombre comercial o marca registrada (artículo 6.12.1.1).

Al respecto, señala que, en su calidad de IT, SAEM gestiona el tráfico de numerosos PCA. Considera razonable la regla de un único SENDER ID por NIT para identificar al originador, pero advierte que exigencias como la marca registrada o las denominaciones reservadas pueden retrasar la vinculación de clientes legítimos y llevarlos hacia canales no regulados.

Indica que Singapur hizo obligatorio en enero de 2023 el SMS Sender ID Registry (SSIR), bajo el cual los remitentes no registrados se identifican como «Likely-SCAM». Aunque inicialmente disminuyó el smishing mediante cabeceras suplantadas, posteriormente el fraude se desplazó hacia plataformas OTT, llamadas de voz y nuevas modalidades de spoofing, mientras las pérdidas totales por estafas continuaron aumentando.

Como conclusión, señala que un registro de remitentes reduce un vector específico, pero no el fraude agregado si no se actúa simultáneamente sobre el origen ilícito. Por ello, considera necesario calibrar la exigencia para no excluir a los actores legítimos.

Finalmente, propone aceptar como soporte del identificador no solo la marca registrada, sino también el nombre comercial, la enseña o el uso notorio acreditado, así como publicar con suficiente antelación la lista de palabras reservadas y establecer un mecanismo de objeción.

SEGUROS BOLÍVAR

Señala que el artículo 10 de la Ley 1581 de 2012 establece excepciones al deber de autorización previa para ciertos casos, como los mensajes regulatorios o las confirmaciones transaccionales inmediatas relacionadas con pólizas. No obstante, para las comunicaciones comerciales, el titular de los datos debe haber autorizado previamente su contacto, lo cual constituye la base del relacionamiento con el cliente.

Lo anterior, en relación con lo dispuesto en los numerales 6.12.1.3.1 a 6.12.1.3.4 del artículo 6.12.1.3 del borrador de resolución y su documento soporte.

SINCH

Señala como impacto positivo en la confianza del usuario el reemplazo de códigos numéricos genéricos por un SENDER ID alfanumérico, al considerarlo una de las medidas más efectivas para mejorar la experiencia del usuario. Este mecanismo permite identificar visualmente y de inmediato a entidades legítimas, como bancos o comercios, reduciendo la efectividad del smishing. No obstante, advierte los siguientes retos operativos:

- El éxito de la medida dependerá de que la CRC establezca un proceso de validación ágil y riguroso para la asignación de los SENDER ID, evitando que actores malintencionados registren nombres similares a marcas reconocidas mediante técnicas de spoofing o suplantación tipográfica.
- Los tiempos de registro podrían constituir una barrera para los proveedores de contenido que requieran implementar rápidamente campañas con SENDER ID asociados a productos o servicios de una empresa.
- Debe definirse la gestión y gobernanza del registro de SENDER ID en escenarios con múltiples proveedores, en los que varios PCA puedan enviar SMS para una misma entidad.
- Asimismo, solicita aclarar el número máximo de SENDER ID que pueden asociarse a un mismo código corto A2P administrado por el agente solicitante.

PTC

Considera indispensable esta medida, dado que el SENDER ID es un recurso de identificación administrado por la CRC que permite identificar de manera única e inequívoca a la persona natural o jurídica responsable de la producción y generación de contenidos o aplicaciones enviados mediante SMS y USSD.

En este sentido, el usuario podrá identificar de forma clara e inmediata al originador del contenido, adoptar decisiones informadas sobre el tratamiento de sus datos personales y valorar con mayor certeza la legitimidad de las comunicaciones recibidas. Asimismo, la medida se alinea con tendencias regulatorias internacionales orientadas a fortalecer la transparencia y trazabilidad de las comunicaciones electrónicas.

Como referencia, menciona el caso de España, donde la implementación del Registro de Alias ha mostrado resultados preliminares positivos en la identificación de remitentes, la reducción de riesgos de fraude y el fortalecimiento de la confianza de los usuarios. No obstante, antes de establecer el bloqueo obligatorio de mensajes y llamadas, se adoptaron medidas técnicas y una implementación gradual.

Al respecto, señala que la Comisión Nacional de los Mercados y la Competencia (CNMC) reconoció los retos técnicos asociados al desarrollo, implementación y operación escalonada de las medidas de bloqueo. Por ello, la modificación de la Orden TDF/149/2025 estableció un periodo aproximado de un año para el bloqueo de mensajes enviados con alias no registrados.

PTC considera necesario establecer un periodo de transición más amplio que el previsto en el Proyecto. Los artículos 2.1.10.7.2.1.5.2 y 2.1.10.7.2.2.4.3 fijan un plazo de tres meses, contado desde la publicación de la resolución en el Diario Oficial, para cumplir y validar obligaciones como la implementación y acreditación ante la CRC de sistemas de monitoreo de SMS, el bloqueo de llamadas internacionales entrantes con CLI nacional, el etiquetado de llamadas publicitarias, el monitoreo en tiempo real del tráfico y la creación de listas de no originación (DNO).

Considera que este plazo es corto frente al conjunto de actividades requeridas, que incluyen gestiones administrativas internas, obtención y aprobación de presupuestos, desarrollos tecnológicos y actuaciones de terceros. La imposibilidad de ejecutar adecuadamente estas actividades podría generar implementaciones irregulares o defectuosas.

Por lo anterior, solicita a la CRC considerar que los PRST no cuentan con el mismo nivel de desarrollo tecnológico y que las inversiones y cargas administrativas deben evaluarse de acuerdo con el tamaño y las capacidades de cada operador.

Respuesta CRC:

La CRC observa que los comentarios presentados por **ANDI**, **ASOBANCARIA**, **ANDESCO**, **BLIPBLIP**, **COLOMBIA FINTECH**, **CCIT**, **CRISTIAN CANTILLO**, **CLARO**, **INETUM**, **NEXVIA**, **TIGO**, **SAEM**, **SEGUROS BOLÍVAR**, **SINCH** y **PTC** abordan distintos aspectos del diseño propuesto para el SENDER ID. De manera general, los agentes reconocen que este recurso puede contribuir a mejorar la identificación del remitente de los mensajes A2P, fortalecer la trazabilidad, reducir los riesgos de suplantación y aumentar la confianza de los usuarios frente a las comunicaciones recibidas mediante SMS y, cuando corresponda, USSD.

En ese sentido, existe una tendencia coincidente en valorar positivamente la finalidad perseguida con la creación del SENDER ID. Sin embargo, los comentarios formulan observaciones específicas sobre su naturaleza jurídica, la regla de asignación, los sujetos legitimados para solicitarlo, la relación con códigos cortos y contratos, los criterios de validación, la clasificación de mensajes, el tratamiento de mensajes

críticos, la publicación de identificadores, los remitentes extranjeros, el ámbito de aplicación, la viabilidad técnica, la posibilidad de pruebas controladas y los requisitos documentales.

A continuación, la CRC se pronuncia sobre cada uno de estos aspectos.

2.1.1 Naturaleza del SENDER ID como recurso de identificación y no como habilitación previa

ANDI y **CCIT** manifestaron una preocupación coincidente en torno a que el SENDER ID pudiera convertirse, en la práctica, en una habilitación previa para que los generadores de contenido puedan comunicarse con sus usuarios. A su juicio, si bien la CRC administra legítimamente recursos de identificación, esa competencia debe ejercerse dentro de los límites propios de la administración técnica, eficiente y segura de dichos recursos, sin transformar el SENDER ID en un instrumento de autorización previa de actividades económicas o comunicaciones legítimas.

Los agentes no cuestionan la utilidad del SENDER ID como mecanismo de identificación del remitente, sino el alcance que podría derivarse de su configuración como requisito para cursar tráfico A2P.

Al respecto, es necesario resaltar que el documento soporte identificó que una de las problemáticas asociadas al fraude mediante SMS es la baja efectividad de las herramientas existentes para prevenir y mitigar la suplantación del remitente y el contacto a usuarios con fines fraudulentos. En ese marco, se consideró pertinente evaluar medidas orientadas a fortalecer la trazabilidad del tráfico A2P, la verificación de clientes y el registro de identificadores de remitentes.

Por su parte, el proyecto de resolución define el SENDER ID como un recurso de identificación administrado por la CRC, asociado al responsable del contenido enviado mediante SMS y USSD, y regula sus condiciones de asignación y uso dentro del Régimen de Administración de Recursos de Identificación.

En ese sentido, la CRC no comparte la interpretación según la cual el SENDER ID constituye una habilitación previa para desarrollar actividades económicas, prestar servicios digitales o cursar comunicaciones legítimas. La medida se limita a regular las condiciones de asignación y uso de un recurso de identificación administrado por la Comisión, en ejercicio de sus competencias sobre administración de recursos escasos y recursos de identificación. Las obligaciones previstas no recaen sobre la actividad económica del agente en abstracto, sino sobre el uso de un identificador dentro del ecosistema de mensajería A2P, cuya finalidad es garantizar trazabilidad, seguridad, uso eficiente del recurso y prevención de suplantaciones.

Adicionalmente, la asignación de un recurso de identificación no puede entenderse exclusivamente como una habilitación para su uso, sino también como una fuente de deberes asociados a su adecuada utilización. En esa medida, quienes pretendan usar recursos de identificación administrados por la CRC

para cursar tráfico A2P deben sujetarse a las condiciones definidas para asegurar su uso eficiente, seguro y trazable.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de modificar la propuesta bajo el entendimiento de que el SENDER ID configuraría una habilitación previa de actividades económicas o comunicaciones legítimas. No obstante, la Comisión mantendrá en la motivación de la medida la precisión de que el SENDER ID corresponde a un recurso de identificación y que su regulación se circunscribe a las condiciones de asignación y uso de dicho recurso.

2.1.2 Regla de un único SENDER ID por titular

ANDESCO, **BLIPBLIP**, **COLOMBIA FINTECH**, **CLARO**, **INETUM**, **NEXVIA** y **SINCH** cuestionaron la regla de asignación de un único SENDER ID por NIT, cédula o documento de identificación. De manera coincidente, señalaron que dicha limitación no refleja la realidad operativa de empresas con múltiples marcas, líneas de negocio, productos, unidades funcionales o tipos de comunicación.

Los agentes indicaron que una misma entidad puede requerir identificadores diferenciados para mensajes de autenticación, alertas de seguridad, notificaciones transaccionales, comunicaciones comerciales, gestión de cobranza, atención al cliente o comunicaciones regulatorias. También advirtieron que concentrar todas las comunicaciones en un único identificador podría afectar la experiencia del usuario, reducir la claridad sobre la finalidad del mensaje e incluso generar incentivos artificiales a la fragmentación societaria.

Al respecto es de mencionar que el documento soporte planteó que el registro e identificación de remitentes constituye una medida relevante para combatir el envío de SMS fraudulentos, en la medida en que permite fortalecer la trazabilidad y reducir la suplantación del originador. El proyecto de resolución propuso inicialmente la asignación de un SENDER ID asociado al responsable del contenido, con el propósito de que el usuario pudiera identificar de forma clara al remitente.

No obstante, a la luz de los comentarios recibidos la CRC considera que la finalidad de identificación y trazabilidad no exige mantener una regla absoluta de unicidad. Reconoce que, en determinados casos, la asignación de varios SENDER ID a un mismo titular puede contribuir a diferenciar adecuadamente la finalidad de las comunicaciones y a mejorar la información disponible para el usuario, siempre que cada identificador se encuentre debidamente registrado, soportado y asociado a un responsable plenamente identificable.

Desde una perspectiva de prevención del fraude, permitir múltiples SENDER ID no elimina la trazabilidad si se conservan reglas claras sobre responsable, finalidad, soporte documental y condiciones de uso. En ese sentido, la segmentación por finalidad, marca, producto, servicio o línea de negocio podría fortalecer el control y facilitar la gestión diferenciada de incidentes.

Teniendo en cuenta lo anterior, la CRC acepta parcialmente los comentarios presentados sobre este punto. En consecuencia, se ajusta la resolución en el parágrafo 2 del artículo 6.12.1.2 para permitir que una misma persona natural o jurídica pueda contar con más de un SENDER ID, siempre que acredite una justificación operativa, funcional, comercial, marcaria, de seguridad, de segmentación de servicios o de diferenciación de comunicaciones frente al usuario.

2.1.3 SENDER ID para grupos empresariales, marcas comunes y flujos previos a decisión

COLOMBIA FINTECH, **ANDESCO**, **CLARO**, **INETUM** y **NEXVIA** plantearon que la asignación estricta por NIT puede generar dificultades para grupos empresariales, estructuras societarias complejas o modelos operativos en los que una marca comercial común es utilizada por varias entidades relacionadas.

COLOMBIA FINTECH explicó que, en determinados flujos de crédito o financiación, el usuario interactúa inicialmente con una marca común antes de que se determine cuál entidad jurídica otorgará efectivamente el producto. **NEXVIA** también señaló que grupos empresariales y entidades con múltiples marcas o unidades funcionales pueden requerir identificadores compartidos o diferenciados que reflejen su operación real.

Frente a este punto, tanto el documento soporte como el proyecto de resolución parten de la necesidad de que el usuario pueda identificar de manera clara al remitente de las comunicaciones y de que exista trazabilidad sobre el responsable del tráfico A2P.

La CRC reconoce que existen estructuras empresariales complejas y modelos en los que varias personas jurídicas pueden operar bajo una misma marca o denominación comercial. Sin embargo, la finalidad del SENDER ID es permitir que el usuario, los agentes de la cadena y las autoridades identifiquen de forma clara al responsable de la comunicación. Permitir que un mismo SENDER ID sea compartido por varias personas jurídicas podría generar ambigüedad sobre la responsabilidad frente al contenido, el tratamiento de datos personales, la atención de requerimientos, la gestión de incidentes y la adopción de medidas correctivas.

En ese orden de ideas, la posibilidad de asignar múltiples SENDER ID a un mismo titular, aceptada en el punto anterior, permite atender la necesidad de diferenciación de marcas, servicios o líneas de negocio sin diluir la responsabilidad jurídica del titular del recurso. Así, cada persona jurídica podrá solicitar los SENDER ID que requiera, siempre que acredite la justificación correspondiente, pero no se considera procedente admitir identificadores compartidos entre varias personas jurídicas como regla general en aras de proteger a los usuarios y atender la prevención del fraude y la adecuada trazabilidad de los SMS.

En consecuencia, la CRC no acepta la solicitud de permitir SENDER ID compartidos entre varias personas jurídicas, grupos empresariales o flujos previos a decisión, y mantendrá la regla según la cual el SENDER

ID debe estar asociado a un titular determinado y responsable identificable, sin perjuicio de que cada titular pueda solicitar múltiples SENDER ID cuando acredite la justificación prevista en la regulación.

2.1.4 Agente legitimado para solicitar la asignación del SENDER ID

ANDESCO y **CLARO** solicitaron que la asignación del SENDER ID pueda ser solicitada directamente por el creador o responsable del contenido, y no necesariamente por el PCA, integrador tecnológico o asignatario del código corto. Argumentaron que el SENDER ID identifica al responsable final de las comunicaciones, por lo que la solicitud directa fortalecería la correspondencia entre el identificador y el remitente.

Al respecto, el documento soporte describe que, en la operación actual del tráfico SMS A2P, los controles y la habilitación de remitentes se desarrollan en el marco de relaciones técnicas y comerciales entre PCA, integradores tecnológicos, operadores y plataformas SMSC. También se indica que la habilitación, modificación o retiro de remitentes requiere procesos internos coordinados entre áreas comerciales, mayoristas y técnicas.

En ese contexto, la CRC considera que el trámite de solicitud debe atender la forma en que opera efectivamente la cadena de valor de la mensajería A2P. En dicha cadena, los integradores tecnológicos son quienes gestionan de manera directa la relación comercial, técnica y operativa con los creadores o responsables de contenido, así como la integración necesaria para el curso de los mensajes.

Por tanto, radicar la solicitud a través del agente responsable de dicha integración permite simplificar y agilizar el trámite, al concentrar en un actor técnicamente habilitado la presentación de la información, la validación documental y la articulación con los demás agentes de la cadena de valor. Esta regla no desconoce la condición de asignatario del recurso de identificación ni la responsabilidad que adquiere el creador o responsable del contenido, y tampoco la responsabilidad sobre la información suministrada, la legitimidad del uso del SENDER ID ni el contenido de las comunicaciones enviadas.

En dicho contexto, la CRC no acepta la solicitud de permitir que la asignación del SENDER ID sea tramitada directamente por el creador o responsable del contenido y, en consecuencia, se mantiene la regla según la cual la solicitud deberá ser presentada por el integrador tecnológico o agente responsable de la integración técnica y operativa, en nombre del creador o responsable del contenido.

2.1.5 Vinculación entre SENDER ID, código corto, contrato o canal operativo

NEXVIA, **BLIPBLIP** y **TIGO** advirtieron que una vinculación rígida entre el SENDER ID, un código corto específico, un contrato vigente o un agente determinado puede generar riesgos de continuidad. En particular, se indicó que la terminación contractual, la recuperación de un código corto, la sustitución de proveedor o la migración técnica podrían afectar comunicaciones legítimas sí implican la pérdida automática o imposibilidad de uso del SENDER ID.

BLIPBLIP también señaló que concentrar el tráfico en un único código corto podría constituir un punto único de falla, mientras que **TIGO** llamó la atención sobre los posibles impactos en capacidad de procesamiento y oportunidad de entrega de mensajes transaccionales o de autenticación.

Al respecto, es importante mencionar que la finalidad de la asociación entre SENDER ID, códigos cortos y agentes de la cadena es asegurar trazabilidad, no impedir ajustes contractuales u operativos legítimos. En esa línea, tanto el documento soporte como la resolución reconocen que la gestión de remitentes y códigos cortos requieren coordinación técnica, pero no impiden que el originador de contenido asignatario de un SENDER ID pueda celebrar contratos con varios integradores tecnológicos para soportar su operación. En se sentido, la CRC no acepta el comentario.

2.1.6 Validación de marcas, nombres comerciales, homógrafos y denominaciones confundibles

CLARO, **ANDESCO**, **SAEM** y **SINCH** coincidieron en la necesidad de evitar que actores malintencionados registren SENDER ID similares a marcas reconocidas, entidades públicas, entidades financieras, operadores o denominaciones legítimas. **CLARO** propuso excluir caracteres especiales y homógrafos, y validar contra registros de marcas o el RUES. **SAEM** propuso admitir no solo marca registrada, sino también nombre comercial, enseña o uso notorio acreditado.

Al respecto es preciso señalar que el proyecto de resolución ya prevé reglas orientadas a evitar que el SENDER ID imite o reproduzca denominaciones que puedan inducir a error, así como requisitos documentales para acreditar la relación entre el identificador solicitado y el responsable del contenido.

En ese sentido, la CRC considera que no resulta procedente convertir el trámite de asignación del SENDER ID en un procedimiento de examen marcario, de oposición o de definición de derechos de propiedad industrial. Dichas materias cuentan con autoridades y procedimientos específicos dentro del ordenamiento jurídico, y en ese contexto la función de la CRC en este punto es administrar un recurso de identificación utilizado en el ecosistema de telecomunicaciones y verificar que su asignación no resulte manifiestamente contraria a las condiciones regulatorias previstas.

La incorporación de un sistema exhaustivo de validación marcaria o de análisis de homógrafos con efectos equivalentes a un examen de propiedad industrial podría generar mayores cargas operativas, retrasar la asignación del recurso y desbordar el alcance de la función regulatoria prevista para la administración de recursos de identificación. Sin perjuicio de ello, se mantienen las restricciones generales previstas en el proyecto para evitar identificadores manifiestamente engañosos, suplantadores o confundibles.

Teniendo en cuenta lo anterior, la CRC no acepta las solicitudes de modificar la propuesta para incorporar un sistema adicional de validación marcaria, verificación cruzada automática o reglas específicas sobre homógrafos distintas a las ya previstas. Se mantendrá la redacción del proyecto en

cuanto exige que el SENDER ID corresponda a soportes verificables y prohíbe identificadores que imiten o puedan inducir a confusión con terceros protegidos.

2.1.7 Clasificación de mensajes transaccionales, comerciales, híbridos, de cobranza y regulatorios

COLOMBIA FINTECH señaló que la distinción entre mensajes transaccionales, comerciales y regulatorios no siempre es clara en el sector financiero, especialmente cuando un mensaje combina elementos informativos, transaccionales y promocionales. También solicitó que las comunicaciones de cobranza, acuerdos de pago, reestructuración o recuperación de cartera asociadas a obligaciones vigentes sean clasificadas como transaccionales.

SEGUROS BOLÍVAR recordó que la Ley 1581 de 2012 contempla excepciones al deber de autorización previa en ciertos eventos, pero que las comunicaciones comerciales requieren autorización del titular.

Frente a este punto el proyecto de resolución establece categorías diferenciadas de mensajes con el propósito de determinar reglas aplicables a cada tipo de comunicación. Dicha clasificación busca aportar claridad al tratamiento de mensajes de autenticación, transaccionales, comerciales y regulatorios, y evitar que comunicaciones con finalidad comercial o promocional se cursen bajo categorías que no les corresponden.

En ese sentido, la CRC considera que no resulta procedente introducir una regla general según la cual los mensajes híbridos se clasifiquen únicamente por su propósito principal. La inclusión de contenidos promocionales, comerciales o de mercadeo dentro de comunicaciones transaccionales puede afectar las reglas aplicables en materia de autorización, exclusión, tratamiento de datos personales y derechos de los usuarios.

De ahí que cuando un mensaje incorpore elementos comerciales, deberán observarse las reglas correspondientes a dicha categoría, sin perjuicio de que el mensaje incluya también información transaccional u operativa. Esta aproximación protege el derecho del usuario a controlar la recepción de comunicaciones comerciales y evita que contenidos promocionales sean incorporados en mensajes exceptuados de autorización.

Respecto de las comunicaciones de cobranza, acuerdos de pago o reestructuración, la CRC considera que no corresponde introducir una regla general que clasifique la totalidad del ciclo de gestión de cartera como contenido transaccional, pues la naturaleza de cada mensaje dependerá de su finalidad concreta, su contenido y las reglas aplicables en materia de protección de datos personales, habeas data, protección al consumidor y contacto con usuarios.

Así las cosas, la CRC no acepta la solicitud de modificar la clasificación de mensajes ni de incorporar reglas especiales para mensajes híbridos o de cobranza. Se mantiene la estructura propuesta en el proyecto de resolución, sin perjuicio de que los agentes deban aplicar la normativa vigente en materia

de protección de datos personales, habeas data, Registro de Números Excluidos y protección al consumidor.

2.1.8 Publicación o consulta pública de SENDER ID, códigos cortos y numeración

COLOMBIA FINTECH manifestó que la publicación abierta de SENDER ID, códigos cortos y numeración corporativa puede convertirse en insumo para ataques de suplantación más sofisticados en canales no regulados. También señaló que, en el caso de numeración de cobranza, la publicación podría afectar la contactabilidad por bloqueos masivos de usuarios.

En relación con este punto, el documento soporte identificó la necesidad de fortalecer la confianza del usuario frente a los mensajes que recibe y de permitir una identificación más clara del remitente. En esa línea, el proyecto de resolución contempló mecanismos de inscripción y consulta de identificadores asociados a remitentes legítimos.

En esta línea, la CRC considera que la transparencia frente al usuario es un componente esencial de la medida. Permitir que los usuarios verifiquen si un SENDER ID, código corto o número se encuentra asociado a un remitente legítimo fortalece la confianza, facilita la identificación de comunicaciones sospechosas y contribuye a la prevención del fraude.

Los riesgos de suplantación en otros canales no se mitigan restringiendo la información al usuario, sino fortaleciendo los controles de validación, monitoreo, trazabilidad y uso adecuado de los recursos de identificación. Limitar de manera excesiva la consulta pública podría reducir la utilidad de la medida y afectar su finalidad preventiva.

En cuanto a los bloqueos de numeración utilizada para cobranza, la CRC recuerda que los usuarios conservan derechos frente a la recepción de comunicaciones, y que la contactabilidad de los agentes no puede prevalecer sobre las reglas aplicables en materia de protección de datos, protección al consumidor y mecanismos de exclusión.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de restringir el acceso público o sustituir la consulta prevista por un mecanismo de acceso limitado, y en ese orden de ideas se mantiene la propuesta orientada a permitir que los usuarios consulten los identificadores registrados, en los términos definidos en la regulación.

2.1.9 Proveedores internacionales de comunicaciones en la nube y remitentes extranjeros

COLOMBIA FINTECH y **NEXVIA** señalaron que el proyecto no contempla de forma suficiente la situación de proveedores internacionales de comunicaciones en la nube, plataformas globales o empresas extranjeras que envían mensajes de autenticación, confirmación, seguridad u otros mensajes

transaccionales a usuarios colombianos. **NEXVIA** sostuvo que exigir sucursal o presencia local a todo remitente extranjero podría llevar a que comunicaciones legítimas migren hacia canales no regulados.

Frente a este punto, es preciso mencionar que la finalidad del SENDER ID es garantizar que exista un responsable identificable por el uso del recurso y por el curso del tráfico A2P. En el caso de remitentes extranjeros, la trazabilidad y exigibilidad de las obligaciones regulatorias requieren que el responsable del SENDER ID pueda ser plenamente identificado y sujeto a requerimientos dentro del marco aplicable.

Así, el permitir el uso de SENDER ID por agentes extranjeros sin una presencia local suficiente o sin sujeción clara al régimen colombiano podría dificultar la supervisión, la adopción de medidas correctivas, la atención de reclamaciones, la verificación documental y la recuperación o suspensión del recurso en caso de uso indebido.

La CRC considera frente al punto que los acuerdos comerciales o técnicos con plataformas internacionales no pueden desplazar la necesidad de contar con un responsable regulatorio verificable para efectos de la administración del recurso de identificación.

En ese orden de ideas, la CRC no acepta la solicitud de flexibilizar los requisitos aplicables a remitentes extranjeros o proveedores internacionales de comunicaciones en la nube y, en consecuencia, se mantiene la exigencia prevista en el proyecto para garantizar trazabilidad, exigibilidad y responsabilidad sobre el uso del SENDER ID en Colombia.

2.1.10 Ámbito de aplicación frente a canales distintos de SMS y USSD

CRISTIAN CANTILLO solicitó aclarar si canales propios o cerrados de mensajería del operador, tales como notificaciones push integradas en aplicaciones, servicios de mensajería mediante applets/STK, protocolos RCS propios o mensajes in-app, quedan excluidos de las obligaciones de validación previa, registro de SENDER ID y uso de plantillas.

En relación con este punto es preciso mencionar que el documento soporte y el proyecto de resolución se estructuraron alrededor de medidas para mitigar el contacto a usuarios con fines fraudulentos mediante servicios móviles tradicionales, particularmente SMS y llamadas de voz, así como USSD cuando corresponda dentro del marco de los recursos de identificación regulados.

En consecuencia, las disposiciones relativas al SENDER ID se circunscriben al ámbito de aplicación definido en el proyecto, esto es, a comunicaciones A2P cursadas mediante SMS y, cuando corresponda, USSD, y por ende estas disposiciones no se extienden automáticamente otros mecanismos que no correspondan a los canales regulados en la actualidad por la CRC.

Teniendo en cuenta lo anterior, si bien la CRC plasma la aclaración solicitada en el presente documento de respuesta a comentarios, no se considera necesario modificar la resolución, en la medida en que el

ámbito de aplicación del proyecto ya delimita las obligaciones a los servicios y recursos regulados en el acto administrativo.

2.1.11 Viabilidad técnica, APIs, capacidad, tráfico bidireccional y plazos de implementación

TIGO, **PTC**, **SINCH**, **CLARO** y **BLIPBLIP** formularon observaciones sobre la necesidad de resolver aspectos técnicos asociados a la implementación del SENDER ID y de las medidas relacionadas. Se mencionaron, entre otros, la interacción con el flujo de mensajes, la especificación de APIs seguras, los planes de contingencia, el funcionamiento con tráfico bidireccional MO/MT, la capacidad de procesamiento —TPS—, los tiempos de activación de códigos cortos y la gradualidad de la implementación.

PTC señaló que no todos los PRST presentan el mismo nivel de desarrollo tecnológico y que los plazos inicialmente previstos podrían resultar insuficientes frente a las actividades de análisis, diseño, contratación, desarrollo, integración, pruebas y estabilización.

Al respecto, es preciso mencionar que el documento soporte reconoce de los comentarios remitidos por los interesados que las plataformas SMSC actualmente utilizadas no incorporan de forma generalizada mecanismos nativos de autenticación criptográfica, validación centralizada ni esquemas de autenticación extremo a extremo, y que cualquier implementación futura de modelos de validación requeriría desarrollos específicos, integración de APIs externas y adecuaciones sobre plataformas SMSC y motores de routing.

Por su parte, la CRC considera procedente revisar los plazos del régimen de transición para garantizar que las obligaciones asociadas al SENDER ID y demás medidas del proyecto sean implementadas de manera gradual, técnicamente viable y sin afectar la continuidad del servicio. En todo caso, la respuesta integral sobre los plazos de implementación y el régimen de transición será desarrollada en el numeral 6.1 del presente documento de respuestas.

En relación con la interoperabilidad, APIs, especificaciones técnicas, pruebas y condiciones operativas de implementación, la CRC considera que estos elementos deben ser desarrollados en el marco del CTLFSM, en tanto requieren coordinación entre los agentes involucrados, análisis de capacidades técnicas, definición de estándares operativos y validación de condiciones de interoperabilidad.

Teniendo en cuenta lo anterior, la CRC acepta parcialmente los comentarios en lo relativo a la revisión de plazos del régimen de transición, y la respuesta completa sobre este aspecto se desarrolla en el numeral 6.1 del documento de respuestas.

2.1.12 Sandbox regulatorio para validar medidas

ASOBANCARIA propuso considerar la implementación de un sandbox regulatorio que permita validar, en entornos controlados, las medidas relativas a identificación de remitentes, monitoreo de tráfico y etiquetado de comunicaciones antes de su despliegue a nivel nacional.

Al respecto, la CRC reconoce la utilidad de los entornos controlados de prueba para validar aspectos técnicos, operativos y de implementación de medidas regulatorias innovadoras. Si bien el documento soporte ya contiene un diagnóstico del problema y un análisis de alternativas que justifica la adopción de medidas para fortalecer la identificación y trazabilidad del tráfico A2P, ello no impide que, durante la fase de implementación, y en el marco de las reglas sobre el periodo de transición, puedan usarse herramientas de innovación como pilotos, pruebas controladas, mesas técnicas o ejercicios de seguimiento que permitan validar la operación de ciertos componentes del esquema.

En esa medida, la CRC considera procedente acoger la propuesta en el sentido de habilitar espacios de validación técnica o regulatoria durante la implementación, sin que ello implique suspender, condicionar la expedición de la regulación definitiva o modificar los plazos contemplados para su implementación.

Así las cosas, si bien la CRC acepta parcialmente el comentario e indica en este documento que se podrán emplear herramientas de innovación regulatoria como espacios de prueba, pilotos, mesas técnicas o mecanismos de seguimiento para validar aspectos operativos de las medidas, insiste también que la adopción de la regulación dentro de los tiempos especificados no puede quedar condicionada a la realización previa de un Sandbox Regulatorio.

En ese sentido, de manera complementaria es preciso mencionar que en el marco del CTLFSM se revisarán y recomendarán las decisiones técnicas que se consideren pertinentes para lograr la implementación de las medidas determinadas en el proyecto regulatorio dentro de los tiempos dispuestos para tal fin.

2.1.13 Requisitos de información, composición accionaria y proporcionalidad documental

BLIPBLIP cuestionó la exigencia de hacer pública la composición accionaria de la sociedad como requisito para solicitar un código corto o SENDER ID. De manera más general, algunos agentes señalaron que las cargas documentales pueden retrasar el onboarding de remitentes legítimos y generar barreras operativas.

Al respecto, el documento soporte identificó la verificación de clientes y remitentes como una medida relevante para prevenir el uso indebido de recursos de identificación y combatir el envío de SMS fraudulentos. En esa línea, el proyecto de resolución contempló requisitos documentales orientados a verificar la identidad del solicitante, la legitimidad del uso del recurso, la trazabilidad del tráfico y la debida diligencia sobre los agentes que participan en la cadena de valor.

En ese orden de ideas, la CRC considera que la información societaria, de control o composición accionaria puede ser relevante para adelantar procesos de debida diligencia, identificar beneficiarios reales, verificar relaciones entre agentes, prevenir el uso indebido de recursos de identificación y detectar riesgos asociados a solicitantes o asignatario y, eventualmente, servir de insumo probatorio con ocasión de un análisis de responsabilidad en sede administrativa o judicial por parte de las autoridades competentes, por lo que, en consecuencia, no se acoge la solicitud de eliminar este requisito.

En todo caso, la exigencia de esta información debe entenderse en función de la finalidad de prevención del fraude, trazabilidad y debida diligencia, y su tratamiento deberá sujetarse a las reglas aplicables en materia de reserva, confidencialidad, protección de datos personales y manejo de información sensible o reservada, cuando corresponda.

2.2 Código Corto A2P

ALDEAMO

Propone que se debe eliminar el artículo 6.4.1.4., en la medida que las empresas deberían tener la capacidad de tener múltiples códigos cortos si así lo consideran necesario y si cumplen con los requisitos, incluyendo los técnicos y de KYC.

Asimismo, de cara al artículo 6.4.2.1 asignación de códigos cortos para SMS, expone que el proceso se modifica y se vuelve complejo, dado que actualmente presenta demoras, no cuenta con claridad y trasparencia. Propone que se revise buscando agilizar la asignación y recuperación con estándares que definan las razones por las cuales una petición de asignación de códigos cortos pueda ser negada, así como qué evidencias y pruebas se consideran suficientes para evitar la recuperación de un código corto

CLARO

Sobre las obligaciones de debida diligencia de los asignatarios de códigos cortos, y el proceso de KYC establecido, **CLARO** menciona que es importante adicionar un artículo que establezca que, en caso de no aprobar el procedimiento, no se podrá celebrar contrato entre el dueño del SENDER ID y el PCA.

BLIPBLIP, NEXVIA E INALAMBRIA

Afirman que la regla que limita a cada agente a un único código corto A2P (artículo 6.4.1.4 y su correlato en el numeral 6.4.2.2.2) desconoce el principio de uso eficiente de los recursos escasos y la propia naturaleza del recurso, concebido para diferenciar tipos de servicio, contenido, modalidad y tarifa. Sus efectos comunes preocupan a las cuatro compañías:

• Convierte el código corto en un punto único de falla: su recuperación produce la invalidación masiva y automática de la totalidad de los SENDER ID vinculados, de modo que un agente que cursa millones de comunicaciones críticas puede quedar fuera de operación en segundos. La pluralidad de códigos que hoy opera como redundancia natural desaparece.
• Hace inoperante la mensajería interactiva de doble vía (MO/MT): con un solo código para todos los clientes y unidades de negocio resulta inviable identificar y enrutar correctamente el tráfico de doble vía, lo que destruye un segmento entero del negocio.
• Restringe un mercado que debería crecer: obligar a cada empresa usuaria a tramitar su propio código y SENDER ID generará una ola de solicitudes y activaciones difícil de absorber, y excluirá de hecho a quienes hoy operan bajo códigos compartidos.

NEXVIA

Señala que el aparte final del artículo 6.4.1.1 contradice la naturaleza del recurso definida por la propia Resolución CRC 5050, el código corto fue concebido para el posicionamiento e identificación de un tipo de servicio frente al usuario, informando el tipo de contenido, la modalidad de compra y los costos asociados, y expresamente no para la creación de canales dedicados. Indica que, bajo la arquitectura del proyecto, el usuario ya no percibe el código sino el SENDER ID alfanumérico, de modo que el código corto único queda reducido a matrícula técnica invisible, vaciado de la función que define su naturaleza, mientras las modalidades de contenido migran al SENDER ID (parágrafo del artículo 6.12.1.3 propuesto). La metodología de los códigos cortos se reproduce así bajo otro nombre, y el SENDER ID, separado ante el usuario por empresa, con plantillas y modalidades propias pasa a operar como el canal dedicado por cliente que la doctrina del recurso proscribe.

Manifiesta que la finalidad legítima de identificación unívoca del remitente cuenta, además, con un recurso preexistente y diseñado exactamente para ese fin, la numeración NDC 940, susceptible de incorporar los requisitos de verificación que el proyecto persigue (titularidad del identificador, soporte documental, plantillas), sin vaciar la función del código corto ni crear un recurso alfanumérico paralelo. Ambas funciones, pueden y deben coexistir conforme al régimen vigente.

Propone la siguiente redacción:

> «El código corto A2P es el recurso de identificación administrado por la CRC que identifica el tipo de servicio de contenidos y aplicaciones cursado por el agente que, en virtud de una relación contractual o de una servidumbre de acceso, cursa tráfico A2P de mensajería de texto (SMS). A través de los códigos cortos A2P que le sean asignados, el asignatario cursará el tráfico A2P de las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID, conservando la diferenciación de códigos por tipo de servicio, modalidad de contenido y tarifa.»

Con respecto al artículo 6.4.1.4. señala que la identificación inequívoca de agentes en el ecosistema ya cuenta con un recurso de numeración específicamente creado para ese fin, el NDC 940. Reasignarle esa

función al código corto desnaturaliza el recurso y duplica innecesariamente instrumentos de identificación. Indica que la unicidad ignora el principio de uso eficiente de los recursos escasos (artículo 2, Ley 1341 de 2009) tal como la propia CRC lo ha aplicado históricamente, los asignatarios cursan tipos de servicio diversos que exigen códigos diferenciados, y la regulación vigente prohíbe que los códigos operen como canales dedicados, lo que presupone pluralidad de códigos por asignatario según el tipo de contenido.

Manifiesta que la unicidad convierte además el código corto en punto único de falla de toda la operación. El código es el corazón técnico del agente, su recuperación, produce la invalidación masiva y automática de la totalidad de los SENDER ID vinculados. Bajo el régimen vigente, la pluralidad de códigos opera como redundancia natural que protege la continuidad del servicio; bajo el proyecto, un solo acto administrativo, o una sola decisión unilateral del PRST conforme al Parágrafo 4 del artículo 6.1.1.8, basta para que una empresa que cursa millones de comunicaciones críticas desaparezca operativamente en segundos. Ningún principio de administración de recursos escasos justifica diseñar deliberadamente un punto único de falla sistémico sobre el cual, además, se asienta la seguridad transaccional de los usuarios.

Respecto al Numeral 6.4.2.2.2, manifiesta que este numeral es la regla operativa de la unicidad cuya eliminación se solicitó en el punto anterior; cae por las mismas razones. Señala que la negación automática de asignaciones adicionales desconoce que la pluralidad de códigos responde a la diferenciación de servicios exigida por la naturaleza misma del recurso, y convierte la gestión eficiente del recurso escaso, función de la CRC, que debe evaluar caso a caso la justificación del uso.

Indica que la «solicitud simultánea de devolución del anterior» agrava el problema, en cuanto a que, fuerza la interrupción de servicios en operación, con usuarios activos, como condición para acceder a un nuevo recurso, sin régimen de continuidad que proteja las comunicaciones en curso.

Señala que el código corto único, invisible para el usuario bajo la arquitectura del proyecto, pierde toda función frente a este, la identificación inequívoca del agente que el artículo persigue es una función que la numeración NDC 940 ya cumple, sin sacrificar nada a cambio. De otro lado, la identificación visible queda confiada a un recurso alfanumérico imitable mediante variaciones tipográficas y homoglifos, elevando el riesgo de suplantación visual frente al usuario, exactamente lo contrario de la finalidad antifraude declarada.

Adicionalmente, menciona que el numeral 19.1.5 del régimen de transición revela la magnitud de la afectación, obliga a devolver códigos en operación con millones de usuarios activos, imponiendo migraciones masivas cuyo costo y riesgo el documento soporte ni siquiera cuantifica.

Afirma que elevar a causal de recuperación del código corto establecido en los términos del numeral 6.4.3.2.5, castiga con la muerte operativa del canal infracciones formales subsanables, sin gradualidad alguna (requerimiento, plan de ajuste, suspensión parcial del SENDER ID involucrado). Adiciona que el diseño concentra además el riesgo en cabeza equivocada, la conducta reprochable es del titular del

SENDER ID o de quien origina el contenido, pero la consecuencia recae sobre el asignatario del código y, por arrastre (Parágrafo 1 del mismo artículo), sobre todos los demás SENDER ID inocentes vinculados al código, incluidas entidades cuyas comunicaciones son críticas para los usuarios. En este punto, propone la siguiente redacción:

> «Envío reiterado y deliberado de mensajes de texto (SMS) en nombre de personas que no cuenten con SENDER ID asignado y vigente, previa verificación de que el asignatario del código corto A2P no adoptó las medidas de control a su alcance. La configuración de esta causal exigirá requerimiento previo del Administrador de Recursos de Identificación, otorgamiento de un plazo de ajuste no inferior a diez (10) días hábiles y persistencia de la conducta. El envío de mensajes sin plantilla verificada dará lugar a la marcación del tráfico conforme al numeral 6.4.3.1.7, y solo constituirá causal de recuperación cuando se acredite su utilización para contenido fraudulento.»

Con respecto al numeral 6.4.3.2.7, menciona que la causal de recuperación presupone que todo asignatario de código corto debe sostener un contrato de acceso directo con el PRST, lo que invierte la arquitectura del ecosistema, la conexión directa es la función del Integrador Tecnológico, no del PCA.

Señala que la causal ignora, además, la realidad contenciosa del acceso, la celebración del contrato no depende solo del solicitante sino de la voluntad del PRST, que históricamente niega y dilata. Un operador puede tardar más de un año en interconectar a un IT, como lo evidencian los procesos de imposición de servidumbre que la propia CRC ha debido tramitar. Indica que sancionar al solicitante con la pérdida del recurso por una demora que el propio régimen reconoce como imputable al operador es trasladar al débil las consecuencias del incumplimiento del fuerte.

Concluye que la solución que la Comisión ofrece a esos agentes es que migren a WhatsApp. Señala que es una admisión implícita de que la regulación no es viable para el pequeño negocio, que es quien más depende del SMS como canal universal de comunicación donde no hay datos. Afirma que si la Comisión estima indispensable verificar la materialización del acceso, la consecuencia proporcionada es la prórroga del plazo cuando la demora obedezca a hechos del PRST, o la activación oficiosa del trámite de solución de controversias, jamás la recuperación del recurso.

Adicionalmente, señala que el Parágrafo del artículo 6.4.3.2 conlleva una sanción por arrastre a terceros inocentes, la recuperación del código de un asignatario priva instantáneamente de canal a todos los SENDER ID vinculados (entidades financieras, prestadores de salud, plataformas) que ninguna conducta reprochable ejecutaron. Mientras esos terceros consiguen, contratan y registran una nueva relación comercial (trámite que en la práctica no se resuelve en días), los usuarios dejan de recibir comunicaciones vitales: códigos OTP, confirmaciones transaccionales, citas médicas. La medida castiga al usuario que dice proteger.

Mientras que, por su parte, el Parágrafo 2 del mismo artículo permite la suspensión del recurso desde el acto de apertura, esto es, antes de cualquier ejercicio del derecho de defensa, hasta por seis meses,

una medida materialmente sancionatoria anticipada, de duración equivalente a la liquidación de facto de una empresa del sector, sin las garantías mínimas de la Sentencia C-214 de 1994.

Señala que, en la práctica, la habilitación del Parágrafo 2 se traduce en la inutilización del recurso en cuestión de horas desde la apertura de la actuación, antes de cualquier traslado o ejercicio del derecho de defensa. Y el término de treinta (30) días hábiles del Parágrafo 1 es técnicamente insuficiente para la migración que presupone, el titular de un SENDER ID afectado (una entidad financiera, por ejemplo) debe identificar un nuevo asignatario de código corto, negociar y suscribir el contrato, registrar la vinculación ante el validador, obtener la aprobación de sus plantillas y reconfigurar sus integraciones técnicas, una secuencia que la operación real no resuelve en ese plazo. Durante el vacío resultante, el usuario queda sin claves OTP, sin confirmaciones transaccionales y sin alertas de seguridad, el riesgo de fraude no se mitiga, se amplifica, porque el defraudador encuentra a un usuario desconectado de los canales legítimos de verificación.

Indica que el contraste con la práctica reciente de la propia Comisión es elocuente. En la Resolución 8144 de 2026, la CRC acogió la solicitud de los PRST y amplió la entrada en vigor de las medidas hasta el 1 de julio de 2026, reconociendo expresamente que se trataba de «un tiempo razonable de aproximadamente cuatro meses y medio» que otorga «seguridad jurídica», y que era necesaria una «ventana de transición para culminar desarrollos técnicos y adelantar pruebas» (ello para una adecuación consistente en ajustar sistemas de medición y conciliación de tráfico). Señala que no es coherente que el regulador conceda a los operadores más robustos del mercado varios meses para una adecuación de sistemas, y otorgue a terceros inocentes (cuyo canal fue suprimido por conducta ajena) treinta (30) días hábiles para una migración contractual, registral y técnica completa, de la cual dependen las comunicaciones críticas de los usuarios.

Advierte que el régimen de los treinta (30) días hábiles del Parágrafo 1 presupone, para no interrumpir el servicio, que el asignatario afectado o los demás agentes del mercado disponen de códigos cortos adicionales hacia los cuales reenrutar de inmediato el tráfico de los SENDER ID vinculados. Ese presupuesto existe bajo el régimen vigente (de pluralidad de códigos) y desaparece bajo el propio proyecto, con la unicidad impuesta por el artículo 6.4.1.4, la recuperación del único código del asignatario deja a la totalidad de sus SENDER ID sin canal alguno desde el primer día, sin posibilidad técnica de re-enrutamiento interno. El proyecto destruye en un artículo el mecanismo de continuidad que presupone en otro, y la degradación del servicio recae directamente sobre los millones de usuarios finales que reciben por esos códigos sus comunicaciones críticas.

La continuidad del servicio al usuario debe ser el eje del régimen, la suspensión preventiva debe ser excepcional, motivada en riesgo grave y actual, limitada al SENDER ID o plantilla involucrados en la presunta infracción (no a todo el código), y de duración estrictamente necesaria. Frente al particular, propone la siguiente redacción:

> «PARÁGRAFO 1. La recuperación del código corto A2P no interrumpirá el tráfico de los SENDER ID vinculados ajenos a la causal que la motivó. El Administrador de Recursos de Identificación

habilitará un régimen de continuidad transitoria de hasta noventa (90) días hábiles durante el cual dichos SENDER ID podrán seguir cursando tráfico a través del integrador o asignatario que designen, mientras acreditan la nueva relación comercial. PARÁGRAFO 2. La suspensión temporal del recurso solo podrá ordenarse mediante acto motivado, previa valoración de riesgo grave y actual para los usuarios, se limitará al SENDER ID o plantilla presuntamente involucrados, se revisará de oficio cada treinta (30) días y no podrá exceder de tres (3) meses.»

SAEM

Sostiene que, según el proyecto, cada agente tendrá un único código corto A2P (art. 6.4.1.4) y los IT con múltiples códigos cortos deben consolidarlos en uno solo durante un período de transición de seis (6) meses (art. 19), eligiendo cuál conservar y migrando el resto, con notificación a usuarios y reglas de consentimiento (art. 19.1.5).

Al respecto, advierte que la consolidación implica perder códigos cortos que los clientes y los usuarios ya reconocen, reconfigurar enrutamientos y migrar consentimientos. Dice que técnicamente la identificación recae ahora en el SENDER ID, pero la pérdida de los códigos históricos tiene costo comercial y operativo real. Indica que seis meses, además condicionados a la previa publicación de la remuneración de la Fase II, es un plazo insuficiente frente a la magnitud del cambio (selección de validador, KYC de todos los PCA, asignación de recursos, registro y aprobación de plantillas, integración por APIs y consolidación), todo en cadena.

Propone lo siguiente: (i) Ampliar el período de transición a 12–18 meses, dado que las fases del artículo 19 son secuenciales y dependen unas de otras; (ii) permitir que un mismo IT conserve más de un código corto A2P cuando acredite necesidad técnica u operativa objetiva (segmentación de tráfico, continuidad de servicios críticos); (iii) reconocer plenamente la continuidad del consentimiento previo migrado y simplificar la notificación a usuarios; (iv) condicionar el inicio de la transición a que el ecosistema —no solo la remuneración de la Fase II— esté efectivamente listo (validador operativo y APIs publicadas).

HABLAME

Frente a las causales de recuperación del código corto A2P deben limitarse a la conducta propia del titular

Al respecto, **HABLAME** menciona que el artículo 12 subroga el Capítulo 4 del Título VI y concentra en el artículo 6.4.3.2 las causales para recuperar el código corto A2P, junto con los criterios de uso eficiente del artículo 6.4.3.1 y la suspensión prevista en sus parágrafos. A su juicio, para el integrador el código corto A2P es el recurso sobre el que se sostiene toda su operación y perderlo no es una sanción más sino que equivale a cerrar el negocio y a dejar sin servicio a todos sus clientes. Afirma que una consecuencia de esa gravedad solo puede proceder por una conducta propia, directa, comprobada y atribuible al titular del código. En su forma de ver, es la aplicación elemental del debido proceso, de la

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

tipicidad y del principio de que nadie responde sino por sus propios actos (artículo 29 de la Constitución). El integrador no puede pagar por lo que hagan terceros ni por obligaciones que la norma asigna al PRSTM, al validador, al originador, al PCA o al asignatario del SENDER ID. Revisadas una a una, varias causales rompen esa regla y deben corregirse.

Envío sin SENDER ID o sin plantilla vigente (numeral 6.4.3.2.5)

Esta causal permite recuperar el código por el envío de mensajes sin SENDER ID asignado o sin plantilla vigente. El problema es que el control que verifica esos requisitos no es del integrador, es del operador. El artículo 6.13.4.7.2 obliga al PRSTM a comprobar, antes de enrutar cada mensaje, que existan código corto, SENDER ID y plantilla válidos, y a bloquear el que no cumpla. Si el filtro está en cabeza del operador y aun así un mensaje sin SENDER ID o sin plantilla llega a cursarse, la falla es del filtro, no del integrador. Sancionar al integrador por un mensaje que el operador tenía el deber de bloquear es trasladarle la responsabilidad de una obligación ajena. A esto se suma que la asignación del SENDER ID y la aprobación de la plantilla dependen del PCA y del validador, de modo que el integrador ni siquiera controla los elementos cuya ausencia se le reprocha. Esta causal debe eliminarse respecto del asignatario del código corto A2P, salvo que se acredite una conducta propia y deliberada de este.

Mensajes atribuibles al mal uso de plantillas (numeral 6.4.3.2.6)

La causal habilita la recuperación por mensajes que potencialmente puedan atribuirse al mal uso de las plantillas. La palabra potencialmente es incompatible con cualquier régimen sancionatorio serio, porque permite retirar el recurso sobre una mera posibilidad, sin certeza ni prueba, lo que vulnera la seguridad jurídica y el principio de tipicidad. Además, el contenido de los mensajes y su correspondencia con la plantilla aprobada son responsabilidad de quien origina, que es el asignatario del SENDER ID, no el integrador. Como está redactada, la causal castiga al operador técnico por un hecho que ni controla ni decide. Debe reformularse para que solo proceda cuando se acredite que el asignatario del código, con conocimiento, permitió o facilitó el envío de tráfico no autorizado, y debe eliminarse la palabra potencialmente.

Infracciones de datos personales o de propiedad intelectual (numeral 6.4.3.2.10)

Esta causal permite recuperar el código por infracciones a las normas de protección de datos personales o de propiedad intelectual. Esas infracciones recaen sobre quien decide y controla el contenido y los datos, es decir, sobre el originador. La Ley 1581 de 2012 distingue con precisión entre el responsable del tratamiento, que define los fines y los medios, y el encargado, que se limita a tratar los datos por instrucción del responsable. El integrador encaja en la segunda categoría, porque transmite por cuenta del originador y no decide sobre el contenido ni sobre los datos. Imputarle a él una infracción de contenido desconoce esa distinción legal y termina sancionando a quien no es responsable. La causal debe reservarse al asignatario del SENDER ID y eliminarse respecto del asignatario del código corto A2P.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Incumplimiento de obligaciones generales y especiales (numerales 6.4.3.2.1 y 6.4.3.2.2)

Estas dos causales remiten de forma genérica al incumplimiento de las obligaciones generales y especiales del régimen. El problema es que entre esas obligaciones especiales figura el artículo 6.13.4.5.1, redactado como obligación de resultado mediante la palabra garantizar. Esa redacción convierte al integrador en garante de hechos que no dependen de él, sino del validador, del operador y del originador. Una causal de recuperación anclada en una obligación imposible de cumplir es, en la práctica, una causal abierta, porque siempre habrá un resultado que el integrador no pudo garantizar por no estar en sus manos. La solución pasa por reformular el artículo 6.13.4.5.1 como una obligación de medios, exigible cuando el integrador consultó los registros del validador y del SIGRI y actuó de buena fe, y por limitar estas causales al incumplimiento propio y comprobado del titular del código.

Criterio de uso eficiente que exige tráfico siempre verificado (numeral 6.4.3.1.7)

Este criterio de uso eficiente exige que el integrador curse únicamente tráfico de originadores con SENDER ID vigente y plantilla aprobada. Con ello se le impone ser garante permanente del estado de validación de terceros, un estado que administra el validador y que puede cambiar en cualquier momento sin que el integrador lo sepa. Si un SENDER ID o una plantilla pierden vigencia por una decisión del validador o del PCA, el integrador no tiene forma de anticiparlo en tiempo real. Convertir esa circunstancia en uso ineficiente, con la consecuencia de perder el código, es sancionarlo por algo que no controla. El criterio debe entenderse cumplido cuando el integrador consulta los registros del validador y del SIGRI antes de cursar el tráfico, y la pérdida sobrevenida de vigencia en cabeza de un tercero no puede imputársele.

Razones de interés general o seguridad nacional (numeral 6.4.3.2.9)

Esta causal permite recuperar el código por razones de interés general o de seguridad nacional, sin precisar el supuesto que la activa ni el procedimiento que debe seguirse. Una cláusula tan abierta deja al titular sin saber cuándo puede perder el recurso y habilita decisiones discrecionales, contrarias a la seguridad jurídica y al debido proceso. El interés general y la seguridad nacional son fines legítimos, pero su invocación no puede sustituir la motivación ni el procedimiento. La causal debe condicionarse a un acto administrativo motivado, con una causa concreta y demostrada, observancia del debido proceso y aplicación del principio de proporcionalidad, indicando siempre la medida menos gravosa disponible.

Efecto en cascada sobre los SENDER ID vinculados (parágrafo 1 del artículo 6.4.3.2)

El parágrafo dispone que la recuperación del código corto A2P afecta a todos los SENDER ID vinculados y concede treinta días hábiles para que cada uno migre a otro proveedor. La medida traslada la sanción a clientes que no incurrieron en ninguna conducta y, además, fija un plazo que en el mundo real es imposible de cumplir. Un banco, una entidad pública o una gran superficie no pueden adelantar una contratación, cambiar de integración tecnológica y certificarse en treinta días hábiles. El resultado sería la interrupción de servicios críticos como la autenticación, las alertas de seguridad y las notificaciones

transaccionales. El propio proyecto reconoce el problema en otro lugar: el parágrafo 1 del artículo 6.1.1.8 ordena, cuando la recuperación afecta a usuarios, una transición de seis meses a un año. No hay ninguna razón para que aquí, donde el número de afectados es mayor, el plazo se reduzca a treinta días. La consecuencia debe recaer sobre el SENDER ID o la plantilla responsable, sin arrastrar a los demás, y, cuando haya usuarios afectados, debe aplicarse la transición de seis meses a un año, preservando la continuidad del tráfico crítico.

Suspensión temporal durante el trámite (parágrafo 2 del artículo 6.4.3.2)

El parágrafo permite suspender el código hasta por seis meses mientras se tramita la actuación por las causales de los numerales 6.4.3.2.5 y 6.4.3.2.6. Una suspensión de esa duración, adoptada antes de cualquier decisión de fondo, equivale a sancionar de manera anticipada. Para cuando se resuelva si hubo o no infracción, la operación del integrador y la de sus clientes ya habrán sufrido un daño difícil de revertir. El efecto es todavía más desproporcionado si se considera que ambas causales se relacionan con conductas de terceros o con el contenido, frente a las cuales el integrador no es responsable. Una medida cautelar de esta gravedad solo puede proceder con prueba sumaria seria, mediante decisión motivada, por el término estrictamente necesario y de manera proporcional, y nunca cuando la causal se funde en conductas atribuibles a terceros.

Para dar coherencia a todo lo anterior, el artículo 6.4.3.2 debería incluir una regla expresa de imputación: la recuperación del código corto A2P solo procede por conducta propia, directa, comprobada y atribuible a su asignatario, y no por el uso indebido que hagan terceros ni por el incumplimiento de obligaciones que la resolución asigna al PRSTM, al validador, al asignatario del SENDER ID, al originador o a cualquier otro agente.

SINCH

Señala que la suspensión provisional del tráfico es la herramienta más efectiva a corto plazo, ya que evita que los actores maliciosos sigan operando durante el tiempo que toman los procesos administrativos tradicionales. Sin embargo, para garantizar la seguridad jurídica de la operación, es indispensable establecer políticas claras que definan con precisión qué casos ameritan esta suspensión. Asimismo, resulta prioritario diseñar un procedimiento ágil de reactivación del tráfico para mitigar el impacto en caso de que la suspensión se ejecute de manera errónea o injustificada.

Respuesta CRC:

La CRC observa que los comentarios presentados frente al diseño del Código Corto A2P se concentran principalmente en la naturaleza y función de este recurso dentro del nuevo ecosistema de mensajería A2P, la regla de unicidad por agente, los eventuales impactos operativos de dicha regla, la mensajería bidireccional, el régimen de transición, las obligaciones de debida diligencia, los requisitos de asignación,

la relación con la numeración NDC 940 y las adecuaciones técnicas requeridas para la implementación del esquema.

De manera general, los comentarios de **BLIPBLIP**, **NEXVIA**, **INALAMBRIA** y **SAEM** presentan una tendencia crítica frente a la regla de un único código corto A2P por agente, al considerar que dicha medida podría afectar la operación actual de integradores tecnológicos y PCA que utilizan múltiples códigos cortos para diferenciar servicios, clientes, contenidos o flujos de tráfico. Por su parte, **CLARO** formuló un comentario específico relacionado con los efectos del proceso de debida diligencia o KYC sobre la celebración de contratos entre el titular del SENDER ID y el PCA.

A continuación, la CRC se pronuncia sobre cada uno de los aspectos comentados.

2.2.1 Naturaleza y función del código corto A2P frente al SENDER ID

NEXVIA manifestó que el proyecto modificaría la naturaleza del código corto A2P, al pasar de ser un recurso orientado al posicionamiento e identificación de un tipo de servicio frente al usuario, a operar como una suerte de matrícula técnica del agente asignatario. Según su comentario, bajo la arquitectura propuesta, el usuario ya no percibiría el código corto, sino el SENDER ID alfanumérico, por lo que el código corto quedaría desprovisto de la función que históricamente le habría correspondido dentro del régimen de recursos de identificación.

Adicionalmente, **NEXVIA** sostuvo que la finalidad de identificación inequívoca del remitente podría satisfacerse mediante otros recursos preexistentes, como la numeración NDC 940, sin necesidad de ajustar la función del código corto ni de crear un recurso alfanumérico complementario.

La tendencia de este comentario es disidente frente al diseño propuesto, aunque no desconoce la necesidad de fortalecer la trazabilidad del tráfico A2P ni la identificación de los agentes que participan en la cadena de envío de mensajes.

Al respecto, es necesario mencionar que el documento soporte identificó que el tráfico SMS A2P presenta desafíos particulares de trazabilidad, verificación de remitentes y asignación de responsabilidades dentro de la cadena de valor. En particular, se reconoció que el ecosistema actual involucra diferentes agentes - integradores tecnológicos, PRST y generadores de contenido—, lo cual hace necesario establecer mecanismos que permitan identificar de manera clara tanto al agente que provee la infraestructura de conexión como al responsable del contenido cursado.

En esa línea, el proyecto de resolución propone diferenciar funcionalmente el código corto A2P y el SENDER ID. El primero identifica al agente que cuenta con la infraestructura y relación de acceso necesaria para cursar tráfico A2P a través de las redes de los PRST, mientras que el segundo identifica al responsable del contenido que se presenta frente al usuario. Esta separación busca corregir una dificultad advertida en el diagnóstico: la imposibilidad de atribuir de manera clara responsabilidades

cuando múltiples originadores o responsables de contenido cursan tráfico mediante un mismo recurso de identificación.

Así las cosas, la CRC no comparte la afirmación según la cual el proyecto desnaturaliza el código corto A2P. La medida no elimina su condición de recurso de identificación administrado por la Comisión, ni desconoce su relevancia dentro del ecosistema de mensajería. Por el contrario, precisa su función dentro de un modelo en el cual la identificación técnica del agente que cursa el tráfico y la identificación visible del remitente responsable del contenido se realizan mediante recursos diferenciados y complementarios.

Esta distinción resulta necesaria para evitar que un mismo recurso cumpla simultáneamente funciones de infraestructura, canal comercial, identificación visible del remitente y atribución de responsabilidad sobre el contenido. Bajo el esquema propuesto, el código corto A2P conserva una función regulatoria esencial: identificar al agente que cuenta con conexión directa o infraestructura de integración para cursar tráfico A2P y sobre quien recaen obligaciones asociadas al uso eficiente, trazabilidad y control del recurso.

En ese orden de ideas, la CRC no acepta la solicitud de modificar la naturaleza del código corto A2P en los términos propuestos y se mantiene el diseño regulatorio según el cual el código corto A2P y el SENDER ID cumplen funciones diferenciadas y complementarias dentro del ecosistema A2P: el primero identifica al agente que cursa técnicamente el tráfico, y el segundo identifica al responsable del contenido frente al usuario.

2.2.2 Regla de un único código corto A2P por agente

BLIPBLIP, **NEXVIA**, **INALAMBRIA** y **SAEM** cuestionaron la regla según la cual cada agente tendría derecho a la asignación de un único código corto A2P. En el mismo sentido, **ALDEAMO** solicitó eliminar el artículo 6.4.1.4, por considerar que las empresas deberían poder contar con múltiples códigos cortos cuando acrediten el cumplimiento de los requisitos aplicables, incluidos los de orden técnico y los asociados al conocimiento del cliente. De manera coincidente, señalaron que dicha regla desconocería la naturaleza del recurso y el principio de uso eficiente de los recursos escasos, en tanto los códigos cortos habrían sido utilizados históricamente para diferenciar tipos de servicio, modalidades de contenido, tarifas, clientes o unidades de negocio.

Estos agentes indicaron que la unicidad del código corto podría generar: i) un punto único de falla para toda la operación del integrador o PCA; ii) dificultades para la mensajería interactiva de doble vía; iii) afectaciones a modelos en los que actualmente un mismo agente cursa tráfico de múltiples clientes o marcas; iv) migraciones masivas de códigos existentes; y v) mayores cargas operativas para integradores y PRST.

La tendencia de los comentarios es coincidente en solicitar la eliminación o flexibilización de la regla de unicidad.

Frente a este punto, es preciso mencionar que el proyecto de resolución establece que cada solicitante tendrá derecho a la asignación de un único código corto A2P, el cual lo identificará de manera inequívoca dentro del ecosistema de mensajería A2P. Esta regla se articula con la creación del SENDER ID y con el régimen de plantillas, de manera que la diferenciación de los responsables del contenido, de las marcas, de las campañas o de las finalidades de los mensajes no recaiga en la multiplicación de códigos cortos, sino en los recursos y mecanismos específicos previstos para tal efecto.

La CRC considera que la regla de unicidad es consistente con el objetivo de ordenar el uso del recurso, reducir la dispersión de códigos asignados, facilitar la supervisión, evitar esquemas de uso no suficientemente trazables y separar claramente las responsabilidades entre quien provee la infraestructura de conexión y quien es responsable del contenido enviado.

Desde el punto de vista operativo, además, la Comisión observa que actualmente mediante un único código corto se cursan comunicaciones de múltiples empresas o clientes, sin que ello haya impedido el funcionamiento del tráfico A2P ni, en particular, la operación de comunicaciones de doble vía. Por tanto, resulta contraria a la realidad la afirmación según la cual un escenario de un único código corto por integrador haría inviable la prestación del servicio o impediría el adecuado enrutamiento de comunicaciones MO/MT, especialmente cuando el propio ecosistema ya opera con modelos en los que un recurso soporta tráfico de múltiples originadores.

Bajo el diseño propuesto, los agentes deberán implementar las medidas técnicas, operativas y de gestión necesarias para cumplir las obligaciones regulatorias asociadas al uso del código corto A2P, del SENDER ID y de las plantillas de contenido. La organización interna del tráfico, la identificación de clientes, la separación de campañas, el enrutamiento de respuestas o la asignación de flujos operativos son aspectos que deben resolverse mediante las capacidades técnicas y de gestión del asignatario, sin que ello justifique la asignación de múltiples códigos cortos como regla general.

La diferenciación frente al usuario se realizará mediante el SENDER ID, mientras que la diferenciación del contenido y finalidad del mensaje se soportará en el régimen de plantillas y en los mecanismos de trazabilidad asociados. En consecuencia, la multiplicación de códigos cortos no resulta necesaria para alcanzar los objetivos de identificación y prevención del fraude perseguidos por el proyecto.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de eliminar o flexibilizar la regla de un único código corto A2P por agente y en consecuencia se mantiene la regla propuesta, en la medida en que contribuye al uso ordenado del recurso, facilita la trazabilidad del tráfico A2P y evita que el código corto continúe siendo utilizado como mecanismo de diferenciación de múltiples clientes o campañas, función que será asumida por el SENDER ID y el régimen de plantillas.

2.2.3 Punto único de falla y continuidad del servicio

BLIPBLIP, **NEXVIA, SINCH** e **INALAMBRIA** sostuvieron que la regla de un único código corto A2P convertiría dicho recurso en un punto único de falla. Según estos comentarios, la recuperación,

suspensión o desconexión de un código corto podría afectar de manera masiva todos los SENDER ID vinculados y, por esa vía, interrumpir comunicaciones legítimas, incluso aquellas asociadas a autenticación, alertas de seguridad o transacciones.

NEXVIA indicó además que, bajo el régimen vigente, la pluralidad de códigos cortos opera como una forma de redundancia natural que protege la continuidad del servicio, mientras que el proyecto concentraría todo el riesgo operativo en un solo recurso.

La tendencia de estos comentarios es coincidente en advertir riesgos de continuidad derivados de la unicidad del código corto.

Al respecto, la CRC no comparte la conclusión según la cual la regla de unicidad convierte por sí misma al código corto A2P en un punto único de falla sistémico. La continuidad del servicio no depende exclusivamente del número de códigos cortos asignados, sino de la existencia de procesos técnicos, operativos, contractuales y regulatorios que permitan administrar adecuadamente el tráfico, prevenir incumplimientos y reaccionar frente a incidentes.

La recuperación o suspensión de un código corto A2P no opera de manera automática ni arbitraria, sino conforme a las causales, procedimientos y garantías previstas en la regulación. Los asignatarios de códigos cortos tienen el deber de administrar adecuadamente el recurso, implementar controles sobre el tráfico cursado, cumplir las obligaciones de debida diligencia y garantizar que los SENDER ID y plantillas asociadas se ajusten a las condiciones regulatorias aplicables.

En este contexto, el riesgo de afectación operativa no deriva de la regla de unicidad, sino de eventuales incumplimientos por parte del asignatario o de los agentes que participan en la cadena de valor. La regulación propuesta busca precisamente reducir los escenarios de dilución de responsabilidades y establecer una arquitectura en la que cada recurso y cada agente tengan una función claramente definida.

Adicionalmente, la existencia de múltiples códigos cortos no garantiza, por sí misma, mayor continuidad ni menor riesgo de fraude. Por el contrario, la dispersión de recursos puede dificultar la supervisión, fragmentar la trazabilidad y facilitar que conductas irregulares migren de un código a otro sin una identificación clara del responsable.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de modificar la regla de unicidad con fundamento en el argumento de punto único de falla, y en consecuencia se mantiene la propuesta, sin perjuicio de las obligaciones de los asignatarios de implementar medidas internas de continuidad, gestión de riesgos, monitoreo y control del tráfico cursado mediante el código corto A2P asignado.

2.2.4 Mensajería interactiva de doble vía —MO/MT

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

BLIPBLIP, **NEXVIA** e **INALAMBRIA** señalaron que la regla de un único código corto por agente podría afectar la mensajería interactiva de doble vía —MO/MT. A su juicio, cuando un mismo código es utilizado para múltiples clientes, unidades de negocio o industrias, se dificultaría la identificación del destinatario de la respuesta del usuario y el enrutamiento adecuado del tráfico entrante.

La tendencia de los comentarios es coincidente en advertir que la unicidad podría generar dificultades para la operación de servicios bidireccionales.

La CRC no acoge esta observación. Como se indicó en el punto anterior, actualmente el ecosistema A2P ya opera con esquemas en los que un mismo código corto soporta comunicaciones de múltiples clientes o empresas, sin que ello haya impedido, en términos generales, el funcionamiento de comunicaciones bidireccionales. Por tanto, no resulta claro que el escenario de un único código corto por integrador genere, por sí mismo, una imposibilidad técnica para la gestión de tráfico MO/MT.

El enrutamiento de respuestas, la identificación del cliente asociado, la separación de flujos y la gestión de interacciones bidireccionales pueden realizarse mediante herramientas técnicas propias del integrador, sistemas de gestión de campañas, parámetros internos, metadatos, reglas de negocio, plantillas, SENDER ID y demás mecanismos de trazabilidad definidos en la arquitectura regulatoria propuesta. La asignación de múltiples códigos cortos no es la única ni necesariamente la forma más eficiente de resolver la operación de tráfico bidireccional.

En ese sentido, corresponde a los asignatarios de códigos cortos A2P implementar las medidas técnicas y operativas necesarias para permitir el cumplimiento de las obligaciones regulatorias, incluyendo aquellas asociadas a la correcta identificación, clasificación, enrutamiento y trazabilidad del tráfico MO/MT que cursen mediante su recurso asignado.

Por lo anterior, la CRC no acepta la solicitud de exceptuar la mensajería MO/MT de la regla de unicidad ni de permitir códigos cortos adicionales con fundamento en dicha operación. Se mantiene la regla de un único código corto A2P por agente, sin perjuicio de que los asignatarios deban adecuar sus sistemas para garantizar el correcto enrutamiento, identificación y trazabilidad de las comunicaciones bidireccionales.

2.2.5 Régimen de transición, migración de códigos existentes y devolución de recursos

SAEM indicó que el régimen de transición propuesto obligaría a los integradores tecnológicos que actualmente cuentan con múltiples códigos cortos a consolidarlos en uno solo dentro del plazo establecido, lo que implicaría escoger el recurso que conservarán y migrar el resto. A su juicio, esta migración conlleva pérdida de códigos que clientes y usuarios ya reconocen, reconfiguración de enrutamientos, migración de consentimientos y costos comerciales y operativos. **NEXVIA** manifestó que el numeral correspondiente al régimen de transición obligaría a devolver códigos en operación, con

millones de usuarios activos, imponiendo migraciones masivas cuyo costo y riesgo no estarían suficientemente cuantificados.

La tendencia de los comentarios es coincidente en solicitar la modificación del régimen de transición, la ampliación de plazos o la conservación de múltiples códigos existentes.

Al respecto, es preciso mencionar que la CRC no acoge la solicitud de modificar el régimen de transición en los términos planteados teniendo en cuenta que la transición prevista en el proyecto responde a la necesidad de ordenar el uso de los códigos cortos A2P bajo el nuevo modelo regulatorio, en el que el código corto identifica al agente que cursa técnicamente el tráfico y el SENDER ID identifica al responsable del contenido frente al usuario.

Mantener indefinidamente múltiples códigos cortos en cabeza de un mismo agente perpetuaría la dispersión que la medida busca corregir y dificultaría la implementación del nuevo esquema de trazabilidad centralizada. La existencia de códigos históricos, reconocidos por determinados clientes o utilizados en configuraciones operativas previas, no justifica conservar un esquema que el proyecto pretende racionalizar en beneficio de la identificación, supervisión y control del tráfico A2P.

El régimen de transición permite que los asignatarios adelanten las adecuaciones necesarias, realicen las migraciones correspondientes y ajusten sus relaciones contractuales y técnicas. Las cargas asociadas a dicha migración son consecuencia de la adopción de un nuevo modelo regulatorio orientado a fortalecer la prevención del fraude y la administración eficiente de recursos de identificación.

Adicionalmente, la CRC considera que los agentes que participan profesionalmente en el mercado de mensajería A2P cuentan con capacidades técnicas y operativas para adelantar procesos de migración, reconfiguración y actualización de recursos, como parte ordinaria de la gestión de sus plataformas y servicios.

Así las cosas, la CRC no acepta la solicitud de modificar el régimen de transición, eliminar la obligación de consolidación o permitir la conservación de múltiples códigos cortos por agente. Se mantiene el régimen propuesto para la migración y devolución de los recursos que no se ajusten al nuevo esquema de unicidad del código corto A2P.

2.2.6 Requisito de KYC y prohibición de contratar cuando no se apruebe la debida diligencia

CLARO propuso adicionar una regla según la cual, en caso de que no se apruebe el procedimiento de debida diligencia o KYC, no pueda celebrarse contrato entre el dueño del SENDER ID y el PCA. La posición es individual, aunque se relaciona con el objetivo general de reforzar la trazabilidad y evitar que agentes no verificados puedan acceder al ecosistema A2P.

Frente al particular es preciso mencionar que el proyecto de resolución ya incorpora obligaciones de debida diligencia, verificación y control asociadas a los agentes que intervienen en el envío de tráfico A2P. En ese sentido, la aprobación de los procesos de KYC y la acreditación de los requisitos correspondientes constituyen condiciones necesarias para la asignación, uso y operación de los recursos de identificación dentro del esquema propuesto.

En ese sentido, la CRC considera que no es necesario incorporar una regla adicional que prohíba expresamente la celebración de contratos en los términos solicitados por **CLARO**, pues el efecto práctico de no superar los procesos de verificación ya se deriva de las reglas de asignación, validación y uso de los recursos. Si un agente no cumple los requisitos de debida diligencia, no podrá acceder válidamente a los recursos o condiciones necesarias para cursar tráfico A2P dentro del esquema regulado.

Adicionalmente, la celebración de relaciones contractuales entre particulares no debe ser regulada de manera abstracta más allá de lo necesario para asegurar el cumplimiento de las condiciones regulatorias asociadas al uso de recursos de identificación. Lo relevante desde la perspectiva de la CRC es que el tráfico A2P solo sea cursado cuando se cumplan las condiciones de identificación, validación, trazabilidad y debida diligencia previstas en la resolución.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de adicionar una disposición específica que prohíba la celebración de contratos cuando no se apruebe el KYC. Se mantiene el diseño propuesto, en el entendido de que el incumplimiento de los procesos de debida diligencia impide el uso válido de los recursos y el curso de tráfico A2P dentro del esquema regulatorio.

2.2.7 Duplicidad de KYC entre integrador, validador y registros existentes

SAEM manifestó que el proyecto exige al integrador tecnológico, en su calidad de asignatario de código corto A2P, adelantar procesos de KYC respecto de cada PCA, incluyendo identificación del agente y del beneficiario final, verificación de objeto social, perfil de riesgo, formalización contractual y conservación de información. A su juicio, estas exigencias podrían duplicar información que ya reposa en registros como el RPCAI, el RUES o el RUT, y generar una superposición entre el KYC realizado por el integrador y la verificación del validador centralizado.

Al respecto, la CRC no comparte la conclusión de que la existencia de información en registros públicos o administrativos sustituya las obligaciones de debida diligencia continua que deben cumplir los asignatarios de códigos cortos A2P. Los registros como el RPCAI, el RUES o el RUT permiten verificar información formal o básica sobre existencia, identificación o registro de los agentes, pero no agotan la evaluación de riesgo ni la trazabilidad requerida para prevenir el uso indebido de recursos de identificación.

La prevención del fraude exige verificar no solo la existencia jurídica del agente, sino también la finalidad del tráfico que cursa, su relación contractual, el responsable efectivo del contenido, las condiciones operativas de envío, el perfil de riesgo y la persistencia de las condiciones verificadas durante la relación

comercial. Por ello, la debida diligencia no puede entenderse como un trámite estático o meramente documental, sino como un proceso continuo de conocimiento, seguimiento y actualización.

Así mismo, la eventual verificación realizada por el validador centralizado no exime al integrador tecnológico o asignatario del código corto de sus propias responsabilidades frente al tráfico que cursa mediante el recurso asignado. Cada actor debe asumir las obligaciones correspondientes al rol que desempeña dentro de la cadena de valor, sin que la existencia de controles en otro eslabón elimine sus deberes propios de prevención, monitoreo y trazabilidad.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de reducir o eliminar las obligaciones de KYC por considerar que duplican información disponible en otros registros o en el proceso de validación centralizada, y en consecuencia se mantienen las obligaciones de debida diligencia previstas en el proyecto, por ser necesarias para la prevención del fraude, la trazabilidad del tráfico y la asignación clara de responsabilidades.

2.2.8 Requisitos de asignación del código corto A2P y roles PCA/IT

En los comentarios se planteó la necesidad de precisar los requisitos de asignación del código corto A2P, particularmente en lo relativo a la calidad en la que actúa el solicitante —PCA, integrador tecnológico o ambas—, la descripción del servicio o función que desempeñará como asignatario, y la identificación de si cuenta con conexión directa a PRST o si cursa tráfico a través de terceros.

Esta solicitud busca evitar ambigüedades sobre el rol del agente, la infraestructura utilizada, la relación de acceso y las responsabilidades que le corresponden dentro de la cadena de valor. La tendencia del comentario es propositiva y orientada a mejorar la claridad regulatoria.

En relación con este punto, es necesario mencionar que el documento soporte reconoce que el ecosistema de mensajería A2P involucra diferentes configuraciones operativas, en las que pueden participar PCA con conexión directa, PCA sin conexión directa, integradores tecnológicos y agentes que combinan funciones. Esta diversidad puede generar dificultades para asignar responsabilidades frente al uso de recursos de identificación y frente al curso de tráfico A2P.

En ese sentido, la CRC considera pertinente precisar los requisitos de asignación del código corto A2P para que el solicitante indique expresamente la calidad en la que actúa, describa su función dentro de la cadena de valor y aporte información suficiente sobre su infraestructura o relación de acceso. Esta precisión permite reforzar la trazabilidad, identificar adecuadamente al responsable de la infraestructura de conexión y reducir zonas grises frente a la responsabilidad de PCA e integradores tecnológicos.

No obstante, dicha precisión debe mantenerse alineada con el diseño del proyecto: el código corto A2P corresponde al agente que cuenta con conexión directa o infraestructura de integración para cursar tráfico A2P, mientras que la identificación del responsable del contenido se realiza mediante el SENDER ID.

Teniendo en cuenta lo anterior, la CRC acepta el comentario orientado a precisar los requisitos de asignación del código corto A2P y los roles de los agentes que pueden solicitarlo. En consecuencia, se ajusta la redacción correspondiente para exigir que el solicitante identifique la calidad en la que actúa y describa la función que desempeñará como asignatario del recurso.

Por ello, se ajustan los numerales 6.4.2.1.1 y 6.4.2.1.3 del artículo 6.4.2.1 correspondiente a los requisitos de asignación del código corto A2P en el sentido de aclarar que, para solicitar la asignación de un código corto A2P, el solicitante deberá acreditar su inscripción previa en el RPCAI e indicar expresamente la calidad en la que actúa, esto es, como integrador tecnológico, como PCA con conexión directa al PRST, o como PRST en los casos en que actúe en calidad de integrador tecnológico para soportar sus propios servicios.

Además, se precisará en esos artículos que, el solicitante deberá describir detalladamente el servicio o función que desempeñará como asignatario del código corto A2P, incluyendo la infraestructura técnica de conexión con el o los PRST, la identificación de los PRST con los cuales mantiene o mantendrá relación de acceso, y los mecanismos de trazabilidad del tráfico A2P cursado mediante el recurso solicitado.

Por otra parte, **ALDEAMO** solicitó revisar el trámite de asignación de códigos cortos con el propósito de agilizarlo y dotarlo de mayor claridad y transparencia, mediante la definición de estándares que precisen las razones por las cuales una solicitud de asignación puede ser negada, así como las evidencias y pruebas que se consideran suficientes para evitar la recuperación del recurso. La tendencia de este comentario es propositiva y se orienta a la simplificación del trámite.

Al respecto, la Comisión precisa que el régimen de administración de los recursos de identificación contenido en el Título VI de la Resolución CRC 5050 de 2016 define de manera reglada los requisitos de asignación, las causales de negación, las causales de recuperación y el procedimiento aplicable, de modo que la actuación del Administrador de los Recursos de Identificación no es discrecional, sino que se sujeta a supuestos previamente definidos y a la motivación del acto correspondiente. Adicionalmente, los ajustes acogidos en el presente aparte refuerzan precisamente esa claridad, al exigir que el solicitante identifique la calidad en la que actúa, describa la función que desempeñará como asignatario y acredite su inscripción previa en el RPCAI, lo que reduce las zonas grises que hoy dificultan la evaluación de las solicitudes.

En cuanto a la solicitud de delimitar anticipadamente las evidencias y pruebas suficientes para enervar una actuación de recuperación, la Comisión no la acoge. La valoración probatoria corresponde a cada actuación administrativa concreta y debe realizarse de manera conjunta y conforme a las reglas de la sana crítica, sin que resulte procedente que la regulación predetermine el mérito de medios probatorios específicos, pues ello restringiría el derecho de defensa del propio asignatario y limitaría la capacidad de la administración para valorar las circunstancias particulares de cada caso.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de incorporar en la resolución estándares adicionales sobre las causales de negación de solicitudes o sobre la suficiencia probatoria en las actuaciones de recuperación, y en consecuencia se mantiene el diseño propuesto, sin perjuicio de las mejoras operativas y de trazabilidad que la Comisión continúe implementando en los sistemas de información asociados a la administración de los recursos de identificación.

2.2.9 Alternativa de utilizar NDC 940 en lugar de código corto A2P y SENDER ID

NEXVIA sostuvo que la identificación inequívoca de agentes o remitentes en el ecosistema ya podría realizarse mediante la numeración NDC 940, recurso que, en su criterio, podría incorporar requisitos de verificación como titularidad del identificador, soporte documental y plantillas, sin necesidad de crear un recurso alfanumérico paralelo ni de modificar el régimen de códigos cortos. Esta posición es individual, aunque se relaciona con la crítica general al diseño propuesto del SENDER ID y del código corto A2P.

Al respecto es necesario mencionar que la CRC no acoge esta propuesta. El proyecto regulatorio define un esquema integral de validación centralizada para el tráfico A2P basado en la interacción de tres elementos: SENDER ID, código corto A2P y plantilla de contenido. Este diseño busca que toda comunicación A2P sea identificable, validada y trazable antes de ser cursada hacia el usuario final.

Permitir el envío de mensajería A2P mediante numeración de 10 dígitos asociada al NDC 940 implicaría desconocer la arquitectura regulatoria propuesta y abrir una vía paralela al sistema de validación centralizado. Esto debilitaría la trazabilidad del tráfico, dificultaría la aplicación uniforme de las reglas de validación y podría generar un canal alternativo para el envío de comunicaciones fraudulentas o no verificadas.

La utilización de numeración E.164 de 10 dígitos para cursar SMS A2P generaría, además, un riesgo regulatorio relevante: permitiría que comunicaciones que deberían sujetarse al esquema de SENDER ID, código corto A2P y plantilla validada se envíen por una vía no sometida a los mismos controles. Lo anterior afectaría la eficacia de la medida, pues los agentes maliciosos podrían migrar hacia ese canal para evadir el sistema de validación centralizado.

En consecuencia, la CRC considera que el NDC 940 no debe operar como una alternativa al régimen propuesto para el envío de mensajería A2P. Por el contrario, teniendo en cuenta que todas las comunicaciones A2P deberán enviarse haciendo uso del sistema de validación centralizado previsto en la resolución, la atribución del NDC 940 para el envío de este tipo de comunicaciones no podrá seguir siendo utilizada para el envío de mensajes en el nuevo ecosistema A2P.

Teniendo en cuenta lo anterior, la CRC no acepta la propuesta de utilizar el NDC 940 como alternativa al código corto A2P y al SENDER ID para el envío de mensajería A2P. Así, no puede perderse de vista que, en línea con el contenido del numeral 6.13.4.7.3., los operadores deben abstenerse de enrutar, entregar o permitir el curso de tráfico A2P que sea presentado mediante numeración E.164, cuando

dicho tráfico no cuente con código corto A2P, SENDER ID debidamente asignado y plantilla de contenido aprobada y vigente en el sistema del validador centralizado.

En otras palabras, la Comisión insiste en que, de conformidad con el nuevo ecosistema A2P, en ningún caso podrá cursarse tráfico A2P mediante numeración E.164, sin código corto A2P, SENDER ID debidamente asignado y plantilla de contenido aprobada y vigente en el sistema del validador centralizado.

Por lo tanto, en virtud de las facultades contenidas en el numeral 6.1.1.4.2 del artículo 6.1.1.4 de la Resolución CRC 5050 de 2016, la atribución del NDC 940 para este uso se debe entender eliminada, en coherencia con el nuevo esquema de validación centralizada.

Así las cosas, mediante circular se modificará la atribución del NDC 940 para fijarla en estado de reserva, y en consecuencia las comunicaciones de mensajería A2P deberán cursarse exclusivamente mediante el esquema de validación previsto en la presente resolución, que comprende el uso de código corto A2P, SENDER ID y plantilla de contenido validada por lo que no se permitirá el uso de numeración E.164 de diez dígitos, incluyendo numeración asociada al NDC 940, para el envío de mensajes A2P sujetos al presente régimen.

Adicionalmente, la CRC considera pertinente precisar también en la resolución que el rechazo de la alternativa basada en la utilización del NDC 940 o de numeración E.164 como mecanismo de identificación del tráfico A2P implica que dicho tráfico debe cursarse dentro de la arquitectura regulatoria definida para el ecosistema A2P. En efecto, el proyecto establece que el tráfico A2P es aquel cursado mediante la utilización de un código corto A2P y un SENDER ID debidamente asignados por la CRC, respaldado por una plantilla de contenido aprobada por el validador centralizado. A su vez, el tráfico P2P se define como la comunicación directa entre usuarios finales mediante numeración E.164 no geográfica de redes.

Así, aunque de la lectura sistemática de las definiciones se desprende que el tráfico A2P no debe cursarse mediante numeración E.164 como si fuera tráfico P2P, la CRC considera conveniente incorporar una prohibición expresa para evitar interpretaciones divergentes o vías paralelas de elusión del sistema de validación centralizado. Esta precisión resulta además coherente con la decisión de no acoger la propuesta de utilizar el NDC 940 como alternativa al código corto A2P y al SENDER ID, pues permitir el envío de mensajería A2P mediante numeración de 10 dígitos implicaría desconocer la arquitectura regulatoria propuesta y abrir una vía paralela al sistema de validación centralizado.

En consecuencia, la CRC incorpora una regla expresa según la cual el tráfico A2P no podrá cursarse mediante numeración E.164, incluida la asociada al NDC 940, sin código corto A2P, SENDER ID debidamente asignado y plantilla de contenido aprobada y vigente en el sistema del validador centralizado. Para tal efecto, se realizan ajustes en tres partes del proyecto de resolución: i) en la definición de tráfico A2P, para precisar expresamente que esta modalidad no puede cursarse mediante numeración E.164 por fuera del régimen A2P; ii) en el artículo 6.13.4.7.2, relativo a las obligaciones

especiales de los PRST frente a la verificación previa al enrutamiento de mensajes A2P, para incluir la obligación de abstenerse de enrutar, entregar o permitir el curso de tráfico A2P presentado mediante numeración E.164 cuando no cuente con los elementos de validación exigidos; y iii) en el artículo 2.1.10.7.2.1.1, relativo al monitoreo y control del tráfico P2P, para precisar que cuando los sistemas de monitoreo identifiquen patrones asociados al uso de numeración E.164 para cursar tráfico A2P simulado como P2P, deberán aplicarse las medidas de monitoreo, control y reporte previstas para la prevención del fraude en tráfico P2P, sin perjuicio de las obligaciones aplicables al régimen A2P.

Esta regla no modifica la definición de tráfico P2P ni impide el uso legítimo de numeración E.164 para comunicaciones directas entre usuarios finales. Su finalidad es evitar que comunicaciones originadas por aplicaciones, plataformas o sistemas automatizados sean presentadas o cursadas como tráfico P2P por fuera del régimen de validación A2P. En esa medida, la precisión normativa refuerza la separación funcional entre el tráfico A2P —sujeto a código corto A2P, SENDER ID y plantilla aprobada— y el tráfico P2P —asociado a la comunicación directa entre personas mediante numeración E.164—, y cierra una posible vía de elusión derivada del uso de numeración E.164 como sustituto del esquema de validación centralizado.

2.2.10 Adecuaciones técnicas, APIs, redimensionamiento y capacidad

Algunos comentarios señalaron que la implementación del nuevo régimen de códigos cortos A2P, SENDER ID y validación centralizada podría requerir adecuaciones técnicas, integración de APIs, redimensionamiento de capacidades, ajustes en plataformas y procesos de interoperabilidad entre agentes. En particular, se advirtió que concentrar el tráfico en un único código corto por agente exigiría desarrollos y adecuaciones por parte de PRST, integradores tecnológicos y asignatarios.

Al respecto, la CRC reconoce que la implementación de las medidas previstas en el proyecto exigirá ajustes técnicos y operativos por parte de los agentes que participan en el ecosistema de mensajería A2P. No obstante, no se acoge la solicitud de modificar el diseño regulatorio por esta razón.

Los agentes que cursan tráfico A2P, en particular quienes son asignatarios de códigos cortos o responsables de la infraestructura de integración, desarrollan una actividad que exige capacidades técnicas para gestionar volúmenes de tráfico, relacionamiento con PRST, enrutamiento, autenticación de sesiones, administración de clientes y trazabilidad de campañas. En ese sentido, la necesidad de realizar adecuaciones técnicas no constituye, por sí misma, una razón para eliminar o modificar las obligaciones regulatorias orientadas a prevenir el fraude y fortalecer la trazabilidad.

Adicionalmente, el hecho de que la implementación requiera APIs, mecanismos de interoperabilidad, pruebas técnicas o redimensionamiento de capacidad no implica que tales especificaciones deban ser incorporadas de manera detallada en la resolución. La regulación debe establecer las obligaciones, principios y resultados esperados, mientras que los aspectos técnicos específicos podrán desarrollarse mediante los espacios de coordinación previstos, incluyendo el CTLFSM, las pruebas de interoperabilidad o los lineamientos operativos que se definan para la implementación.

Por tanto, la CRC considera que las adecuaciones técnicas hacen parte de las cargas razonables derivadas de la participación en un mercado que utiliza recursos de identificación administrados por el Estado y que, por su impacto en la seguridad de los usuarios, requiere mayores estándares de control.

En ese orden de ideas, la CRC no acepta la solicitud de modificar la propuesta regulatoria con fundamento en las adecuaciones técnicas, APIs, redimensionamiento o capacidad requeridas para la implementación y, en consecuencia, se mantiene el diseño propuesto, sin perjuicio de que los detalles técnicos de interoperabilidad y operación sean desarrollados en los espacios técnicos correspondientes, esto es, el CTLFSM.

2.2.11 Causales de recuperación del código corto A2P y garantías del debido proceso

HABLAME cuestionó de manera individualizada las causales de recuperación del código corto A2P contenidas en el artículo 6.4.3.2, así como el criterio de uso eficiente del numeral 6.4.3.1.7 y los parágrafos 1 y 2 del citado artículo. En su criterio, la pérdida del recurso equivale al cierre de la operación del integrador tecnológico, por lo que solo podría proceder por una conducta propia, directa, comprobada y atribuible al titular del código, conforme al artículo 29 de la Constitución Política. Sobre esa base, solicitó eliminar o reformular las causales de los numerales 6.4.3.2.1, 6.4.3.2.2, 6.4.3.2.5, 6.4.3.2.6, 6.4.3.2.9 y 6.4.3.2.10 respecto del asignatario del código corto A2P, e incorporar en el artículo 6.4.3.2 una regla expresa de imputación.

En la misma línea, **NEXVIA** solicitó reformular el numeral 6.4.3.2.5 mediante una redacción que condicione la causal al envío reiterado y deliberado, a la verificación previa de que el asignatario no adoptó las medidas de control a su alcance, a un requerimiento previo del Administrador de los Recursos de Identificación y a un plazo de ajuste no inferior a diez (10) días hábiles; cuestionó igualmente el numeral 6.4.3.2.7, por considerar que presupone que todo asignatario debe sostener una relación de acceso directa con el PRSTM, cuya celebración no depende exclusivamente del solicitante; y solicitó modificar los parágrafos 1 y 2 del artículo 6.4.3.2 por el efecto en cascada sobre los SENDER ID vinculados y por la duración de la suspensión durante el trámite.

La tendencia de estos comentarios es coincidente en solicitar la eliminación, condicionamiento o graduación de las causales de recuperación del código corto A2P, sin cuestionar la existencia misma de un régimen de recuperación del recurso.

Frente a este punto, la Comisión precisa, como consideración general, que la recuperación de un recurso de identificación no constituye una sanción, sino la consecuencia administrativa del incumplimiento de las condiciones bajo las cuales el recurso fue asignado. Los recursos de identificación son bienes públicos escasos cuya administración y gestión corresponde a la CRC en ejercicio de las funciones que le atribuye la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, y su asignación no confiere a los asignatarios un derecho de propiedad, sino una habilitación de uso sujeta al cumplimiento de deberes de uso

eficiente, trazabilidad y control. Adicionalmente, la configuración de cualquiera de las causales del artículo 6.4.3.2 no opera de manera automática ni por la mera constatación objetiva de un hecho, pues su declaración exige el adelantamiento de una actuación administrativa con observancia plena de las garantías del debido proceso previstas en el artículo 29 de la Constitución Política, incluidas la motivación del acto, la posibilidad de contradicción y la procedencia de los recursos correspondientes.

Sentado lo anterior, y en relación con la causal del numeral 6.4.3.2.5, la Comisión no comparte la premisa según la cual la obligación de verificación previa al enrutamiento a cargo del PRSTM, prevista en el artículo 6.13.4.7.2, desplace o extinga los deberes propios del asignatario del código corto A2P. Se trata de obligaciones concurrentes y no excluyentes, que operan en momentos distintos de la cadena de valor: el asignatario del código corto A2P es quien controla el acceso al recurso, quien contrata con los originadores y quien decide qué tráfico ofrece a la red, mientras que el PRSTM interviene en el enrutamiento. Admitir que la existencia de un filtro en la red exonera a quien entrega el tráfico equivaldría a vaciar de contenido los deberes de diligencia, monitoreo y control que el propio régimen impone al asignatario y a trasladar íntegramente al PRSTM la gestión del riesgo de un recurso que no administra. En todo caso, la atribución de responsabilidad no es objetiva y se rige por las reglas del artículo 6.13.4.4, cuyo alcance se precisa en el capítulo denominado «Atribución de responsabilidad».

Respecto de la causal del numeral 6.4.3.2.6, la observación sobre la expresión «potencialmente» resulta fundada y fue acogida en los términos explicados en el capítulo denominado «Atribución de responsabilidad», por lo que no procede un pronunciamiento adicional en este capítulo.

En cuanto a la causal del numeral 6.4.3.2.7, la Comisión reitera que el código corto A2P identifica al agente que cuenta con conexión directa o con infraestructura de integración para cursar tráfico A2P a través de las redes de los PRSTM, de manera que la ausencia sobrevenida y prolongada de relación de acceso desnaturaliza la atribución del recurso y compromete el principio de uso eficiente. Ahora bien, la causal no se configura por la sola demora imputable a un tercero: su declaración exige, como se indicó, una actuación administrativa en la que se valoren las circunstancias del caso, incluida la conducta del PRSTM. Adicionalmente, el ordenamiento sectorial prevé mecanismos específicos para superar las dificultades de acceso invocadas por el agente, entre ellos la solución de controversias y la imposición de servidumbre de acceso, uso e interconexión, a los cuales puede acudirse sin que la existencia de la causal los sustituya.

Frente a las causales de los numerales 6.4.3.2.1 y 6.4.3.2.2, referidas al incumplimiento de las obligaciones generales y especiales del régimen, la Comisión advierte que la remisión al conjunto de obligaciones aplicables es una técnica normativa necesaria para evitar vacíos, y que su aplicación se encuentra acotada por la exigencia de una conducta atribuible al asignatario, valorada conforme a los estándares de diligencia precisados en el capítulo denominado «Atribución de responsabilidad». Por la misma razón, tampoco se acoge la solicitud de reformular el criterio de uso eficiente del numeral 6.4.3.1.7 ni las obligaciones del artículo 6.13.4.5.1 como obligaciones de medios, pues el deber de cursar únicamente tráfico respaldado por SENDER ID vigente y plantilla aprobada constituye el núcleo

funcional del esquema de validación, y su cumplimiento es verificable mediante la consulta de los registros del validador centralizado y del SIGRI, integración que el propio proyecto exige.

En relación con la causal del numeral 6.4.3.2.10, la Comisión precisa que su invocación respecto del asignatario del código corto A2P no supone imputarle infracciones cometidas por el originador del contenido, sino la valoración de su propia conducta cuando, conociendo o debiendo conocer la situación, persiste en cursar el tráfico correspondiente. La distinción entre responsable y encargado del tratamiento invocada por el agente opera en el ámbito del régimen de protección de datos personales y ante la autoridad competente para aplicarlo, sin que ello excluya los deberes sectoriales de diligencia asociados a la administración del recurso de identificación.

Sobre la causal del numeral 6.4.3.2.9, la Comisión reitera que las razones de interés general o de seguridad nacional no habilitan decisiones discrecionales ni exoneran de motivación. Como toda causal de recuperación, su declaración exige acto administrativo motivado, sustentado en una causa concreta y demostrada, y sujeto al principio de proporcionalidad, garantías que se derivan directamente del artículo 29 de la Constitución Política y del procedimiento administrativo aplicable, sin que resulte necesario reiterarlas en el texto de la resolución.

En cuanto al parágrafo 1 del artículo 6.4.3.2, la Comisión observa que la disposición no produce una interrupción inmediata de las comunicaciones de los SENDER ID vinculados, pues concede un término de treinta (30) días hábiles para que sus titulares se vinculen a otro asignatario de código corto A2P. Ese término, sumado a la ampliación del período de transición del nuevo ecosistema A2P y a la posibilidad de vincular un mismo SENDER ID a un nuevo asignatario sin necesidad de tramitar un recurso nuevo, ofrece un margen razonable de continuidad. Aceptar, en cambio, que la recuperación del código corto A2P no afecte a los SENDER ID vinculados implicaría mantener en operación un canal técnico respecto del cual se declaró un incumplimiento, con el consiguiente riesgo para los usuarios que la medida busca proteger. La comparación con el parágrafo 1 del artículo 6.1.1.8 tampoco resulta procedente, en la medida en que aquella disposición regula supuestos de recuperación de recursos asignados directamente a usuarios finales, situación que no se asimila a la vinculación contractual entre agentes del ecosistema A2P.

Finalmente, respecto del parágrafo 2 del mismo artículo, la Comisión precisa que la suspensión durante el trámite tiene naturaleza cautelar y preventiva, se adopta mediante acto motivado dentro de una actuación administrativa en curso, opera únicamente frente a las causales de los numerales 6.4.3.2.5 y 6.4.3.2.6 y constituye un término máximo y no un plazo de aplicación obligatoria. Su finalidad es evitar que la continuidad del tráfico cuestionado prolongue la exposición de los usuarios al fraude mientras se resuelve el fondo del asunto, lo que resulta consistente con la naturaleza preventiva del conjunto de medidas adoptadas.

Teniendo en cuenta lo anterior, la CRC no acepta las solicitudes de eliminar, condicionar o graduar las causales de recuperación del código corto A2P contenidas en el artículo 6.4.3.2, ni las de modificar el criterio de uso eficiente del numeral 6.4.3.1.7 o los parágrafos 1 y 2 del citado artículo, y en

consecuencia se mantiene el texto propuesto, sin perjuicio del ajuste al numeral 6.4.3.2.6 explicado en el capítulo denominado «Atribución de responsabilidad».

2.3 Validador centralizado: forma de selección, competencias y funciones

ALDEAMO

Expone las siguientes inquietudes frente al validador:

● Será una entidad seleccionada por los PRSTM y financiada por quienes soliciten códigos cortos y SENDER ID, bajo un modelo aún no definido con claridad.

● Los PRSTM también envían mensajes de texto, por lo que seleccionarían una entidad encargada de regular un mercado en el que participan, excluyendo a otros competidores de dicha decisión y generando un posible riesgo de competencia desleal.

● Le preocupa el tiempo requerido para la puesta en operación del validador, considerando las funciones de control de plantillas, revisión de KYC y asignación de códigos cortos y SENDER ID.

Por lo anterior, propone evitar la creación de una nueva entidad y distribuir sus funciones entre los actores existentes: la CRC asumiría los procesos de KYC y asignación de códigos cortos y SENDER ID, mientras los operadores móviles gestionarían las plantillas mediante procedimientos técnicos estandarizados que faciliten la coordinación y el control por parte de los PCA e integradores tecnológicos.

AMCHAM

Señala que el Proyecto propone la creación de un validador centralizado, operado por un único tercero privado, conforme a los artículos 6.13.1.1 a 6.13.1.6. Aunque reconoce que esta figura busca establecer un punto de control para mitigar el uso fraudulento de los servicios móviles, considera necesario revisar su diseño, pues podría convertirse en un punto de falla sistémico, una barrera de entrada y una fuente adicional de costos y latencia para los actores del ecosistema digital.

Desde una perspectiva técnica y regulatoria, considera más conveniente avanzar hacia un modelo basado en interoperabilidad, estándares abiertos y protocolos de seguridad verificables, que permita a proveedores locales y globales integrar sus sistemas de verificación, autenticación y prevención del fraude con el ecosistema colombiano, sin depender de un intermediario obligatorio y centralizado.

Añade que los modelos interoperables pueden facilitar la coordinación entre actores públicos y privados sin afectar la innovación, escalabilidad ni resiliencia técnica. En lugar de concentrar la validación en un

único operador, propone promover APIs de seguridad, estándares técnicos para el intercambio de información, mecanismos automatizados de reporte de fraude y criterios comunes de identificación de riesgos.

En particular, sugiere evaluar un estándar técnico para intercambiar información relacionada con procesos de conocimiento del cliente, reporte de incidentes, señales de fraude y autenticación de mensajes. Esto permitiría una respuesta más ágil y coordinada frente a amenazas cibernéticas, reduciría fricciones operativas y facilitaría la integración de proveedores globales con el marco colombiano..

Por lo anterior, solicita a la CRC reevaluar la necesidad de establecer un validador centralizado obligatorio y considerar un modelo regulatorio basado en interoperabilidad, estándares abiertos, certificaciones técnicas y obligaciones de resultado en prevención del fraude. A su juicio, este enfoque permitiría proteger al usuario sin afectar la innovación, la competencia ni la eficiencia operativa.

ANDESCO

Señala que la CRC propone crear una persona jurídica privada, seleccionada por los PRSTM, encargada de expedir certificaciones habilitantes para acceder a recursos de identificación administrados por el Estado, aprobar las plantillas que condicionan el envío del tráfico A2P, gestionar el KYC de los agentes del ecosistema y operar el registro de marcas. Indica que esta alternativa no fue comparada rigurosamente con el fortalecimiento de las capacidades internas de la CRC como Administradora de los Recursos de Identificación.

Técnicamente, a juicio de **ANDESCO**, el validador centralizado introduce tres riesgos graves: (i) Single Point of Failure (SPOF): si el validador falla, todos los PRST podrían perder simultáneamente la capacidad de validar el tráfico A2P, afectando mensajes OTP, alertas de seguridad, notificaciones de emergencia y mensajería crítica de IoT. El nivel de disponibilidad mensual del 99,5 % permitiría hasta 3,6 horas de indisponibilidad al mes. (ii) Honeypot para ciberataques: concentrar en un solo nodo la información de los remitentes autorizados, las plantillas activas y los dominios validados crea un objetivo atractivo para actores maliciosos. Un ataque exitoso podría permitir la inyección masiva de smishing mediante plantillas previamente aprobadas. (iii) el validador deberá atender simultáneamente las consultas de todos los PRST, con volúmenes estimados entre 6.000 y 12.000 consultas por segundo en hora pico. **ANDESCO** considera que garantizar la disponibilidad y los tiempos de respuesta exigidos requeriría inversiones de infraestructura que el Proyecto no cuantifica.

No obstante, **ANDESCO** no descarta la figura del validador y considera que puede ser un instrumento útil para brindar al ecosistema A2P trazabilidad homogénea, neutralidad operativa y reglas comunes de validación, siempre que su diseño incluya salvaguardas suficientes frente a riesgos sistémicos, indisponibilidad, afectación de mensajes legítimos y concentración de información sensible. Por tanto, sus advertencias deben entenderse como la necesidad de establecer un diseño institucional robusto y no como un rechazo a la figura.

En consecuencia, solicita que la CRC defina reglas mínimas sobre gobernanza, independencia funcional, neutralidad, acceso no discriminatorio, confidencialidad, protección de datos, minimización de información, trazabilidad de consultas, auditoría, ciberseguridad, niveles de servicio, disponibilidad, redundancia, continuidad operacional y manejo de incidentes, tomando como referencia la gobernanza de la base de datos administrativa de portabilidad numérica.

Asimismo, considera que el validador debe contar con un plan de contingencia ante indisponibilidad total o parcial, degradación de las API, incumplimiento de tiempos de respuesta, incidentes de seguridad o fallas de interoperabilidad. Este plan deberá preservar la entrega de mensajes legítimos, especialmente los relacionados con autenticación, seguridad, alertas transaccionales, salud, servicios públicos, entidades financieras y demás comunicaciones críticas.

Finalmente, señala que no debería atribuirse responsabilidad regulatoria al PRST por fallas, indisponibilidad, degradación o incidentes del validador centralizado que no sean imputables a su red, operación o conducta.

ANDI

Afirma que los artículos 6.13.1.1 a 6.13.1.6 y 18 crean un validador centralizado, entendido como una persona jurídica única seleccionada por los PRST móviles y financiada por los asignatarios de códigos cortos A2P, encargada de verificar el KYC, aprobar plantillas y emitir certificaciones necesarias para acceder a los recursos y cursar tráfico.

Señala que esta configuración impone una arquitectura compleja que puede entorpecer la operación técnica y generar distorsiones en el mercado, al incorporar un intermediario obligatorio en la cadena de valor de la mensajería A2P.

Advierte que resulta preocupante concentrar en un único actor privado funciones que condicionan el acceso al mercado, la asignación de recursos y el flujo de comunicaciones. Considera que delegar en un particular funciones que inciden en una actividad económica y en las comunicaciones exige una base legal clara, por lo que la ausencia de una habilitación legal expresa plantea problemas de legalidad y proporcionalidad.

Añade que, aunque el Proyecto prevé la supervisión de la CRC o del Administrador de los Recursos de Identificación, no establece salvaguardas suficientes en materia de debido proceso, auditoría, responsabilidad, transparencia, no discriminación y mecanismos de revisión de las decisiones del validador.

Asimismo, considera necesario precisar la gobernanza de los registros, bases de datos, listas y mecanismos de clasificación utilizados para validar, bloquear, etiquetar o restringir comunicaciones. En particular, debe definirse quién los administra, actualiza y supervisa; los criterios técnicos y probatorios

para incluir, excluir, suspender o reclasificar originadores, SENDER ID, códigos cortos o plantillas; y los plazos máximos para resolver solicitudes de revisión o corrección.

Estas precisiones son indispensables para evitar decisiones arbitrarias, reducir falsos positivos y garantizar mecanismos efectivos de contradicción y debido proceso.

Por otra parte, la **ANDI** señala que un validador único introduce riesgos sistémicos y de eficiencia. En primer lugar, constituye un punto único de falla que podría afectar la entrega masiva de mensajes críticos, salvo que se implementen mecanismos robustos de contingencia, validación diferida y continuidad para comunicaciones de seguridad. En segundo lugar, la ausencia de presión competitiva podría desincentivar la innovación tecnológica en soluciones de validación. Finalmente, el esquema traslada el costo de la infraestructura a los asignatarios de códigos cortos A2P, quienes financiarían un actor privado cuya gobernanza y estructura deben someterse a controles estrictos.

ASOBANCARIA

Manifiesta preocupación por la gobernanza del validador centralizado y los tiempos de respuesta para el takedown de campañas de smishing y URLs. Señala que actualmente este proceso exige que el titular legítimo reporte el dominio y que, en plataformas como Shopify o WooCommerce, la revisión por parte del propietario puede retrasar el retiro, aumentando la efectividad de las campañas fraudulentas.

Por lo anterior, sugiere que el Proyecto establezca estándares mínimos de disponibilidad, tiempos máximos de respuesta, mecanismos de auditoría, trazabilidad de las decisiones y procedimientos expeditos de revisión frente a bloqueos o clasificaciones erradas.

Añade que el artículo 6.13.2.2 ya permite cursar, durante contingencias, el tráfico asociado a registros previamente validados, por lo que bastaría extender esta previsión a las comunicaciones críticas. En concreto, propone que durante la indisponibilidad del validador continúen cursándose las plantillas de autenticación y seguridad aprobadas y vigentes; se establezca un trámite expedito para las plantillas de alertas de fraude, dada su naturaleza urgente y cambiante; y se reconozca el carácter crítico de este tráfico en los niveles de servicio del validador.

BLIPBLIP

Señala que el Proyecto asigna a un tercero privado, seleccionado por los PRST y financiado por los PCA e integradores, la función de aprobar, rechazar y validar las plantillas de contenido necesarias para cursar tráfico. Considera que esto podría generar una aplicación desigual de las normas, dado que los envíos de los PRST no estarían sujetos a las mismas validaciones, y trasladaría a un particular funciones de control que deberían estar a cargo del Estado. En este sentido, advierte los siguientes riesgos:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Conflicto de Interés, dado que el centralizador sería seleccionado por los PRST, sin participación de los PCA, aunque su sostenimiento dependería de los agentes sometidos a validación. Además, los PRST tendrían una menor exposición a dichos controles.

- Sobrecostos, ya que la implementación del validador requeriría plataformas, servicios, acuerdos de nivel de servicio y una estructura operativa financiada por los PCA e integradores, lo que incrementaría los costos del envío de SMS y podría apartarse del principio de costos eficientes.

- Ausencia de control operativo, debido a que no se definen las condiciones técnicas y operativas necesarias para garantizar capacidad, niveles de servicio, entrega de mensajes y respeto de las condiciones previamente acordadas entre los PCA y los PRST. Asimismo, la incorporación de un nuevo intermediario podría aumentar los puntos de falla y afectar la trazabilidad y conciliación del tráfico aprobado, rechazado o auditado.

- Garantía de Operación, teniendo en cuenta que el rechazo de una plantilla, sin mecanismos claros de explicación, reposición o apelación, podría impedir el envío de comunicaciones, afectar la continuidad del servicio y limitar la capacidad de respuesta de las empresas frente a las necesidades cambiantes del mercado.

CAMPAIGN REGISTRY

Señala que actualmente no cuenta con personería jurídica en Colombia y solicita que el requisito de estar constituido legalmente en el país o contar con una sucursal no limite la participación de empresas extranjeras como validador centralizado. Considera que exigir una constitución local previa puede restringir la libre concurrencia y excluir empresas internacionales con experiencia y tecnología especializada. Por ello, propone que el proceso de selección esté abierto a participantes internacionales, sin exigir que estén previamente constituidos o domiciliados en Colombia.

Respecto de la financiación del validador centralizado, indica que, aunque el Proyecto dispone que los costos de implementación, gestión, operación y mantenimiento sean asumidos por los asignatarios de códigos cortos A2P bajo el principio de costos más utilidad razonable, considera más adecuado que estos recaigan sobre los asignatarios de SENDER ID, específicamente los agregadores que mantienen una relación directa con las marcas, lo que permitiría un flujo de información más ágil y preciso.

CCIT

Advierte que los artículos 6.13.1.1 a 6.13.1.6 y 18 crean un validador centralizado, entendido como una persona jurídica única financiada por los asignatarios de códigos cortos A2P, encargada de verificar el KYC, aprobar plantillas y emitir certificaciones necesarias para acceder a los recursos y cursar tráfico.

Sostiene que esta configuración impone una arquitectura compleja que puede entorpecer la operación técnica y generar distorsiones en el mercado, al incorporar un intermediario obligatorio en la cadena de valor de la mensajería A2P. Asimismo, considera preocupante que el Proyecto concentre en un único actor privado funciones que condicionan el acceso al mercado, la asignación de recursos y el flujo de comunicaciones.

Afirma que delegar en un particular funciones que inciden en una actividad económica y en el flujo de comunicaciones exige una base legal clara, por lo que la ausencia de una habilitación legal expresa para el validador central plantea problemas de legalidad y proporcionalidad. Añade que, aunque el Proyecto prevé la supervisión de la CRC o del Administrador de los Recursos de Identificación, no establece salvaguardas suficientes en materia de debido proceso, auditoría, responsabilidad, transparencia, no discriminación y revisión de las decisiones del validador.

Por otra parte, señala que la creación de un validador único introduce riesgos sistémicos y de eficiencia. En primer lugar, constituye un punto único de falla que podría afectar masivamente la entrega de mensajes críticos, salvo que se implementen mecanismos robustos de contingencia, validación diferida o continuidad para comunicaciones de seguridad. En segundo lugar, la ausencia de presión competitiva podría desincentivar la innovación tecnológica en soluciones de validación. Finalmente, el esquema traslada el costo de esta infraestructura a los asignatarios de códigos cortos A2P, quienes financiarían un actor privado cuya gobernanza y estructura deberán someterse a controles estrictos.

COLOMBIA FINTECH

Indica que el artículo 6.13.4.7.1 establece que los PRST deben integrar sus plataformas de mensajería —SMSC— con el sistema del validador centralizado mediante API, para consultar en tiempo real la validez del código corto A2P, el SENDER ID y la plantilla antes del enrutamiento de cada mensaje. Considera que esta es una de las disposiciones técnicamente más avanzadas del Proyecto y que, por constituir un punto central para el tráfico A2P nacional, requiere mayor desarrollo en materia de robustez, continuidad y capacidad. Para ello, propone:

1. Comportamiento ante falla o latencia del validador. La norma no define qué debe hacer el PRST cuando la consulta falle o supere el umbral de latencia. Sugiere complementar el artículo 6.13.2.2 —Plan de Contingencia del Validador— para exigir a los PRST cachés locales de validación de corto plazo, con una vigencia no superior a 60 minutos, que permitan mantener el tráfico A2P legítimo durante una falla. Estos cachés deberían poder invalidarse de manera remota e inmediata por instrucción del Administrador de los Recursos de Identificación ante un incidente de fraude activo.

2. Carácter obligatorio de la etiqueta «sin verificar» en contingencia. El artículo 6.13.4.7.2 permite a los PRST marcar los mensajes como «sin verificar» en lugar de bloquearlos, pero de forma facultativa. Dado que el bloqueo total podría afectar comunicaciones críticas, como OTP y alertas de seguridad, solicita que esta etiqueta sea obligatoria durante las

contingencias y que se precisen el alcance de las listas de emergencia del artículo 6.13.2.2 para el sector financiero y las condiciones de activación del plan.

3. Señales de riesgo dinámicas. Propone que el sistema de consulta en tiempo real incorpore señales dinámicas de riesgo, basadas, por ejemplo, en el comportamiento reciente del SENDER ID o en alertas del CTLFSM, y no se limite a verificar el estado binario de los recursos. Esto permitiría que el validador funcione como un sistema de inteligencia de fraude y no únicamente como un directorio de asignaciones.

4. Capacidad mínima garantizada. El artículo 6.13.2.1.2 establece tiempos máximos de respuesta de 200 y 500 ms y un informe semestral de capacidad, pero no define un throughput mínimo de peticiones concurrentes por segundo. Para las entidades financieras, que presentan ráfagas transaccionales en procesos de autenticación, cobranza o eventos comerciales, el dimensionamiento basado en promedios históricos podría ser insuficiente. Una saturación del validador afectaría simultáneamente la capacidad del ecosistema A2P, sin una alternativa inmediata.

Por lo anterior, solicita incluir en el artículo 6.13.2.1.2 un throughput mínimo garantizado, expresado en peticiones concurrentes por segundo, e incorporar este parámetro como criterio técnico obligatorio en el proceso de selección del validador. Sugiere un mínimo de 1.000 solicitudes por segundo, con escalamiento automático ante picos de hasta cinco veces el promedio.

Por otro lado, **COLOMBIA FINTECH** observa que el diseño de gobernanza del validador centralizado podría fortalecerse en los siguientes aspectos:

1. Experiencia acreditada en detección de fraude. Los requisitos del artículo 6.13.1.3 no exigen expresamente experiencia en la operación de sistemas de detección de fraude en tiempo real para ecosistemas de mensajería A2P. Propone incorporar este requisito, dado que la función del validador no se limita a la verificación documental, sino que es relevante para la prevención del fraude.

2. Independencia y supervisión. El artículo 18.1 asigna la selección del validador a los PRSTM, que compiten con algunos de los agentes que deberán ser certificados. Aunque el artículo 6.13.1.3.4 prohíbe vínculos accionarios entre el validador y los agentes registrados, no establece auditorías independientes permanentes ni un procedimiento de quejas con efectos vinculantes. Por ello, solicita un esquema de supervisión independiente, auditorías periódicas obligatorias y un canal formal de quejas ante el Administrador de los Recursos de Identificación.

3. Régimen tarifario. El artículo 6.13.1.2 dispone que los costos del validador sean asumidos por los asignatarios de códigos cortos A2P, bajo el principio de costos más utilidad razonable. Sin embargo, no establece un tope tarifario ni un mecanismo de revisión periódica, pese a

que estos costos podrían trasladarse a los asignatarios de SENDER ID, incluidas las entidades financieras. En consecuencia, solicita un mecanismo formal de regulación tarifaria, con revisión periódica y publicación previa de la metodología de cálculo de costos.

Finalmente, señala que, aunque el artículo 6.13.1.4 establece causales de revisión anticipada de la selección del validador y el artículo 6.13.1.6 define sus prohibiciones, las consecuencias del incumplimiento se limitan a reportes al Administrador de los Recursos de Identificación. No se prevén sanciones económicas directas ni mecanismos de indemnización para los asignatarios afectados por su mal funcionamiento.

Por ello, solicita establecer un régimen sancionatorio explícito, proporcional y de aplicación directa para los incumplimientos del validador centralizado, incluida la obligación de indemnizar a los asignatarios afectados por interrupciones imputables a su negligencia.

CRISTIAN CANTILLO

Formula las siguientes preguntas:

- ¿Cómo define la Comisión el tráfico A2P cuando el originador es el propio operador de servicios de telecomunicaciones (PRM u OMV) y utiliza numeración móvil convencional de diez dígitos (MSISDN)? Si el operador envía desde su plataforma interna notificaciones regulatorias, de facturación o de servicio a sus propios usuarios, ¿este tráfico será considerado A2P comercial o mantendrá su condición de comunicación de red o servicio?

- Cuando un operador utiliza numeración móvil ordinaria, en lugar de códigos cortos, para comunicarse de manera automatizada con sus usuarios, ¿estas líneas deberán registrarse ante el validador centralizado como SENDER ID? De ser así, ¿cómo se evitará que los sistemas de filtrado bloqueen este tráfico legítimo al considerarlo proveniente de una línea móvil personal?

- ¿El envío de SMS informativos propios del operador generará el pago de tasas o contraprestaciones al validador centralizado? Exigir el pago por validar comunicaciones obligatorias impuestas por el Régimen de Protección de los Derechos de los Usuarios (como avisos de fecha de corte o consumo de datos) podría constituir una doble carga económica para el prestador.

- Si un OMV decide mitigar el fraude trasladando sus comunicaciones informativas y transaccionales a canales digitales propios, como una aplicación móvil o mensajería web, ¿garantizará la CRC que este tráfico no sea inspeccionado, clasificado como fraudulento o bloqueado por el operador anfitrión por no haber pasado por el validador centralizado?

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Asimismo, señala que los sistemas automatizados y el validador podrían generar falsos positivos y bloquear mensajes legítimos, como códigos OTP o avisos de suspensión del servicio. En este contexto, pregunta

- ¿Quién responde por los daños económicos al usuario o al operador?
- ¿Cuál será el régimen de responsabilidad administrativa y civil aplicable al validador centralizado o al operador de red por el bloqueo erróneo de tráfico legítimo? Si una falla en el sistema de plantillas o un error del validador interrumpe mensajes transaccionales críticos, ¿quién asumirá los perjuicios, la CRC, el validador o el operador que originó el tráfico?
- ¿Cuál será el procedimiento y el tiempo máximo de respuesta —SLA— para apelar y reactivar un SENDER ID o una plantilla bloqueada por una sospecha errónea de fraude? Considera que la norma debe impedir bloqueos preventivos indefinidos y establecer un mecanismo de reactivación en tiempo real, medido en minutos y no en días hábiles, para proteger la continuidad de la operación.

Asimismo, expone que para que el validador centralizado apruebe una plantilla, el operador tiene que «mostrarle» el texto del mensaje y ahí viaja el core del negocio del operador (estrategias de marketing, copy creativo, ofertas comerciales antes de lanzarlas al mercado). En ese contexto, pregunta ¿Qué protocolos de ciberseguridad y confidencialidad se le exigirán al validador centralizado para garantizar que la base de datos de «plantillas preaprobadas» no sea vulnerable a filtraciones o espionaje industrial? Indica que dado que las plantillas contienen las estrategias comerciales, de fidelización y de precios de los operadores antes de ser enviadas al mercado, ¿cómo garantizará la CRC que el personal del validador centralizado (o terceros competidores) no tenga acceso a esta información privilegiada y sensible para el mercado competitivo?

Respecto de los costos de conectividad e interoperabilidad técnica con el validador centralizado, formula las siguientes preguntas:

- ¿Los costos de desarrollo de software, API de integración, mantenimiento y servidores requeridos para la conexión en tiempo real serán asumidos por el validador o por cada operador? En este último caso, ¿ha evaluado la CRC si estos costos fijos podrían constituir una barrera de entrada para los operadores de menor escala, especialmente los OMV?
- ¿ Qué estándar tecnológico de interoperabilidad utilizará el validador, por ejemplo, API REST sobre HTTP o SMPP? Solicita que la CRC defina en la resolución un estándar abierto, público y tecnológicamente neutral, que no obligue a los operadores a adquirir soluciones de marcas o proveedores específicos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CLEARTECH

Propone que se incorporen mecanismos como el uso de motores de reputación URLs en tiempo real, análisis semánticos del contenido mediante modelos de inteligencia artificial, identificación de patrones asociados a campañas masivas (mensajes con estructuras similares enviados a gran escala) e integración con bases de datos internacionales de amenazas.

CLARO

Señala que la propuesta regulatoria parte de la premisa de que la implementación de mecanismos de validación y autenticación de remitentes requiere la creación o designación de un tercero centralizado encargado de administrar, validar y gestionar la información de los remitentes habilitados para enviar mensajes.

No obstante, considera que el documento soporte no demuestra por qué estas funciones no podrían ser desarrolladas directamente por la CRC, en ejercicio de las competencias atribuidas por la ley y la regulación vigente.

CLARO sostiene que, conforme al artículo 22 de la Ley 1341 de 2009, la CRC administra los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones. En desarrollo de esta competencia, la Resolución CRC 5968 de 2020 consolidó el Régimen de Administración de Recursos de Identificación del Título VI de la Resolución CRC 5050 de 2016, que incluye los códigos cortos para SMS y USSD.

La regulación vigente establece que la CRC asigna los códigos cortos, verifica los requisitos para su otorgamiento, mantiene información de los asignatarios, controla el uso eficiente del recurso, adelanta procesos de recuperación ante incumplimientos y ejerce su administración permanente. Por tanto, ya dispone de parte sustancial de la información necesaria para identificar a los titulares, conocer las condiciones de asignación, verificar los servicios asociados y adelantar actuaciones ante usos presuntamente irregulares.

Sin embargo, el documento soporte no explica por qué estas capacidades serían insuficientes para implementar mecanismos de validación y autenticación de remitentes, ni demuestra que un tercero centralizado generaría mayores beneficios que el fortalecimiento de las herramientas institucionales existentes.

Además, la propuesta no analiza aspectos esenciales como la supervisión, el régimen de responsabilidad, el tratamiento de información sensible, los estándares de ciberseguridad, el manejo de incidentes, los conflictos de interés y los mecanismos de resolución de controversias. Esta ausencia resulta relevante, dado que un nuevo intermediario generaría costos, dependencias operativas y

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

tecnológicas, y riesgos de concentración en un mercado que actualmente funciona bajo esquemas descentralizados.

Desde la perspectiva del Análisis de Impacto Normativo, **CLARO** considera que corresponde a la CRC demostrar que la creación del nuevo actor es la alternativa más eficiente, proporcional y menos gravosa. No obstante, el documento soporte no compara esta opción con alternativas menos intrusivas, como fortalecer las funciones que ya ejerce la CRC sobre los recursos de identificación.

En consecuencia, antes de imponer un esquema centralizado, la Comisión debería justificar por qué la verificación de remitentes no puede desarrollarse dentro del marco institucional existente y por qué debe trasladarse a un tercero, considerando sus costos, riesgos e impactos competitivos, especialmente cuando el mercado fue intervenido recientemente mediante una tarifa de terminación de $0,03 por SMS.

Adicional, **CLARO** realiza los siguientes comentarios puntuales sobre la propuesta de creación de un validador centralizado:

- La propuesta es incompatible con la arquitectura, la capacidad de procesamiento y los niveles de servicio actuales.

- La consulta en tiempo real al validador introduciría una latencia adicional mínima de 200 ms por mensaje sobre una plataforma GW PCA que actualmente opera entre 50 y 150 ms.

- Con un tráfico pico de 2.000 a 3.000 mensajes por segundo, se generarían igual número de llamadas API externas síncronas, volumen para el cual el GW PCA de COMCEL no fue diseñado ni cuenta con capacidad nativa.

- Sin un rediseño arquitectónico profundo, el cumplimiento literal de la norma degradaría la mensajería A2P hasta hacerla inoperativa en horas pico.

- La latencia actual permite cumplir los SLA de mensajes transaccionales, como OTP y alertas bancarias, que normalmente requieren entregas inferiores a 500 ms. Con la consulta síncrona al validador, la latencia podría ubicarse entre 290 y 495 ms antes de llegar al SMSC y superar entre 610 y 890 ms en escenarios de alta demanda, incumpliendo dichos niveles de servicio.

- Los mensajes OTP y las alertas de seguridad serían los más afectados por esta degradación.

- La obligación de consultar al validador por cada mensaje genera una demanda de API proporcional al tráfico del GW PCA. Con una latencia adicional aproximada de 240 ms, el throughput efectivo podría reducirse a entre 340 y 510 mensajes por segundo, equivalente a una pérdida cercana al 83 % de la capacidad en hora pico.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Los mensajes no procesados se acumularían en cola, generando timeouts SMPP, rechazos y una degradación progresiva del servicio.

- La resolución no exige una sola validación por mensaje: exige verificar tres (3) elementos de forma simultánea antes del enrutamiento de cada mensaje A2P, lo que hace el proceso más complejo.

- La resolución NO contempla la posibilidad de validación por sesión, por lote (batch), ni por ventana de tiempo, lo cual debería ser contemplado para evitar impactos de encolamiento, dado el nivel y mensajes que se manejan.

- La exigencia es literalmente 'previo al enrutamiento de CADA mensaje A2P' (Art. 6.13.4.7.2).

- La CRC no realizó un análisis de impacto sobre la viabilidad técnica de esta exigencia en plataformas de alto throughput como el GW PCA de Claro Colombia.

- Tampoco establece mecanismos de caché local, tiempos de vigencia —TTL— ni validaciones optimizadas por combinación de SENDER ID y plantilla.

- La inviabilidad técnica también afecta al validador, que deberá atender simultáneamente las consultas de todos los PRSTM. Un único sistema podría recibir entre 6.000 y 12.000 consultas API por segundo.

- Cada PRSTM tiene su propio GW PCA cursando tráfico A2P y el validador centralizado debe atender las consultas de todos simultáneamente, por lo que su procesamiento por mayor capacidad que se tenga va a encolar el proceso de alguno de los PRSTM.

- Cualquier degradación del validador afectaría simultáneamente los GW PCA de todos los operadores. Incluso una disponibilidad del 99,5 % mensual permite hasta 3,6 horas de indisponibilidad, con impacto sobre todo el ecosistema A2P.

- La resolución crea inadvertidamente un Single Point of Failure (SPOF) de alcance nacional para el servicio de mensajería A2P, concentrando en un único tercero privado la disponibilidad de un servicio de telecomunicaciones esencial.

En virtud de lo anterior, Comcel presenta la siguiente propuesta, la cual, a su juicio, puede contribuir a solucionar la problemática, se compadece con las capacidades de la red, es más rápida en la implementación y sus costos no son tan excesivos como los que propone la CRC en el documento objeto de comentarios:

PROPUESTA TÉCNICA DE CLARO A IMPLEMENTAR:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

COMCEL no se opone al objetivo de la norma (garantizar que solo mensajes con SENDER ID y plantilla válidos sean entregados al usuario). El impacto se traduce es en la implementación técnica específica exigida (consulta síncrona por mensaje), que es operativamente inviable. Al respecto propone las siguientes alternativas técnicas que logran el mismo objetivo regulatorio con viabilidad de implementación real:

Alternativa: Validación por sesión de acceso con actualización en tiempo real ante cambios de estado.

- En lugar de validar por cada mensaje, el GW PCA valida al momento de establecer o renovar la sesión de acceso SMPP del PCA/IT. El validador centralizado notificaría al GW PCA vía push (webhook o señalización) únicamente cuando el estado de un SENDER ID, código corto A2P o plantilla cambie. El GW PCA mantiene un estado local en caché.

- Reducción de consultas al Validador: de 7-10 millones/hora a decenas de notificaciones/hora.

- Tiempo de respuesta ante una suspensión por CRC: < 30 segundos (notificación push) vs. inmediato por consulta por mensaje.

- Resultado regulatorio equivalente: ningún mensaje de un SENDER ID suspendido es entregado, con un margen de gracia de < 30 segundos que es operativamente aceptable.

- Esta propuesta es técnicamente viable e implementable en 10 a 12 meses desde la disponibilidad del Validador.

En conclusión, **COMCEL** acepta validar el SENDER ID, el código corto A2P y la plantilla antes de cursar tráfico, pero solicita que la CRC permita mecanismos equivalentes, como validación por sesión con notificación de cambios o caché con TTL regulado.

También propone excluir de la validación síncrona por mensaje las comunicaciones de autenticación y seguridad —OTP—, dada su criticidad y el riesgo asociado a la latencia adicional.

Adicional a lo señalado por Comcel para poder implementar el validador centralizado, incluye las siguientes observaciones:

Validador como «Punto Único de Falla» (Single Point of Failure - SPoF): En la arquitectura tecnológica actual, la falla de un nodo SMS puede mitigarse desviando el tráfico a otro. Con un validador centralizado, una falla tecnológica, de software o del proveedor de nube podría impedir en todo el país la recepción de OTP bancarias, alertas de pánico, coordenadas de vehículos de transporte de valores o confirmaciones de alarmas, con impactos sobre la actividad financiera y la seguridad de personas y empresas.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

El «Efecto Atractivo» para Ciberataques (Honeypot): El validador centralizado concentraría la información de marcas, códigos cortos, plantillas y metadatos de transacciones. Un ataque exitoso podría permitir modificar plantillas e inyectar campañas masivas de smishing desde servidores aparentemente autorizados, evadiendo controles de los operadores.

Bloqueo de Mensajes Críticos por Campos Dinámicos en IoT y Georreferenciación: Los SMS de IoT (ej. rastreadores de vehículos, sensores industriales) envían cadenas de datos altamente variables y dinámicas como coordenadas GPS (4.6097,-74.0817), alertas de velocidad o códigos de falla de motores. Si el algoritmo de validación de plantillas del Validador es demasiado rígido, puede clasificar erróneamente una trama de datos hexadecimal o un cambio abrupto de coordenadas como «contenido no aprobado» o «sospechoso».

Sobre la función de validación de la plantilla: Respecto de la validación de las plantillas solicita precisar que el validador deberá informar inmediatamente al PRSTM para que suspenda el envío de los SMS asociados.

Asimismo, no considera clara la necesidad del validador si los PRSTM deben continuar verificando los mismos elementos (código corto, SENDER ID y plantilla) y conectarse mediante API al sistema central.

Señala que el validador no debe limitarse a administrar información, sino que debe validarla y advertir anomalías en los envíos. Si la responsabilidad de verificar permanece en los PRSTM, se refuerza la posibilidad de que la CRC administre directamente esta información sin crear un tercero.

Tampoco considera claro el reporte de mensajes bloqueados por ausencia o invalidez de identificadores o plantillas, dado que el validador tendría acceso a la información mediante la API.

Sobre los tiempos establecidos para seleccionar el Validador centralizado:

CLARO considera que los plazos previstos son insuficientes frente a la complejidad del proceso y la necesidad de contar con empresas que cumplan los requisitos técnicos. Por ello, propone:

- Que los términos se contabilicen en días hábiles y no calendario.
- Que el plazo para elaborar los documentos del proceso de selección sea de al menos quince días hábiles.
- Que el proceso de selección tenga una duración mínima de un mes, prorrogable por otro mes cuando ninguno de los oferentes cumpla los requisitos.

ETB

Considera que el Análisis de Impacto Normativo no desarrolla suficientemente los riesgos operativos, tecnológicos y sistémicos asociados a la creación de un componente centralizado que se convertiría en un elemento crítico para el funcionamiento del ecosistema nacional de mensajería.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Señala que la consulta obligatoria previa introduce un punto único de falla (single point of failure), cuya indisponibilidad, degradación o mal funcionamiento podría afectar masivamente múltiples servicios esenciales. Cualquier incidente tecnológico, falla de conectividad o integración, degradación del desempeño, ataque cibernético o problema de capacidad podría impactar simultáneamente a los operadores, integradores y entidades que dependen del mecanismo para validar sus comunicaciones.

Asimismo, expresa preocupación por la ausencia de un análisis detallado sobre los efectos del incremento de las latencias. Indica que el Proyecto establece tiempos de validación exigentes, sin evidencia suficiente sobre el comportamiento de una plataforma de esta naturaleza bajo condiciones de carga masiva, contingencias o crecimiento acelerado del tráfico. Una degradación en los tiempos de respuesta podría generar retrasos significativos en la entrega de comunicaciones críticas.

Este riesgo resulta especialmente relevante para sectores dependientes de la mensajería transaccional, como el financiero, asegurador, salud, transporte, comercio electrónico, servicios públicos y gobierno digital. Una parte importante de sus operaciones de autenticación y seguridad depende del envío oportuno de mensajes OTP, códigos de verificación, alertas transaccionales, confirmaciones de pago, validaciones biométricas y otras notificaciones cuya utilidad desaparece si no se entregan dentro de ventanas de tiempo reducidas.

En este sentido, manifiesta que un retraso de pocos segundos por fallas de sincronización, indisponibilidad temporal del validador o congestión de las API podría interrumpir operaciones financieras legítimas y procesos de validación de identidad, afectar la experiencia de millones de usuarios y generar impactos económicos significativos.

Por lo anterior, considera indispensable que la Comisión evalúe las exigencias económicas, técnicas y operativas de la propuesta frente a su efectividad, ya que su implementación requiere inversiones significativas y condiciones robustas de continuidad operativa, alta disponibilidad, redundancia geográfica, planes de contingencia, operación degradada, respaldo y recuperación ante desastres.

Asimismo, pone de manifiesto que deberían definirse niveles mínimos de servicio (SLA), mecanismos de compensación ante fallas, procedimientos aplicables durante la indisponibilidad del validador y responsabilidades frente a afectaciones derivadas de incidentes imputables al administrador de la plataforma.

Finalmente, considera necesario evaluar arquitecturas menos centralizadas o mecanismos distribuidos de validación que mitiguen los riesgos de concentrar funciones críticas en un único componente. Añade que la medida no cubre a las plataformas OTT, por lo que el fraude podría migrar desde los servicios tradicionales hacia espacios no regulados, comprometiendo la efectividad de las obligaciones impuestas a los PRST.

INETUM

Solicita aclarar la forma en que los agentes consultarán la base de datos centralizada, precisando si la consulta deberá realizarse en línea o en modo batch.

Asimismo, frente a lo previsto en el Capítulo 13 del Título VI de la versión preliminar del Proyecto, según el cual ningún mensaje A2P podrá cursarse por las redes de los PRST sin una plantilla de contenido aprobada y vigente en el sistema del validador centralizado, formula las siguientes inquietudes:

- ¿Solo deberá validar las plantillas y senderID que haya enviado la CRC? ¿Si no existe la plantilla o el sender ID, se informa al prestador y su SMS no debe ser enviado?
- ¿Que sucede si el PRSTM envía en SMS sin pasar por el validador?
- ¿Qué pasa si el PRSTM está en proceso de validación, pero el ente central tuvo alguna intermitencia, puede reintentar la consulta al validador antes de enviar el SMS?
- ¿Como sería el proceso de conciliación entre el centralizador y el PRSTM?
- ¿Como sería el proceso para que el centralizador se entere de una nueva plantilla o senderID?
- ¿Los PCA también deben interactuar con el centralizador? ¿O solo el PRSTM?
- ¿El acceso al RNE debe ser solo por parte del PRSTM antes de enviar el SMS? O del centralizador también lo debe implementar.
- ¿El SMS lo debe entregar el centralizador al usuario final? ¿O solo el centralizador valida y devuelve la validación al PRSTM para que este finalmente lo envíe al usuario final?
- ¿El proceso de validación del cliente (KYC) es responsabilidad del centralizador?
- ¿Aclarar si el Administrador de Recursos de Identificación forma parte del validador centralizado y cuál es su rol y procedimientos asignados?
- ¿Aclarar cómo el Administrador Recursos de Identificación va a auditar las causales indicadas para recuperación del SENDER ID?

INALAMBRIA

Señala que la imposición de controles previos, validaciones o procesos de aprobación podría afectar la oportunidad de mensajes cuyo retraso puede generar riesgos para la vida, riesgos para la salud, pérdidas económicas y afectaciones de servicios esenciales. Frente a lo anterior, solicita la posibilidad de aplicar validaciones sólo para aquellos mensajes de texto que realmente puedan ser sujetos de fraude y que cumplan las características observadas previamente: Originación a partir de mayoristas internacionales y presencia de URLs.

JULIO NULDEMAR

Expone que debe existir un mecanismo que impida la parálisis de las comunicaciones del país ante caídas del validador centralizado, y propone el siguiente parágrafo «**PARÁGRAFO NUEVO. PROTOCOLO DE FALLA SEGURA (FAIL-SAFE).** En caso de presentarse indisponibilidad técnica, caídas de sistema, degradación de plataforma o fuerza mayor en el validador centralizado que impidan

la verificación de plantillas en tiempo real, los PRST quedarán plenamente facultados para cursar de forma directa el tráfico A2P legítimo de sus clientes corporativos, priorizando el principio de continuidad del servicio público de telecomunicaciones. Durante el tiempo que dure la contingencia, se suspenderá la aplicación de sanciones por tráfico no validado»

NEXVIA

Señala que el Proyecto otorga a una persona jurídica privada —seleccionada por los PRSTM conforme a condiciones definidas por estos, según el artículo 18, pero financiada por los PCA e IT— la facultad de aprobar o rechazar las plantillas de contenido necesarias para operar, sin que exista recurso administrativo contra sus decisiones.

Frente a lo anterior, plantea los siguientes conflictos de interés:

- Violación del artículo 209 C.P. La imparcialidad de la función administrativa delegada se rompe de origen, el validador depende, para su designación y permanencia, de los competidores directos de los sujetos que valida.

- Violación del artículo 29 C.P. El rechazo de una plantilla paraliza la operación del PCA/IT sin que el proyecto prevea recurso de reposición ni apelación, por la misma suspensión preventiva.

- Violación de los artículos 333 y 13 C.P. El tráfico A2P propio del PRSTM (publicidad de planes, notificaciones de cobro, OTP propios) queda exento de la validación que sí se impone a los independientes, configurando una ventaja competitiva regulatoria injustificada.

En este sentido, sostiene que el diseño del validador vulnera los artículos 13, 29, 209 y 333 de la Constitución, debido a su selección por competidores, financiación por los agentes supervisados, exención del tráfico propio de los seleccionadores y ausencia de recursos. Aclara que no controvierte la utilidad de una instancia técnica de verificación, sino que su control corresponda a una de las partes del mercado.

Por ello, considera que la reformulación mínima debe incluir:

(i) selección del validador mediante proceso público adelantado y decidido por la CRC, con requisitos de independencia verificables respecto de todos los agentes del ecosistema;
(ii) gobernanza con participación de todos los actores (PRST, PCA, IT) y supervisión permanente de la Comisión;
(iii) sometimiento del tráfico A2P propio de los PRST al mismo régimen de validación aplicable a los demás agentes;
(iv) financiación proporcional entre todos los agentes que cursan tráfico, incluidos los PRST; y,

(v) recurso de reposición ante la CRC contra los rechazos de plantillas y certificaciones, con cinco (5) días hábiles para interponerlo, diez (10) días hábiles para resolverlo y efecto suspensivo (entendiéndose provisionalmente vigente la plantilla) salvo fraude activo comprobado.

Concluye que, sin estos elementos, el validador no sería un instrumento de mitigación del fraude, sino un mecanismo de administración privada del acceso al mercado por parte del duopolio, configurando una captura regulatoria.

SAEM

Sostiene que el artículo 6.13.1.2 establece que los costos de implementación, gestión, operación y mantenimiento del validador centralizado serán asumidos por los asignatarios de códigos cortos A2P (es decir, los IT). Sin embargo, el artículo 18.1 atribuye su selección exclusivamente a los PRSTM, mientras que el artículo 6.13.5.1 conforma el Comité de Seguimiento con los asignatarios de códigos cortos A2P, sin voto del validador.

Afirma que esta configuración genera una asimetría estructural: quien paga (el IT) no decide, y quien decide (el PRSTM) no asume necesariamente el costo. Añade que los PRSTM también pueden competir como IT, conforme al artículo 6.4.1.3, por lo que un competidor seleccionaría y definiría las condiciones del proveedor monopólico que los demás agentes deben contratar y financiar. Esto podría generar riesgos de abuso de posición de dominio y de fijación de tarifas o especificaciones técnicas favorables a determinados actores.

Asimismo, advierte que concentrar toda la validación A2P en una única persona jurídica crea un punto único de falla sobre el tráfico A2P nacional. Señala que la experiencia de India con el sistema DLT muestra que la dependencia de un único proceso de validación, ante una falla, puede bloquear masivamente tráfico legítimo, incluidos OTP y mensajes transaccionales críticos.

Por lo anterior, propone: (i) Que el órgano de selección y gobierno del validador esté integrado, con voz y voto, por los IT que financian su operación, y no solo por los PRSTM; (ii) que el financiamiento se distribuya entre toda la cadena de valor (PRSTM, IT y PCA) y no exclusivamente sobre los IT, o que su costo sea remunerado dentro del esquema de remuneración de la Fase II; (iii) que la tarifa del validador se someta a un tope o a revisión de la CRC bajo el principio de orientación a costos, con publicidad de su estructura; y (iv) que el régimen contemple expresamente la posibilidad de más de un validador acreditado e interoperable, para evitar el monopolio y el punto único de falla.

De manera concreta solicita rediseñar el gobierno y la financiación del validador centralizado: participación de los IT en su selección y gobierno; distribución del costo en toda la cadena de valor (o su reconocimiento en la remuneración de la Fase II); tope o revisión de tarifa orientada a costos; y posibilidad de validadores múltiples e interoperables para evitar el monopolio y el punto único de falla. Además, que ante la indisponibilidad del validador, se adopte por defecto un esquema fail-open con la

etiqueta «sin verificar», se eleve la disponibilidad mínima a por lo menos 99,95% y se permita la validación mediante caché sincronizada para reducir la latencia y la dependencia del sistema central.

SINCH

Identifica las siguientes fricciones en el mercado:

• Aunque no representa necesariamente una mejora real en seguridad, exigir la preaprobación de todas las plantillas puede traducirse en mayor burocracia, fricción y demoras para las empresas legítimas. Por ello, el validador centralizado deberá contar con tecnología, automatización o inteligencia artificial que permita aprobarlas rápidamente sin afectar el dinamismo del comercio electrónico.

• Trasladar la totalidad de los costos a los asignatarios de códigos cortos A2P puede generar una barrera de entrada para nuevos proveedores o agregadores de menor tamaño. Aunque se prevén tarifas diferenciadas por volumen, los costos fijos de la implementación tecnológica inicial podrían encarecer el acceso al recurso.

• La validación de plantillas y la consulta en tiempo real antes del enrutamiento pueden generar cuellos de botella y problemas de latencia. En el ecosistema A2P, donde la inmediatez de mensajes como los OTP es esencial, depender de una consulta centralizada por cada mensaje podría degradar la calidad del servicio y generar fallas ante la indisponibilidad del validador.

• La falta de exigencia de APIs convertirá al Validador en un cuello de botella: Si el sistema no está automatizado desde su concepción, los procesos serán insosteniblemente lentos. Para evitar esta fricción, la norma debería exigir al validador API estandarizadas, robustas y de muy baja latencia para el registro de plantillas y las consultas de enrutamiento, sin procesos manuales en la ruta crítica del tráfico.

• El Proyecto debe delimitar la responsabilidad civil y contractual cuando el validador apruebe por error una plantilla fraudulenta o bloquee injustificadamente tráfico legítimo por fallas en sus bases de datos, con el fin de proteger a los asignatarios de pérdidas económicas y reputacionales.

• También se requiere un procedimiento expedito para apelar decisiones como el rechazo de una plantilla o marca, sin acudir directamente a un proceso administrativo prolongado ante la CRC, garantizando la continuidad del negocio.

Adicionalmente, señala que los costos de creación y mantenimiento de la infraestructura del validador y del registro de SENDER ID serán asumidos inicialmente por operadores y agregadores, pero probablemente se trasladarán a las empresas y, finalmente, a los usuarios mediante tarifas más altas.

Finalmente, considera que, así como se establecen obligaciones estrictas para operadores y marcas, la regulación debe prever multas y sanciones para el validador centralizado cuando incumpla los acuerdos

de niveles de servicio o sufra una brecha de seguridad que exponga la base de datos de SENDER ID y la información de KYC de las empresas.

SUMA

Considera que el validador no debería tener funciones relacionadas con la revisión o validación de plantillas de contenido del tráfico A2P. No obstante, considera razonables las funciones de administración, gestión e integridad del proceso de validación de los agentes que participan en el ecosistema A2P, siempre que no impliquen acciones coercitivas ni restricciones a la libre actividad empresarial.

Señala que, si el validador identifica malas prácticas o comportamientos atípicos, su función debe limitarse a recopilar y remitir la información correspondiente para que sea evaluada por las autoridades competentes. Advierte que otorgarle facultades de censura o limitación sobre la generación de contenidos podría generar controversias jurídicas y afectar los objetivos regulatorios perseguidos.

Finalmente, propone eliminar las funciones atribuidas al VALIDADOR CENTRALIZADO en el artículo 6.13.1.5 del proyecto de resolución, especialmente aquellas relacionadas con la validación o fiscalización del contenido de los mensajes A2P mediante plantillas u otros mecanismos.

TRANSUNION

Considera indispensable que el proceso de selección del validador centralizado previsto en el artículo 18 del Proyecto se ajuste a estándares rigurosos de transparencia, objetividad y concurrencia, incorporando como mínimo:

a. Una convocatoria abierta que permita la participación de terceros neutrales, especializados e idóneos.

b. La publicación previa de criterios técnicos, operativos, de seguridad, independencia, gobernanza y experiencia relevante.

c. La documentación objetiva de los criterios de elegibilidad, metodologías de evaluación, puntajes y razones que fundamenten la decisión de selección.

d. Mecanismos claros para que la CRC pueda revisar la conformidad del proceso con los principios de transparencia, competencia, independencia, imparcialidad y no discriminación.

e. La incorporación de criterios que evalúen experiencia en validación de identidad, gestión de riesgo de fraude, procesamiento transaccional de alta disponibilidad, seguridad de la información y gobernanza de ecosistemas de telecomunicaciones.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

f. Un plan documentado de transición, continuidad operacional y entrega ordenada de información en caso de sustitución del validador luego del período inicial de operación.

En materia de independencia y conflictos de interés, señala que el numeral 6.13.1.3.4 establece que el validador no debe tener vínculos accionarios, contractuales o de control con los PRSTM, los asignatarios de códigos cortos A2P o sus grupos empresariales cuando puedan comprometer su independencia e imparcialidad.

Aunque comparte la necesidad de preservar la autonomía y objetividad del validador, considera necesario precisar cuándo un vínculo compromete efectivamente su independencia. Una interpretación amplia podría restringir injustificadamente la participación de proveedores especializados que mantengan relaciones comerciales legítimas con agentes del ecosistema.

Por ello, solicita que la incompatibilidad se limite a vínculos que, por su naturaleza, alcance, duración o efecto económico, generen un conflicto de interés real, actual y verificable. Asimismo, propone permitir que la independencia se acredite mediante segregación funcional, gobierno corporativo, controles de acceso, murallas de información, auditorías independientes, declaración y gestión de conflictos de interés y supervisión de la CRC.

También solicita aclarar que la prohibición no comprende los contratos de operación o prestación de servicios celebrados bajo condiciones objetivas, transparentes y no discriminatorias

Respecto de la interoperabilidad, modularidad y uso de proveedores especializados, señala que el esquema exige capacidades diversas, como KYC, validación documental, verificación de marcas y plantillas, administración de registros, gestión de URLs y dominios, análisis de incidentes, consultas en tiempo real, seguridad de la información y reportes regulatorios.

Por esta razón, considera conveniente permitir que la persona jurídica seleccionada actúe como responsable integral ante la CRC, aunque se apoye en proveedores especializados para determinados componentes tecnológicos, operativos o de ciberseguridad. Este modelo mantendría un único responsable regulatorio y permitiría aprovechar capacidades complementarias.

Solicita precisar que la prohibición de delegar funciones de verificación documental y KYC no impide utilizar herramientas tecnológicas, infraestructura, analítica, ciberseguridad o proveedores especializados, siempre que el validador conserve la dirección, control, responsabilidad y trazabilidad de las funciones.

Para las actividades que requieran autorización de la CRC, propone establecer un procedimiento claro, objetivo y oportuno, evitando decisiones discrecionales o trámites que afecten la continuidad del servicio.

Añade que la regulación debe evitar arquitecturas cerradas, herramientas específicas o soluciones propietarias que limiten la participación de proveedores con capacidades equivalentes o superiores. Los requisitos técnicos deberían formularse bajo un enfoque de neutralidad tecnológica y permitir soluciones innovadoras que cumplan los niveles mínimos de desempeño, seguridad y continuidad.

Finalmente, señala que la efectividad del modelo dependerá de la remuneración y los incentivos que se definan en la Fase II. Considera necesario que el modelo económico permita inversiones sostenibles en validación, seguridad, monitoreo, reportes, gestión de incidentes y protección del consumidor.

Por lo anterior, solicita que desde la Fase I se contemplen: la recuperación razonable de costos asociados a la validación e infraestructura de confianza; una distribución clara de responsabilidades económicas entre los actores beneficiados por el sistema; incentivos para procesos robustos de KYC, gestión de plantillas y monitoreo antifraude; criterios de asequibilidad que prevengan el abuso de los canales; y tratamientos diferenciados para casos de uso de mayor o menor riesgo, con base en parámetros objetivos.

PTC

Plantea que en relación con los artículos 6.13.1.1 a 6.13.1.6 y 18 del Proyecto, mediante los cuales se establece la figura de un **validador centralizado**, entendido como una persona jurídica única, seleccionada por los PRST móviles y financiada por los asignatarios de códigos cortos A2P, al que se le atribuyen funciones como la verificación de requisitos de conocimiento del cliente (KYC), la aprobación de plantillas de mensajería y la expedición de certificaciones necesarias para acceder a los recursos y cursar tráfico, **PTC** formula las siguientes consideraciones:

Considera preocupante que el Proyecto concentre en un **actor privado** un conjunto de funciones que, en la práctica, **condicionan el acceso al mercado, la asignación de recursos escasos y el flujo de comunicaciones electrónicas**. A su juicio, esta configuración regulatoria podría generar riesgos relevantes en materia de delegación de competencias, al otorgar a dicho actor una posición determinante en la cadena de valor del servicio A2P.

Adicionalmente, señala que, aunque el Proyecto contempla instancias de supervisión por parte de la CRC **no establece salvaguardas suficientes** para garantizar:

- El respeto del **debido proceso** en las decisiones adoptadas por el validador;
- La implementación de mecanismos robustos de **auditoría y rendición de cuentas**;
- La definición clara de un **régimen de responsabilidad** frente a eventuales perjuicios;
- La observancia de principios de **transparencia y no discriminación** en el ejercicio de sus funciones;
- La existencia de **mecanismos efectivos de revisión o impugnación** de las decisiones adoptadas.
- La confidencialidad y el adecuado manejo de la información contenida en los SMS

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

De igual manera, **PTC** considera que mas allá de las observaciones de política regulatoria planteadas, la creación del validador centralizado suscita un reparo de legalidad que antecede cualquier discusión sobre su diseño institucional.

Expone que la administración de los recursos de identificación, dentro de los cuales se encuentran los códigos cortos A2P y el SENDER ID creado por el propio Proyecto, constituye una función pública atribuida de manera expresa y exclusiva a la CRC por el numeral 12 del artículo 22 de la Ley 1341 de 2009, modificado por el artículo 19 de la Ley 1978 de 2019.

Agrega, que esta atribución comprende no solo la asignación y recuperación de los recursos, sino también las actividades de verificación, validación y certificación que condicionan su otorgamiento, por cuanto estas constituyen un presupuesto necesario e inescindible para el ejercicio de dicha competencia legal.

En su criterio, ninguna de las normas que atribuyen a la CRC la administración de los recursos de identificación, ni la Ley 1341 de 2009, ni la Ley 1978 de 2019, habilita a la Comisión para delegar, encargar o trasladar a un tercero particular las funciones de verificación, validación inherentes a dicha competencia. En consecuencia, considera que la creación del validador centralizado mediante una resolución de carácter general excedería la potestad reglamentaria de la CRC y no cumpliría la reserva de la Ley 489 de 1998 para atribuir de funciones públicas a particulares.

Por lo anterior, PTC solicita que las funciones previstas para el validador centralizado sean ejercidas directamente por la CRC, en su calidad de Administrador de los Recursos de Identificación, sin perjuicio de que pueda apoyarse en terceros para la prestación de servicios técnicos u operativos puramente instrumentales como infraestructura tecnológica o soporte operativo, siempre que las decisiones de verificación, validación, certificación, aprobación o rechazo que incidan directamente en el acceso a los recursos de identificación permanezcan en cabeza de la Comisión.

Así mismo propone incorporar medidas regulatorias adicionales que mitiguen los riesgos identificados, garanticen condiciones equitativas de acceso al mercado y eviten la generación de barreras de entrada o restricciones indebidas a la competencia.

Adicionalmente, considera que el Proyecto debe **precisar de manera expresa y detallada la gobernanza** aplicable a los registros, bases de datos, listas y mecanismos de clasificación utilizados para validar, bloquear, etiquetar o restringir comunicaciones dentro del ecosistema A2P.

En particular, estima necesario definir:

- La **titularidad, administración y supervisión** de dichos registros, así como las responsabilidades de cada actor involucrado;

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Los **criterios técnicos, objetivos y verificables** para la inclusión, exclusión, suspensión o reclasificación de originadores, SENDER ID, códigos cortos y plantillas;
- Los estándares mínimos de **soporte probatorio** requeridos para adoptar decisiones que generen efectos restrictivos; y
- Los **plazos máximos** para atender y resolver solicitudes de revisión, actualización o corrección de la información contenida en dichos sistemas.

Advierte que la ausencia de estas definiciones puede generar margenes de discrecionalidad, **decisiones arbitrarias o inconsistentes**, aumento de falsos positivos y afectaciones desproporcionadas para los agentes del mercado. Estas precisiones serían necesarias para brindar seguridad jurídica y operativa al esquema, así como para garantizar **mecanismos efectivos de contradicción, defensa y debido proceso**, en concordancia con los principios de transparencia, trato no discriminatorio y promoción de la competencia.

Teniendo en cuenta las contingencias que se derivan del proyecto, **PTC** solicita que la CRC evalúe sus efectos dentro del Análisis de Impacto Normativo (AIN), mediante indicadores de desempeño y efectividad relacionados, entre otros aspectos, con los falsos positivos en el bloqueo o etiquetado de mensajes, la disponibilidad del validador, los tiempos respuesta a consultas, la entrega de comunicaciones críticas, las solicitudes de corrección o reclasificación y la evolución de eventos de fraude asociados a SMS o llamadas.

Esa trazabilidad permitiría verificar y adoptar oportunamente los ajustes necesarios, evaluar la proporcionalidad de las obligaciones impuestas y evitar que las medidas destinadas a proteger al usuario terminen afectando servicios legítimos y esenciales.

Por otra parte, aunque el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles constituye un canal de interacción previsto en el proyecto, PTC considera conveniente **habilitar canales seguros y estandarizados para el intercambio de información entre los PRST, los asignatarios de códigos cortos A2P**, los proveedores de contenido y aplicaciones (PCA), y los integradores tecnológicos, de **manera independiente a la CRC.** Estos mecanismos deben estructurarse bajo principios claros de gobernanza de datos y regirse por criterios estrictos de necesidad, finalidad y proporcionalidad, limitando el tratamiento de la información a los fines legítimos de prevención, detección y mitigación de fraudes y abusos. Asimismo, deberán contemplar salvaguardas robustas en materia de reserva de la información y protección de datos personales, conforme al marco normativo aplicable.

Finalmente, PTC considera que la implementación adecuada de estos canales fortalecería la coordinación entre los actores, mejoraría la eficacia de las medidas preventivas y reduciría los riesgos sistémicos, sin afectar indebidamente sus derechos, permitiendo alcanzar un equilibrio entre la seguridad del ecosistema y la promoción de condiciones de competencia leal y transparente.

ACCESO AL REGISTRO DE NÚMEROS EXCLUIDOS

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Frente al parágrafo del artículo 2.1.18.1. del proyecto de resolución, se establece que «La Superintendencia de Industria y Comercio (SIC), en el marco de sus competencias y especialmente de la facultad prevista en el artículo 95 de la Ley 2300 de 2023, podrá solicitar a la CRC información relacionada con los trámites administrativos de recuperación de recursos de identificación establecidos en el TÍTULO VI de la Resolución CRC 5050 de 2016, para que sirvan de insumo en las investigaciones vinculadas con el RNE**. Asimismo, se prevé que la SIC pueda requerir información directamente al validador centralizado, una vez este entre en operación**.

PTC señala que, si bien la CRC tiene la obligación legal de suministrar información que sirva de insumo para las investigaciones adelantadas por la SIC en relación con el RNE, dicha facultad no puede extenderse al validador centralizado sin una disposición legal expresa. En su criterio, esta previsión desconoce los límites legales de dicha atribución y reafirma que las funciones previstas para el validador centralizado deberían ser ejercidas directamente por la CRC.

En este sentido, el artículo 5 de la Ley 2300 de 2023 dispone que el gobierno nacional, a través del MINTIC y en coordinación con la CRC, implementará **las medidas técnicas necesarias para la adopción del RNE**. No obstante, esta disposición no otorga a la CRC una competencia reglamentaria para imponer al validador centralizado la obligación de suministrar información directamente a la SIC.

PTC resalta que la CRC es la entidad encargada de disponer y administrar el RNE y, por tanto, es quien cuenta con la información actualizada sobre su registro y consulta. En consecuencia corresponderá a la SIC vigilar en ejercicio de sus competencias legalmente definidas, solicitar dicha información directamente a la entidad señalada en la Ley.

Por lo anterior, PTC solicita respetuosamente a la CRC eliminar la disposición que habilita a la SIC para requerir información de manera directa al validador centralizado.

BLIPBLIP, NEXVIA E INALAMBRIA

Plantean que el proyecto otorga a una persona jurídica privada —seleccionada por los PRST conforme a condiciones definidas por estos, pero financiada por los PCA e IT— la facultad de aprobar o rechazar las plantillas de contenido necesarias para cursar tráfico, sin que exista recurso administrativo contra sus decisiones. Advierten que quienes seleccionan y controla al validador son competidores directos de los agentes sometidos a su revisión.

Consideran que este esquema reproduce en el servicio de SMS, el modelo del administrador centralizado de la portabilidad, al establecer un tercero designado por los operadores con capacidad para determinar que mensajes pueden enviarse y con qué urgencia. En este contexto, formulan las siguientes objeciones:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

• Conflicto de interés y riesgo de captura regulatoria: el validador depende, para su selección y permanencia, de los competidores directos de los agentes que valida, mientras el tráfico A2P propio de los PRST quedaría exento de la validación exigida a los agentes independientes.
• Sobrecostos ajenos al régimen de remuneración: el costo de validación, sumado a los demás cargos asociados al canal, podría incrementar el precio por SMS por encima de su valor regulado en contravía del principio de costo eficiente más utilidad razonable.
• Intervención indebida en relaciones privadas: Trasladar al validador la fiscalización de la relación comercial entre un IT o PCA y sus clientes podría restringir la libre competencia y la libertad contractual, además de exponer información confidencial a un tercero que no debería tenerla.
• Indeterminación operativa: el proyecto no define con claridad el funcionamiento del validador (flujo de revisión de plantillas, integración por API, conciliación de tráfico con cada PRST, respeto de las TPS pactadas en la OBI y en los contratos de interconexión), lo que genera incertidumbre técnica y jurídica.
• Ausencia de garantías: el rechazo de una plantilla podría paralizar la operación sin que existan recursos de reposición o apelación, con afectación del debido proceso.

HABLAME

Plantea que quienes financian el validador debe participar en su gobierno. Mientras el artículo 18 atribuye su selección a los operadores, el artículo 6.13.1.2 asigna su financiación a los asignatarios de códigos cortos A2P. En consecuencia quienes pagan no participan en la elección del proveedor ni en la definición de la tarifa, situación que podría generar sobrecostos. Por ello propone que los asignatarios de código corto A2P tengan voz y voto en la selección del validador y en la fijación y revisión de su tarifa, con un tope y con costos verificables.

Asimismo, señala que las decisiones del comité no pueden crear obligaciones sin los controles correspondientes. El numeral 6.13.5.1.11 otorga carácter obligatorio a decisiones técnicas del Comité Técnico de Seguimiento recogidas en actas que, conforme al proyecto, no constituyen actos administrativos ni admiten recursos, mientras el artículo 16 exceptúa de publicación determinadas resoluciones.

A su juicio este esquema permitiría imponer cargas sin acto motivado, publicidad ni posibilidad de impugnación, en desconocimiento del debido proceso. En consecuencia, considera que toda obligación nueva debe establecerse mediante un acto administrativo motivado, publicado y susceptible de recursos, y que la excepción de publicación debe limitarse a aspectos estrictamente técnicos.

Respuesta CRC:

En esta sección fueron agrupados los comentarios generales presentados por **ALDEAMO**, **AMCHAM**, **ANDESCO**, **ANDI**, **ASOBANCARIA**, **BLIP BLIP**, **CAMPAIGN REGISTRY**, **CCIT**, **CLARO**, **COLOMBIA FINTECH**, **CRISTIAN CANTILLO**, **CLEARTECH**, **ETB**, **INETUM**, **INALAMBRIA**, **JULIO NULDEMAR, NEXVIA**, **SAEM**, **SINCH, SUMA**, **TRANSUNION**, **PTC** y **HABLAME,** así como

los comentarios generales que se desprenden del escrito conjunto presentado por **BLIPBLIP**, **NEXVIA** e **INALAMBRIA**. Revisadas dichas intervenciones, la Comisión identifica tendencias coincidentes que agrupa en los ejes temáticos que se desarrollan a continuación, no obstante, con el propósito de brindar mayor claridad al análisis, previo se expone la siguiente consideración técnica preliminar:

2.3.1 Consideración técnica preliminar

Del análisis integral de las observaciones recibidas, la CRC evidencia que una parte importante de las inquietudes formuladas por los participantes parte de una interpretación según la cual el sistema de información del validador centralizado se constituiría como un nuevo elemento funcional incorporado dentro de la arquitectura operativa de las redes de mensajería SMS, encargado de validar, autorizar, inspeccionar o intervenir en tiempo real, en el procesamiento de cada mensaje antes de su enrutamiento hacia el usuario final.

No obstante, es pertinente hacer las debidas aclaraciones sobre dicha interpretación, que de igual forma conllevarán a los ajustes en las secciones que corresponda en el Proyecto de Resolución y que se irán indicando de forma particular en el desarrollo de los ejes temáticos propuestos. Respecto al sistema planteado en el modelo regulatorio, se contempla una arquitectura funcional distribuida, en la cual el sistema de información del validador centralizado cumple funciones de administración, mantenimiento, sincronización y distribución de la base de información asociada al régimen de código corto A2P, SENDER ID y plantillas de contenido A2P, mientras que las actividades de procesamiento operativo del tráfico de SMS continúan siendo ejecutadas de manera autónoma por cada PRST dentro de sus propias plataformas de SMS. En consecuencia, la arquitectura proyectada desacopla expresamente la administración de la base de información del procesamiento del tráfico SMS, evitando incorporar un nuevo elemento operativo funcional dentro de la ruta de procesamiento de los mensajes.

Bajo este entendimiento, la CRC considera pertinente precisar los siguientes principios de arquitectura que orientan la propuesta regulatoria y sirven de fundamento para el análisis de las observaciones recibidas.

I. **El sistema de información del validador centralizado no hace parte del plano operativo de procesamiento del tráfico SMS**

El sistema de información del validador centralizado no constituye un elemento operativo funcional encargado del transporte, procesamiento, inspección, autorización o enrutamiento en tiempo real de los mensajes SMS. En consecuencia, no opera como un Centro de Servicios de Mensajes Cortos (SMSC), Gateway PCA, Proxy de señalización, elemento de inspección o similar, ubicado dentro de la ruta de procesamiento del tráfico de SMS.

Su función consiste exclusivamente en la administración, mantenimiento, sincronización y distribución de la base de información asociada al régimen de código corto A2P, SENDER ID y plantillas de contenido

A2P, que soporta los procesos de validación definidos en el modelo regulatorio, sin intervenir durante el procesamiento operativo de cada mensaje cursado por las redes de los operadores.

II. La arquitectura proyectada corresponde a un modelo distribuido basado en sincronización de información

El modelo de arquitectura proyectada se fundamenta en un modelo distribuido en el que el sistema de información del validador administra una base centralizada que contiene la información correspondiente a los diferentes registros habilitados dentro del ecosistema A2P. Mediante mecanismos de sincronización soportados en interfaces de interoperabilidad, esta información es distribuida hacia los PRST, permitiendo que cada operador disponga de una copia local permanentemente actualizada de los registros requeridos para ejecutar sus procesos de validación de manera autónoma y eficiente.

En consecuencia, la distribución y actualización de la base de información constituyen procesos independientes del procesamiento del tráfico de SMS, de manera que la sincronización de registros se mantiene funcionalmente desacoplada de la operación de las plataformas de mensajería de los operadores dentro de la arquitectura proyectada.

III. Las validaciones operativas continúan siendo realizadas por los PRST

La arquitectura proyectada mantiene las responsabilidades propias de los PRST respecto del tratamiento operativo del tráfico SMS, en este sentido, las verificaciones asociadas a códigos cortos, Sender ID, plantillas y demás elementos definidos en el modelo regulatorio deben ser ejecutadas por cada operador utilizando la información previamente sincronizada desde la base de información centralizada administrada por el sistema de información del validador.

Por consiguiente, el procesamiento de los mensajes no requiere de consultas transaccionales al sistema de información del validador para cada SMS cursado, sino de la utilización de información previamente almacenada y actualizada dentro de las plataformas de cada PRST, preservando la autonomía operacional de las redes y contribuyendo a mantener eficiencia y continuidad de la operación durante el procesamiento del tráfico.

IV. El sistema de información del validador administra información, no administra el tráfico

Las funciones atribuidas al sistema de información del validador se orientan a garantizar la integridad, consistencia, disponibilidad y sincronización de la información utilizada por los diferentes actores del ecosistema A2P, en consecuencia, su rol consiste en administrar los registros que soportan los procesos de validación, sin intervenir en las decisiones operativas asociadas al tratamiento de mensajes individuales ni sustituir las responsabilidades que le corresponden a los PRST durante la operación de sus redes.

Así mismo, la arquitectura proyectada no implica que el sistema de información del validador desempeñe funciones de inspección del contenido de los mensajes, análisis de identidad en tiempo real, monitoreo continuo del tráfico o procesamiento centralizado de comunicaciones, preservando de esta manera la separación funcional entre la administración de la información y la operación de las redes de telecomunicaciones.

2.3.2 Consideración general para el análisis de las observaciones

Con fundamento en los principios anteriormente expuestos, la CRC observa que varias de las inquietudes formuladas por los participantes, particularmente aquellas relacionadas con incrementos de latencia, consultas síncronas para cada mensaje, disminución del throughput de las plataformas de mensajería, afectaciones generalizadas derivadas de la indisponibilidad del sistema de información del validador o la incorporación de un nuevo elemento dentro del procesamiento operativo del tráfico SMS, se encuentran asociadas a interpretaciones que han sido abordadas y aclaradas en los cuatro puntos precedentes.

En consecuencia, el análisis de las observaciones desarrollado en los ejes temáticos siguientes toma como referencia lo expuesto en la ***Consideración técnica preliminar***, en la cual se brinda claridad en relación a que el sistema de información del validador tiene como propósito administrar y gestionar una base de información centralizada que debe ser sincronizada con las plataformas de los PRST, mientras que el procesamiento operativo del tráfico y las validaciones asociadas al tratamiento de cada SMS continúan siendo responsabilidad de los operadores, quienes deben utilizar para ello la información previamente sincronizada en sus respectivas plataformas.

2.3.3 Arquitectura funcional y alcance del sistema de información del validador

AMCHAM, **ANDESCO**, **ANDI**, **ASOBANCARIA**, **BLIP BLIP**, **CCIT**, **CLARO**, **CRISTIAN CANTILLO**, **COLOMBIA FINTECH**, **ETB**, **JULIO NULDEMAR**, **PTC**, **SINCH** y **TRANSUNION** coinciden en manifestar inquietudes respecto al alcance funcional del sistema de información del validador, particularmente en relación con su rol dentro de la arquitectura de red, conforme a la interpretación según la cual actuaría como un nuevo elemento operativo encargado de validar o inspeccionar en tiempo real, cada mensaje SMS antes de su enrutamiento hacía el usuario final, la posible duplicidad de funciones con los SMS Firewall, los SMSC y demás plataformas de control y seguridad implementadas por los operadores y el riesgo de que se incorpore como un nuevo intermediario dentro de la cadena de procesamiento del tráfico A2P.

Adicionalmente, solicitan precisar el alcance de las funciones del sistema de información del validador y las responsabilidades que continuarán siendo ejercidas por los PRST, especialmente en materia de validación de mensajes, autenticación de remitentes, aplicación de controles antifraude y operación de los elementos de red asociados al servicio de mensajería. Finalmente, las observaciones buscan aclarar si la incorporación del sistema de información del validador implica modificaciones en la arquitectura de red de los operadores o si su propósito se limita a administrar la información requerida para soportar

los procesos de validación que continúan realizándose dentro de las redes de los PRST. En conjunto, las inquietudes ponen de manifiesto la necesidad de diferenciar las funciones de gestión de información del sistema de información del validador frente a las funciones operativas de procesamiento del tráfico SMS.

Del análisis de las observaciones recibidas se evidencia que una parte importante de las inquietudes parte de la interpretación que constituye al sistema de información del validador como un nuevo elemento funcional encargado de intervenir directamente en el procesamiento operativo en tiempo real de cada mensaje SMS antes de su enrutamiento; no obstante, dicho escenario se aclara debidamente en la ***Consideración técnica preliminar*** observando que el rol del sistema de información del validador consiste en la administración de la base de información asociada al régimen de código corto A2P, SENDER ID y plantillas de contenido A2P, que proporciona soporte a los procesos de validación establecidos en el modelo regulatorio, sin intervenir durante el procesamiento operativo de los SMS cursados por las redes de los operadores.

En consecuencia, se brinda claridad en relación con que el sistema de información del validador no hace parte del plano operativo de procesamiento del tráfico SMS y como tal las decisiones operativas asociadas al tratamiento de cada SMS continúan siendo ejecutadas por los PRST a través de sus propias plataformas de mensajería, utilizando para ello la información previamente sincronizada desde la base de información centralizada administrada por el Validador. Bajo esta aproximación arquitectónica se aclara que el propósito del sistema de información del validador consiste en garantizar la existencia de una fuente única, consistente, actualizada y confiable de información sobre los agentes, marcas y plantillas de contenido contemplados en el modelo regulatorio, sin sustituir las funciones propias de los PRST ni asumir competencias inherentes a la operación de sus redes. De esta forma se opta por la separación funcional de la administración centralizada de información ejercida por el validador, de las propias de procesamiento de tráfico que continúan ejecutándose de forma distribuida por cada operador, conforme a sus plataformas, herramientas y capacidades tecnológicas.

En consecuencia, la CRC considera procedente acoger las observaciones orientadas a solicitar una mayor precisión respecto del rol y alcance funcional del sistema de información del validador, por lo que procede a realizar ajustes encaminados a brindar la debida claridad en los numerales 6.13.1.3.2., 6.13.1.5.10., 6.13.2.1.2., 6.13.2.1.5., 6.13.2.2.6., 6.13.4.5.2., 6.13.4.7.1. del Proyecto de Resolución.

2.3.4 Esquema de sincronización, interoperabilidad y desempeño

AMCHAM, **ANDESCO**, **CLARO**, **COLOMBIA FINTECH**, **ETB**, **INETUM**, **SINCH**, **SAEM**, **PTC**, **CRISTIAN CANTILLO** y **ANDESCO** manifiestan su preocupación al considerar que una interpretación según la cual cada mensaje SMS deba ser validado mediante una consulta síncrona al sistema de información del validador previo a su enrutamiento, incrementaría ostensiblemente los niveles de latencia del flujo de SMS, aumentaría los tiempos de procesamiento, reduciría la capacidad de las plataformas de mensajería, introduciría cuellos de botella operativos y comprometería el cumplimiento de los niveles de servicio requeridos para comunicaciones críticas, tales como códigos OTP, procesos de autenticación y notificaciones transaccionales. En este contexto, proponen la adopción de mecanismos

alternativos basados en cachés locales, sincronización por eventos, validaciones por sesión, procesos en batch o mecanismos de actualización incremental que permitan reducir el volumen de consultas en línea. Adicionalmente, solicitan que se precisen los esquemas de interoperabilidad, los protocolos de integración, los mecanismos de sincronización de información entre el sistema de información del validador y los PRST, los estándares tecnológicos que deberán emplearse, así como la posibilidad de incorporar soluciones interoperables, modulares y tecnológicamente neutrales que permitan la evolución futura del ecosistema sin imponer tecnologías, proveedores o implementaciones específicas.

A este respecto, la CRC considera pertinente precisar que conforme a lo expuesto en la ***Consideración técnica***, el sistema de información del validador administra una base central de información cuya data es distribuida hacia las bases de datos locales administradas por cada PRST mediante mecanismos de sincronización que podrán ser incrementales en tiempo real, periódicos, de sondeo u otros, y cuyo detalle técnico será debidamente puesto en consideración para su análisis y definición en el CTLFSM. En consecuencia, las verificaciones requeridas para el tratamiento operativo del tráfico de SMS se realizan de manera local, sobre las copias de las bases de datos previamente sincronizadas por cada PRST y sin que el procesamiento de cada mensaje dependa de una consulta en línea al Validador.

En este sentido, las preocupaciones relacionadas con eventuales incrementos sistemáticos de latencia, disminución del throughput de las plataformas SMSC, generación de múltiples consultas API por mensaje o afectaciones al procesamiento masivo del tráfico parten de una interpretación de la arquitectura que ha sido debidamente aclarada. La arquitectura distribuida proyectada tiene como principio de diseño que el sistema de información del validador actúe como administrador centralizado de la información y no como un componente transaccional integrado dentro de la ruta crítica del procesamiento de los mensajes; de esta manera, la sincronización de las bases de información ocurre como un proceso independiente de la operación de mensajería, preservando el desempeño de las plataformas existentes y manteniendo la autonomía técnica de los PRST para implementar internamente los mecanismos de consulta sobre sus propias bases de datos sincronizadas.

Por otra parte, la CRC considera pertinente mantener un enfoque de neutralidad tecnológica respecto de las implementaciones particulares que cada PRST adopte para administrar sus bases de datos locales, optimizar sus mecanismos de consulta o gestionar internamente el desempeño de sus plataformas. En efecto, el modelo regulatorio define los principios de la arquitectura funcional y de interoperabilidad requeridos para garantizar la consistencia, disponibilidad e integridad de la información dentro del ecosistema, sin imponer tecnologías propietarias, fabricantes específicos o diseños particulares de infraestructura. En este contexto, corresponde a cada operador implementar las soluciones tecnológicas que mejor se adapten a su arquitectura de red, siempre que aseguren la correcta sincronización de la información administrada por el sistema de información del validador y el cumplimiento de las obligaciones regulatorias establecidas.

En consecuencia, la CRC considera procedente acoger las observaciones orientadas a solicitar mayores precisiones sobre los aspectos relacionados con la sincronización, interoperabilidad y desempeño operacional del sistema de información del validador, por lo cual, se realizaron los ajustes

correspondientes sobre los numerales referidos en el eje temático 1, y adicionalmente, se hace una modificación complementaria sobre el numeral 6.13.1.5.10. del Proyecto Regulatorio.

2.3.5 Disponibilidad, resiliencia y continuidad operacional

ANDESCO, **ANDI**, **ASOBANCARIA**, **BLIPBLIP**, **CCIT**, **CLARO**, **COLOMBIA FINTECH**, **ETB**, **JULIO NULDEMAR**, **SAEM**, **SINCH**, **PTC**, **AMCHAM** e **INETUM** manifiestan su preocupación frente a la posibilidad de que el sistema de información del validador se convierta en un punto único de falla (Single Point of Failure - SPOF) para el ecosistema nacional de mensajería A2P, bajo esta interpretación, consideran que una eventual indisponibilidad, degradación de sus interfaces de integración APIs, incidentes de ciberseguridad o insuficiencias de capacidad podrían impedir el procesamiento de mensajes críticos tales como códigos OTP, procesos de autenticación, alertas financieras, mensajes de emergencia, servicios IoT y demás comunicaciones transaccionales cuya oportunidad resulta esencial para los usuarios y para múltiples sectores de la economía. En consecuencia, proponen fortalecer los mecanismos de continuidad operacional mediante la incorporación de esquemas de redundancia geográfica, planes de recuperación ante desastres, modalidades de operación degradada, mecanismos fail-safe, utilización de bases de datos o cachés locales, conservación temporal de validaciones previamente sincronizadas, incremento de los niveles de disponibilidad, establecimiento de parámetros objetivos de capacidad y definición de procedimientos específicos para garantizar la continuidad del servicio ante contingencias del sistema de información del validador.

A este respecto, la CRC considera pertinente precisar, conforme a lo expuesto en los ejes temáticos anteriores y la ***Consideración técnica***, que la arquitectura proyectada corresponde a un principio de separación entre la administración de la base de información centralizada y el procesamiento operativo del tráfico SMS, en consecuencia, se reitera que el sistema de información del validador no forma parte de la ruta crítica de procesamiento de los mensajes ni constituye un elemento funcional cuya disponibilidad condicione el envío individual de cada SMS. Conforme a lo previamente aclarado, el sistema de información del VALIDADOR administra una base de información centralizada que es sincronizada hacia las bases de datos locales de los PRST, sobre las cuales se deben realizan las validaciones de códigos cortos A2P, SENDER ID, plantillas de contenido A2P y demás dispuestas en el modelo regulatorio. Así, la indisponibilidad temporal del sistema de información del validador no implica, por sí misma, la imposibilidad de cursar el tráfico sustentado en información previamente sincronizada, toda vez que las validaciones operativas continúan efectuándose localmente sobre las copias disponibles en cada una de las redes de los PRST.

Bajo esta proyección de arquitectura distribuida, las observaciones que asocian de manera directa una eventual falla del Validador con la interrupción inmediata de toda la mensajería A2P parten de un supuesto que esta Comisión se ha permitido a aclarar en las secciones previas. Dado que sistema de información del validador no interviene de manera directa en el procesamiento transaccional de cada mensaje, no constituye un punto único de procesamiento de tráfico, no obstante, la CRC coincide con los participantes en la importancia de que la infraestructura encargada de administrar la base de información centralizada disponga de mecanismos adecuados de continuidad operacional, alta

disponibilidad, respaldo, recuperación ante desastres, monitoreo permanente y gestión de incidentes, conforme a lo expuesto en la SECCIÓN 2. REQUERIMIENTOS TÉCNICOS Y OPERATIVOS DEL SISTEMA DE VALIDACIÓN del Proyecto Regulatorio, toda vez que su continuidad operativa resulta relevante para garantizar la actualización oportuna de la información sincronizada entre las plataformas locales de los diferentes actores del ecosistema. En este sentido, las observaciones orientadas a fortalecer los requisitos de disponibilidad, resiliencia y continuidad constituyen un aporte valioso para el diseño operativo del modelo.

De igual forma, la CRC considera que los procedimientos de contingencia deben orientarse a preservar la continuidad del servicio ante eventos excepcionales, procurando que cualquier afectación temporal sobre la base de información centralizada o sobre los mecanismos de sincronización implique la menor afectación en el procesamiento de comunicaciones que, ante este tipo de situaciones, deberán ser soportadas en la información previamente sincronizada y disponible en las bases de datos locales de los PRST. En consecuencia, esta Comisión estima procedente mantener los mecanismos de disponibilidad y continuidad operacional asociados a la administración de la base de información centralizada, precisando los principios generales bajo los cuales se gestionarán los procesos de sincronización, recuperación y actualización de la información, y resaltando el modelo arquitectónico según el cual las validaciones operativas continúan siendo realizadas por los PRST sobre sus respectivas bases de datos locales.

Por lo expuesto, la Comisión acoge las observaciones encaminadas a fortalecer los mecanismos de disponibilidad, continuidad operacional, recuperación ante desastres y resiliencia asociados al sistema de información del validador y en esta dirección se fortalece el artículo 6.13.2.2 del proyecto de resolución, relativo al plan de contingencia del validador centralizado, por cuanto contribuyen a fortalecer la robustez operativa del ecosistema y a garantizar la actualización confiable, segura y oportuna de la información compartida entre sus diferentes actores.

En concreto, el artículo 6.13.2.2 se ajusta en los siguientes términos: (i) se amplía su ámbito de aplicación para comprender, además de las fallas totales o parciales del sistema principal, los eventos de degradación del servicio, los incidentes de seguridad de la información y cualquier otro evento que afecte o pueda afectar la disponibilidad, integridad, confidencialidad, capacidad o desempeño del sistema de información, y se exige que el plan se encuentre debidamente documentado, actualizado y probado; (ii) en el numeral 6.13.2.2.1 se precisa que la información disponible para consulta offline por parte de los PRST deberá estar sincronizada de manera continua, mantenerse en una infraestructura independiente o funcionalmente desacoplada del sistema principal y contar con mecanismos que permitan verificar su versión, la fecha y hora de la última actualización, su integridad y su vigencia; (iii) en el numeral 6.13.2.2.2 se tipifican los eventos que deben ser objeto de procedimientos diferenciados de identificación, clasificación, diagnóstico, escalamiento y atención, con definición de los tiempos máximos de recuperación y de los criterios de retorno a la operación normal; (iv) en el numeral 6.13.2.2.3 se define el contenido mínimo de la notificación de fallas y el deber de suministrar actualizaciones periódicas mientras persista la contingencia; (v) en el numeral 6.13.2.2.4 se incorpora la obligación de resincronizar la base de información con las bases locales de los PRST y del

Administrador de los Recursos de Identificación una vez restablecida la operación normal; (vi) en el numeral 6.13.2.2.6 se establece el acceso del Administrador de los Recursos de Identificación al plan de contingencia y a sus documentos asociados, mediante repositorio seguro o mecanismo tecnológico equivalente; y (vii) se adiciona el numeral 6.13.2.2.7, relativo al acceso a la información sobre disponibilidad, desempeño, capacidad y operación del sistema de validación, con la consiguiente renumeración del anterior numeral 6.13.2.2.7 como numeral 6.13.2.2.8.

De igual manera, y en atención a las observaciones sobre supervisión, neutralidad y trazabilidad del sistema de información del validador centralizado, se incorpora en los numerales 6.13.1.5.13 y 6.13.2.1.6 el acceso seguro, permanente y en tiempo real de la CRC a la información administrada por el validador centralizado, mediante API o mecanismo tecnológico equivalente. Este acceso permite al Administrador de los Recursos de Identificación verificar de manera directa el estado de los recursos de identificación y de las plantillas de contenido, sin necesidad de requerimientos individuales de información, y constituye una garantía adicional frente a las preocupaciones expresadas por los agentes sobre el control y la supervisión del validador centralizado.

2.3.6 Funciones técnicas del sistema de información del validador y alcance de las validaciones

ALDEAMO, ANDESCO, ANDI, ASOBANCARIA, BLIP BLIP, CCIT, CLARO, COLOMBIA FINTECH, ETB, INETUM, INALAMBRIA, JULIO NULDEMAR, CLEARTECH, CRISTIAN CANTILLO, SINCH, SUMA, PTC y NEXVIA presentan observaciones respecto al alcance funcional del sistema de información del validador al advertir el riesgo de que este pueda asumir funciones que excedan la administración de los registros asociados al ecosistema de mensajería A2P, convirtiéndose en un componente encargado de inspeccionar, interpretar, aprobar o rechazar el contenido de los mensajes antes de su envío al usuario final. En particular, se cuestiona la validación de plantillas de contenido, el tratamiento de mensajes dinámicos, las comunicaciones IoT, los códigos OTP, los mensajes de carácter regulatorio y demás comunicaciones cuyo contenido puede variar de manera permanente o responder a circunstancias operativas específicas.

De igual forma, **COLOMBIA FINTECH** y **CLEARTECH** consideran que el sistema de información del validador debería evolucionar hacia un sistema de inteligencia que incorpore capacidades avanzadas de detección y prevención del fraude tales como motores de reputación, análisis semántico, inteligencia artificial, señales dinámicas de riesgo e integración con fuentes nacionales e internacionales de información sobre amenazas. Por el contrario, de forma generalizada se recomienda que su función deba limitarse exclusivamente a la administración de información objetiva asociada a los identificadores habilitados para la prestación de servicios de mensajería A2P, evitando asumir competencias relacionadas con el análisis del contenido de las comunicaciones o la toma de decisiones operativas sobre el tráfico cursado por los PRST.

Al respecto, la Comisión considera necesario reiterar, conforme a lo expuesto en la ***Consideración técnica***, que las funciones atribuidas al sistema de información del validador se circunscriben a la

administración, mantenimiento, actualización y sincronización de la información requerida para soportar los procesos de validación previstos en el modelo regulatorio, en este sentido, el sistema de información del validador administra la base de información centralizada que contiene los registros asociados al régimen de códigos cortos A2P, SENDER ID, plantillas de contenido A2P y demás elementos previstos en el modelo, garantizando su integridad, consistencia y disponibilidad para la sincronización hacia las bases de datos locales administradas por los PRST. En consecuencia, se resalta que sus funciones no comprenden el procesamiento del tráfico de mensajería, la inspección del contenido de las comunicaciones, el análisis individual de cada SMS ni la adopción de decisiones operativas sobre el tratamiento, aceptación, rechazo o enrutamiento del tráfico cursado por las redes de los operadores.

En particular, la validación de plantillas debe entenderse como un mecanismo que se ejecuta de manera local en las plataformas de los PRST orientado a verificar la correspondencia entre la información previamente registrada y habilitada en las bases de información y el flujo de tráfico de SMS dentro del ecosistema, sin que ello implique que el sistema de información del validador ejerza funciones de censura, interpretación semántica o evaluación permanente del contenido de las comunicaciones.

De igual forma, la arquitectura proyectada no asigna al sistema de información del validador funciones propias de motores inteligentes de detección de fraude, sistemas de inspección profunda de tráfico, plataformas de inteligencia artificial o mecanismos de análisis dinámico en tiempo real. Lo anterior no impide que dichas capacidades puedan ser implementadas por los diferentes actores del ecosistema dentro del ámbito de sus competencias y responsabilidades, sin que esto altere la naturaleza funcional del sistema de información del validador ni modifique el principio arquitectónico según el cual este actúa como administrador de la información habilitante para los procesos de validación, sin intervenir directamente en la operación del servicio de mensajería.

Así mismo, como se ha expuesto en los ejes temáticos precedentes, la CRC considera pertinente mantener una separación funcional entre las actividades de administración de registros y operación de las redes de telecomunicaciones, esta delimitación permite preservar la neutralidad tecnológica de la arquitectura, evita concentrar funciones heterogéneas en un único componente y da lugar a la constitución de un modelo escalable y adaptable a futuras evoluciones del ecosistema que permitan la incorporación de nuevos mecanismos tecnológicos de gestión y mitigación del fraude sin modificar la función esencial del sistema de información del validador como administrador de la base de información centralizada. Bajo este enfoque, corresponde a los PRST ejecutar las validaciones operativas previstas en la regulación utilizando como insumo la información previamente sincronizada desde la base de información administrada por el Validador, y adoptar las medidas de seguridad, control y gestión de riesgos dentro de sus plataformas de mensajería.

La Comisión acoge las observaciones orientadas a brindar mayor claridad respecto del alcance funcional del sistema de información del validador y la distribución de responsabilidades entre este, los PRST y el Administrador de Recursos de Identificación, por cuanto ello contribuye a evitar interpretaciones que podrían extender indebidamente las competencias asignadas a dicho componente, en esta dirección, como se indicó en los ejes temáticos precedentes, se hicieron los respectivos ajustes sobre los numerales

6.13.1.3.2., 6.13.1.5.10., 6.13.2.1.2., 6.13.2.1.5., 6.13.2.2.6., 6.13.4.5.2., 6.13.4.7.1. y 6.13.1.5.10. del Proyecto de Resolución. Por el contrario, la CRC no considera procedente acoger aquellas observaciones que proponen ampliar sustancialmente las funciones del sistema de información del validador para convertirlo en un sistema integral de inteligencia antifraude, una plataforma de inspección permanente de tráfico, un mecanismo de análisis semántico o un motor de reputación basado en señales dinámicas de riesgo con capacidad para adoptar decisiones operativas sobre el curso de las comunicaciones, toda vez que dichas funciones desbordan la arquitectura proyectada en el modelo regulatorio y modificarían la naturaleza del sistema de información del validador que consiste en administrar y sincronizar la base centralizada de información de referencia para los procesos de validación ejecutados por los PRST.

2.3.7 Justificación institucional del Sistema de Información del Validador

AMCHAM, **ANDESCO**, **ETB**, **PTC** y **ALDEAMO** manifestaron que la CRC no justificó suficientemente la necesidad de incorporar la figura del validador centralizado dentro del modelo regulatorio propuesto. En particular, señalaron que el Análisis de Impacto Normativo no comparó adecuadamente esta alternativa frente a otras opciones, como fortalecer las capacidades del Administrador de Recursos de Identificación o mantener la administración directamente en cabeza de la CRC. Algunos intervinientes incluso indicaron que la creación de un componente adicional podría incrementar la complejidad operativa del ecosistema sin aportar beneficios proporcionales en materia de mitigación del fraude.

Al respecto, la Comisión considera pertinente precisar que la incorporación del sistema de información del validador responde a una necesidad funcional propia del modelo regulatorio diseñado para el ecosistema de mensajería A2P y no a la creación de una instancia adicional de administración de recursos de identificación o de control sobre las redes de telecomunicaciones.

En efecto, el esquema regulatorio propuesto incorpora nuevos elementos cuya administración requiere actividades permanentes de registro, validación, actualización, sincronización y disponibilidad de información, entre ellos los agentes habilitados, las relaciones entre los diferentes actores del ecosistema, las marcas (Sender ID), las plantillas de contenido A2P, los estados de validación y demás información necesaria para soportar los procesos de autenticación previstos en la regulación. El documento soporte establece que dicha información debe mantenerse en una base única, consistente, actualizada y permanentemente disponible, de forma que pueda ser sincronizada hacia las bases de datos locales de los PRST para la ejecución de las validaciones operativas dentro de sus propias redes.

Bajo este enfoque, el sistema de información del validador constituye un componente de soporte que permite garantizar la integridad, consistencia y trazabilidad de la información habilitante utilizada por todos los actores del ecosistema, evitando que cada proveedor mantenga registros independientes susceptibles de generar inconsistencias, duplicidades o diferencias respecto de la legitimidad de los remitentes, las marcas y las plantillas autorizadas. Precisamente por ello, la arquitectura propuesta separa las funciones de administración centralizada de la información de las funciones operativas de procesamiento del tráfico, las cuales continúan siendo ejecutadas exclusivamente por cada PRST dentro de su propia infraestructura tecnológica.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

¿Por qué no basta con fortalecer al Administrador de Recursos de Identificación?

Frente a las observaciones según las cuales estas actividades podrían ser asumidas directamente por el Administrador de Recursos de Identificación, la Comisión considera necesario diferenciar las funciones propias de la administración de los recursos de identificación de las actividades operativas requeridas para soportar el funcionamiento cotidiano del ecosistema A2P.

En efecto, el Administrador de Recursos de Identificación, es decir la CRC, conserva íntegramente las competencias regulatorias y administrativas relacionadas con la asignación, recuperación, suspensión y administración de los recursos de identificación, así como las actuaciones administrativas que le corresponden conforme al régimen vigente. En contraste, el sistema de información del validador desarrolla actividades permanentes de carácter técnico y operativo asociadas a la verificación documental, procesos de conocimiento del cliente (KYC), mantenimiento de registros, validación de plantillas, sincronización de información, disponibilidad de servicios de consulta en tiempo real y actualización continua de la información utilizada por los PRST durante la operación del ecosistema. El propio proyecto regulatorio establece expresamente que el Validador no tiene competencias de Administrador de Recursos de Identificación ni actúa en nombre de la CRC, conservándose plenamente diferenciadas ambas funciones.

En concreto, es importante dejar claro que el modelo regulatorio propuesto no implica la transferencia ni la delegación de competencias administrativas. En este sentido, el proyecto regulatorio establece expresamente que el validador centralizado no tiene competencias de Administrador de los Recursos de Identificación ni actúa en nombre de la CRC, y que sus funciones se limitan a actividades de naturaleza técnica, operativa y de verificación documental desarrolladas conforme a los lineamientos regulatorios expedidos por el Administrador de los Recursos de Identificación. Así mismo, se reitera que las decisiones de asignación, recuperación y devolución de los recursos de identificación continúan siendo competencia exclusiva de la CRC.

Así las cosas, fortalecer al Administrador de Recursos de Identificación no elimina la necesidad de contar con un componente especializado encargado de ejecutar las actividades permanentes de administración y mantenimiento de la información requeridas por el nuevo modelo regulatorio, sino que implicaría concentrar en una misma instancia funciones administrativas y actividades técnicas de naturaleza distinta, contrariando el principio de separación funcional que orienta la arquitectura propuesta.

Finalmente, frente a quienes plantean que estas actividades podrían ser desarrolladas directamente por la CRC, la Comisión considera que ello tampoco resulta consistente con la naturaleza de las funciones que demanda el modelo. Las actividades de validación documental, conocimiento del cliente, administración continua de registros, actualización permanente de plantillas, sincronización tecnológica con múltiples PRST, mantenimiento de interfaces de consulta en tiempo real y operación permanente de una plataforma tecnológica de alta disponibilidad corresponden a procesos de ejecución continua

que requieren capacidades operativas especializadas y disponibilidad permanente, distintas de las funciones regulatorias, de administración de recursos de identificación que corresponden a la Comisión.

En consecuencia, el modelo propuesto preserva la separación entre las funciones regulatorias ejercidas por la CRC, las funciones de administración de recursos de identificación y las actividades técnicas necesarias para administrar la información habilitante del ecosistema A2P. Esta distribución funcional permite mantener claramente delimitadas las responsabilidades de cada actor, fortalece la trazabilidad y consistencia de la información utilizada por el ecosistema y evita trasladar a la autoridad regulatoria actividades permanentes de operación tecnológica que no hacen parte de sus competencias institucionales.

2.3.8 Gobernanza, independencia y neutralidad del validador centralizado

ANDESCO, **ANDI**, **CCIT**, **BLIP BLIP**, **NEXVIA**, **INALAMBRIA** manifestaron inquietudes respecto de la gobernanza del validador centralizado, particularmente en relación con su independencia, neutralidad, posibles conflictos de interés, mecanismos de supervisión, transparencia en su actuación y continuidad del servicio.

Al respecto, la Comisión considera que el proyecto regulatorio incorpora un conjunto de salvaguardas orientadas a garantizar la independencia funcional y la adecuada gobernanza del validador centralizado. En particular, se establecen requisitos de selección, prohibiciones expresas para prevenir conflictos de interés, causales de terminación anticipada de la designación, obligaciones de transferencia ordenada de la información y los sistemas, así como mecanismos de seguimiento y coordinación con el Administrador de Recursos de Identificación, todo ello encaminado a asegurar la continuidad, imparcialidad y transparencia en el ejercicio de sus funciones.

En consecuencia, la Comisión no considera necesario incorporar medidas regulatorias adicionales sobre esta materia, por cuanto el proyecto ya contiene un marco de gobernanza suficiente para garantizar la independencia del validador centralizado y el adecuado desarrollo de sus funciones.

2.3.9 Modelo de selección, operación y garantías institucionales del validador centralizado

Con respecto a los comentarios realizados por **BLIP BLIP**, **CAMPAIGN REGISTRY**, **COLOMBIA FINTECH**, **NEXVIA**, **SAEM**, **SINCH**, **CLARO**, **ANDI**, **CCIT** y **PTC** en donde formularon observaciones relacionadas con el modelo de selección y operación del validador centralizado. En particular, manifestaron inquietudes respecto de la transparencia del procedimiento de selección, la independencia del operador seleccionado, la participación de los distintos actores del ecosistema, los criterios mínimos de experiencia e idoneidad, el esquema de financiación, la protección de la información administrada por el sistema, la distribución de responsabilidades entre los diferentes actores y las garantías de continuidad, supervisión y debido proceso durante su operación.

La Comisión considera que estas observaciones convergen sobre un mismo aspecto: la necesidad de que el modelo institucional del validador centralizado garantice independencia, neutralidad, transparencia y continuidad operacional. En ese sentido, la CRC acoge parcialmente los comentarios e incorpora ajustes en el artículo 17 «Proceso de Selección de validador centralizado» del proyecto de resolución con el propósito de fortalecer el esquema de selección, gobernanza y operación del validador centralizado.

Sobre el procedimiento de selección:

La Comisión considera que el proceso de selección del validador centralizado debe privilegiar, en primera instancia, la participación de los actores directamente involucrados en el ecosistema A2P, manteniendo al mismo tiempo mecanismos subsidiarios que permitan garantizar la entrada en operación del modelo dentro de los plazos regulatorios previstos. En consecuencia, el procedimiento se desarrollará conforme a las siguientes etapas:

1. **Registro de los Integradores Tecnológicos.** Los agentes que pretendan participar en el ecosistema A2P deberán encontrarse previamente registrados ante el Administrador de los Recursos de Identificación, particularmente en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos (RPCAI) y declararse como Integradores Tecnológicos, de conformidad con las disposiciones previstas en la presente resolución.

2. **Convocatoria para la selección del Validador**. Una vez culminado el proceso de registro, la CRC convocará a los Integradores Tecnológicos registrados para adelantar el proceso de selección del validador centralizado, definiendo previamente los requisitos mínimos de experiencia, capacidad técnica, independencia, solvencia, continuidad operacional y demás condiciones objetivas que deberán cumplir los candidatos, de conformidad con lo establecido en el artículo 6.13.1.3 de la Resolución 5050 de 2016 y el numeral 17.1.3 de la resolución «por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones».

3. **Participación voluntaria**. El proceso de selección se desarrollará con los Integradores Tecnológicos que manifiesten expresamente su interés en participar. Para tal efecto, no se exigirá un quórum mínimo de participación ni la concurrencia de una mayoría determinada de los Integradores registrados, evitando que la ausencia de algunos agentes impida el desarrollo del proceso.

4. **Plazo para la selección**. Los Integradores Tecnológicos contarán con un plazo determinado en la resolución para adelantar el procedimiento y seleccionar al validador centralizado, conforme a las condiciones establecidas por la CRC.

5. **Mecanismo subsidiario.** Si vencido dicho plazo no se logra seleccionar el validador centralizado o el procedimiento no cumple las condiciones objetivas definidas por la Comisión,

la facultad de selección será trasladada a los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM), quienes dispondrán del mismo plazo para adelantar dicho proceso.

6. **Intervención excepcional de la CRC**. En caso de que tampoco se logre efectuar la selección dentro del plazo previsto o no se satisfagan los requisitos establecidos por la regulación, la CRC adelantará directamente el procedimiento de selección correspondiente, con el fin de garantizar la implementación oportuna del modelo regulatorio y la continuidad del cronograma previsto para su entrada en operación.

7. **Inicio de la implementación.** Una vez seleccionado el validador centralizado, se dará inicio al cronograma de implementación previsto en la presente resolución, incluyendo las actividades de integración tecnológica, pruebas de interoperabilidad, migración de información, operación controlada y puesta en producción del sistema.

La Comisión considera que este procedimiento equilibra adecuadamente la participación de la industria con la necesidad de asegurar la implementación efectiva del modelo regulatorio, evitando que la falta de consenso entre los agentes impida la entrada en operación del sistema.

En virtud de los comentarios de **BLIP BLIP**, **CAMPAIGN REGISTRY**, **COLOMBIA FINTECH**, **NEXVIA**, **SAEM**, **SINCH**, **CLARO**, **ANDI**, **CCIT** y **PTC**, la Comisión acepta la necesidad de ajustar el artículo 17 «Proceso de Selección de validador centralizado» del proyecto de resolución, en el sentido de modificar las reglas del proceso, los actores responsables, los mecanismos subsidiarios para garantizar la continuidad del proceso de selección, los criterios de supervisión por parte de la CRC y las consecuencias derivadas del incumplimiento de los plazos o de las condiciones previstas en la regulación. No se acogen los comentarios dirigidos a aceptar que el validador centralizado no cuente con personería jurídica en Colombia o presencia, toda vez que la magnitud de las responsabilidades que esa persona jurídica asumirá son de tal importancia y relevancia que ameritan que exista un ente plenamente identificado y determinado, con presencia en Colombia, que responda por el cumplimiento de todas las obligaciones regulatorias que asumirá. Esto no implica que en el proceso de selección sean excluidos participantes internacionales, pero lo que se pretende garantizar es que el participante, sea nacional o internacional, tenga una presencia jurídica en Colombia que le permita responder y garantizar las cargas que eventualmente asumirá.

Sobre la financiación del modelo

Frente a las observaciones relacionadas con la financiación del validador centralizado, la Comisión considera que el modelo debe responder a los principios de eficiencia económica, recuperación de costos y utilidad razonable. En consecuencia, la remuneración del Validador deberá corresponder exclusivamente a los costos de implementación, operación, mantenimiento, seguridad y actualización tecnológica asociados al cumplimiento de las funciones previstas en la regulación, evitando subsidios cruzados o ventajas competitivas para cualquiera de los actores del ecosistema.

Así mismo, la CRC verificará la razonabilidad de dicho esquema de remuneración dentro del proceso de selección, validando que los costos reconocidos guarden correspondencia con las actividades efectivamente desarrolladas por el Validador.

Sobre la protección de la información

La Comisión también comparte la importancia de garantizar la adecuada protección de la información administrada por el validador centralizado. Por ello, el proyecto establece que la información administrada por este corresponde exclusivamente a aquella necesaria para soportar el funcionamiento del modelo regulatorio y deberá ser utilizada únicamente para las finalidades previstas en la regulación. En consecuencia:

- el Validador no podrá utilizar la información para fines comerciales;
- deberá implementar controles de seguridad de la información acordes con las mejores prácticas internacionales y con lo dispuesto en el artículo 5.1.2.3 del Capítulo 1 del Título V y en el Anexo 5.8 del Título de Anexos de la Resolución CRC 5050 de 2016, así como con aquellas normas que las modifiquen, adicionen o sustituyan;
- deberá preservar la confidencialidad de la información obtenida durante la operación del sistema;
- deberá garantizar la integridad, disponibilidad y trazabilidad de la información administrada; y
- deberá adoptar mecanismos que permitan la transferencia íntegra y segura de la información cuando finalice su designación.

De igual manera, la Comisión acoge parcialmente las observaciones relacionadas con la confidencialidad, tratamiento y protección de la información administrada por el validador centralizado. En consecuencia, se ajusta el numeral 6.13.1.3.5. con el fin de precisar que dicha información solo podrá ser utilizada para el cumplimiento de las funciones previstas en la regulación, prohibir su uso con fines comerciales o competitivos, reforzar las obligaciones de seguridad de la información y garantizar su entrega íntegra y segura al finalizar la designación del validador centralizado. Asimismo, se establece que este deberá sujetarse a las disposiciones sobre gestión de seguridad de la información previstas en el artículo 5.1.2.3 y en el Anexo 5.8 del Título de Anexos de la Resolución CRC 5050 de 2016.

Sobre la distribución de responsabilidades

Finalmente, la Comisión considera necesario reiterar que el proyecto mantiene claramente delimitadas las responsabilidades de los distintos actores:

- Los PRST continúan siendo responsables del procesamiento del tráfico, la ejecución de las validaciones operativas y el cumplimiento de las obligaciones regulatorias aplicables a sus redes.

- El validador centralizado responde exclusivamente por la administración del sistema de información, el cumplimiento de las obligaciones técnicas y contractuales que le correspondan y la adecuada prestación de los servicios asociados al modelo.
- La CRC conserva íntegramente las competencias relacionadas con la administración de los recursos de identificación, así como las funciones regulatorias, de seguimiento y supervisión previstas en la Ley 1341 de 2009.

En conclusión, se destaca que el validador centralizado no ejerce potestades regulatorias ni administrativas, no sustituye a la CRC ni al Administrador de los Recursos de Identificación y no adopta decisiones que modifiquen derechos u obligaciones de los agentes del mercado.

2.4 Bloqueo o etiquetado de mensajes

PTC

Afirma que el artículo 6.13.4.7.2 del Proyecto establece que, antes de enrutar cada mensaje A2P, el Proveedor de Redes y Servicios de Telecomunicaciones —PRST— deberá verificar en el sistema validador la existencia del código corto A2P, del *Sender ID* y de la plantilla vigente. En caso de que alguno de estos elementos no se encuentre registrado o validado, el PRST deberá bloquear el mensaje e impedir su entrega al usuario final o, **alternativamente, marcarlo con una etiqueta de «no verificado».**

Dice que la medida puede generar efectos adversos sobre la confianza del usuario. A su juicio, si un mensaje legítimo de autenticación, seguridad o prevención de fraude es marcado como «no verificado», el usuario puede interpretar que se trata de una comunicación fraudulenta, aun cuando provenga de un remitente legítimo. Afirma que lo descrito puede debilitar la confianza en los canales formales utilizados por entidades financieras, plataformas digitales, comercios, prestadores de servicios esenciales y remitentes globales.

En complemento de lo anterior, **PTC** indica que una señalización inconsistente o errónea podría ser aprovechada por actores maliciosos mediante esquemas de ingeniería social, ya que los defraudadores podrían explotar la confusión generada por mensajes legítimos etiquetados como «no verificados» para inducir al usuario a abandonar los canales oficiales y dirigirlo hacia canales alternativos menos seguros.

Por todo lo anterior, **PTC** recomienda que se ajuste la redacción del artículo 6.13.4.7.2 para incorporar salvaguardas que permitan equilibrar los objetivos de seguridad con la necesidad de garantizar la entrega oportuna de comunicaciones críticas. Finalmente, el PRST no debe asumir la responsabilidad de marcar la etiqueta como «No verificado» es un riesgo bastante critico que no puede recaer en discusión mediante regulación.

Respuesta CRC:

La CRC analizó el comentario presentado por **PTC** en relación con la regla prevista en el artículo 6.13.4.7.2 del proyecto de resolución, conforme a la cual, antes de enrutar cada mensaje A2P, el PRST debe verificar en el sistema del validador centralizado la existencia del código corto A2P, del SENDER ID y de la plantilla de contenido aprobada y vigente; y, en ausencia de alguno de estos elementos, debe bloquear el mensaje o, alternativamente, marcarlo con la etiqueta «sin verificar».

PTC advierte al respecto que la posibilidad de etiquetar mensajes como «no verificados» puede generar efectos adversos sobre la confianza del usuario. En particular, señala que, si un mensaje legítimo de autenticación, seguridad o prevención del fraude es marcado como «no verificado», el usuario podría interpretar que se trata de una comunicación fraudulenta, aun cuando provenga de un remitente legítimo, lo que podría debilitar la confianza en los canales formales utilizados por entidades financieras, plataformas digitales, comercios, prestadores de servicios esenciales y remitentes globales.

Sobre este punto, la CRC considera pertinente precisar que el propósito del sistema de validación centralizado no es únicamente registrar información o verificar formalmente la existencia de los elementos asociados al mensaje A2P. Su finalidad práctica es permitir que, a partir de dicha validación, se genere una consecuencia operativa efectiva frente al tráfico que no cumpla las condiciones mínimas de trazabilidad previstas en la regulación. En ese sentido, la verificación de la existencia y vigencia del código corto A2P, del SENDER ID y de la plantilla de contenido no constituye un fin en sí mismo, sino un mecanismo para impedir que comunicaciones que no cumplen los requisitos del esquema regulado sean cursadas hacia los usuarios como si fueran mensajes legítimos.

Ahora bien, en el proyecto publicado para comentarios, la CRC planteó dos posibles efectos frente a la ausencia de alguno de estos elementos: i) el bloqueo del mensaje, impidiendo su entrega al usuario final; o ii) permitir su entrega, pero con una etiqueta de «sin verificar». Esta segunda alternativa buscaba ofrecer al usuario información sobre el estado de verificación del mensaje y permitirle tomar una decisión frente a la comunicación recibida. No obstante, a partir del comentario de **PTC**, la Comisión encuentra que la opción del etiquetado en este caso particular puede generar riesgos no deseados sobre la confianza del usuario y sobre la efectividad misma de la medida.

En efecto, si un mensaje legítimo pero marcado como «sin verificar» es percibido por el usuario como sospechoso o fraudulento, la medida podría afectar la confianza en canales formales de comunicación. Adicionalmente, como lo menciona **PTC** en sus comentarios, existe el riesgo de que actores maliciosos exploten la confusión generada por este tipo de etiquetas mediante esquemas de ingeniería social, induciendo al usuario a desconfiar de comunicaciones legítimas o a migrar hacia canales alternativos menos seguros. Esta preocupación resulta consistente con lo señalado en el documento soporte, en cuanto advierte que el diseño de esquemas de etiquetado debe atender cuidadosamente la experiencia del usuario, pues un exceso de etiquetas negativas puede generar también fatiga o desconfianza.

Por lo anterior, la CRC acepta parcialmente el comentario de **PTC**, y en ese sentido, si bien mantiene la obligación de verificación previa como elemento esencial del sistema de trazabilidad y prevención del

fraude, considera procedente ajustar la consecuencia prevista para los mensajes que no cuenten con código corto A2P, SENDER ID o plantilla de contenido aprobada y vigente. En consecuencia, se modifica el numeral 6.13.4.7.2 para eliminar la alternativa de etiquetado «sin verificar» y se mantendrá únicamente el bloqueo del mensaje como efecto frente a la ausencia de cualquiera de los elementos exigidos.

Esta decisión permite preservar la finalidad central del esquema de validación: impedir que mensajes A2P no trazables o no validados lleguen al usuario final. Al mismo tiempo, evita trasladar al usuario la carga de interpretar el significado de una etiqueta negativa y reduce el riesgo de que dicha etiqueta sea utilizada de manera indirecta para generar confusión, desconfianza o escenarios de ingeniería social.

La CRC considera que, bajo el esquema ajustado, el usuario no deberá recibir mensajes A2P que no cumplan con los elementos mínimos de validación. De esta forma, el sistema se orienta a una regla más clara y protectora: cuando el mensaje no cuente con los elementos exigidos para acreditar su trazabilidad dentro del sistema —código corto A2P, SENDER ID y plantilla vigente—, el mensaje no será entregado al usuario final. Esta solución fortalece la seguridad jurídica de los agentes obligados, simplifica la operación para los PRST y ofrece una señal regulatoria más consistente con el objetivo de prevenir el contacto a usuarios con fines fraudulentos.

Teniendo en cuenta lo antes descrito, la CRC acepta parcialmente el comentario presentado por PTC y, en consecuencia, se reitera que se modifica el numeral 6.13.4.7.2 para eliminar la posibilidad de que el PRST permita la entrega del mensaje con la etiqueta «sin verificar» y se establecerá que, en ausencia de código corto A2P, SENDER ID o plantilla de contenido aprobada y vigente, el PRST deberá bloquear el mensaje e impedir su entrega al usuario final.

2.5 KYC

ANDI

Explica que, según el proyecto, el asignatario de SENDER ID (el PCA) inicia ante el asignatario de código corto A2P un proceso de KYC como cliente, obtiene la certificación y formaliza los contratos, y objeta que ello impone cargas administrativas desproporcionadas que no aportan seguridad al ecosistema.

Sostiene que el PCA queda sujeto a una habilitación previa ante un particular y a una certificación, con revisiones duplicadas (el asignatario del código corto examina al PCA y el validador vuelve a revisar ese examen), lo que constituye una barrera de acceso dependiente de la decisión de un tercero sin control estatal, que restringe la libre entrada, incrementa el riesgo de conductas discriminatorias y desincentiva la inversión.

Le preocupa que el proyecto exija identificar al beneficiario final con base en criterios de prevención del lavado de activos y financiación del terrorismo, pues incorporar estándares LA/FT en una regulación

antifraude por SMS puede generar ambigüedad jurídica, duplicidad y cargas desproporcionadas para empresas que no son sujetos obligados de ese régimen especializado. Añade que condicionar la asignación del SENDER ID a una certificación de KYC en un modelo centralizado puede convertirse en barrera de acceso, en especial para pequeñas empresas, desarrolladores, comercios electrónicos, startups y proveedores globales.

Finalmente, considera que el artículo 6.13.3.1.7 es excesivamente amplio al exigir conservar toda la información KYC por cinco años tras la terminación del contrato sin diferenciar tipos de datos, niveles de riesgo o necesidad probatoria, lo que incrementa los riesgos de seguridad y de exposición innecesaria de datos personales y empresariales sensibles.

ASOBANCARIA

Respalda la incorporación de la debida diligencia como control necesario, pero advierte que las entidades vigiladas por la SFC ya son objeto de comprobación permanente de su existencia, representación, estructura de propiedad, beneficiario final y perfil de riesgo, de modo que exigir a un agente privado rehacer esa verificación no añade seguridad y sí impone una carga redundante que multiplica la circulación de información sensible, en tensión con el principio de proporcionalidad. Señala que el propio proyecto reconoce la condición de entidad vigilada como criterio relevante (por ejemplo, al regular las plantillas de autenticación y transaccional en el artículo 6.13.4.2.7).

Solicita que, tratándose de entidades vigiladas por la SFC, el conocimiento del cliente pueda satisfacerse acreditando esa condición y la titularidad del signo distintivo, de modo que el validador y el asignatario del código corto A2P se apoyen en la información ya verificada por el supervisor natural, sin duplicar diligencias.

ANDESCO

Propone sustituir el validador centralizado con posición monopólica por un modelo en el que cada asignatario de código corto realice el KYC bajo estándares mínimos definidos por la CRC, con auditorías periódicas de la Comisión, manteniendo la responsabilidad en los agentes privados que tienen la relación contractual con los PCA, eliminando el punto único de falla, reduciendo costos y sin crear un nuevo actor regulatorio.

BLIPBLIP

Sostiene que el KYC corresponde a una relación contractual privada regida por la buena fe, la confidencialidad y la libre contratación, y advierte que centralizar su fiscalización en un tercero designado por los PRST puede generar conflictos por una posible posición de juez y parte. Añade que conocer al cliente no necesariamente mejora la calidad del tráfico ni reduce el fraude, por lo que la carga burocrática no aportaría a ese objetivo.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CCIT

Sostiene que, de acuerdo con el Proyecto de Resolución, los asignatarios de SENDER ID iniciarán ante los asignatarios de código corto A2P el proceso de KYC como clientes, obtendrán la certificación correspondiente y formalizarán los contratos requeridos. Frente a este modelo señala que el PCA asume la posición de cliente y debe ser examinado y certificado.

Al respecto, dice que el Proyecto de Resolución incluye cargas administrativas desproporcionadas y obligatorias para los PCA que no aportan seguridad al ecosistema y sí generan costos y demoras injustificadas para el PCA. Así, afirma que antes de acceder al SENDER ID, el PCA queda sujeto a un trámite de habilitación ante un particular y a la obtención de una certificación. El resultado, en su criterio, es la existencia de trámites excesivos sobre el mismo sujeto dado que el asignatario del código corto A2P examina al PCA y el validador vuelve a revisar ese examen.

Además, sostiene que la habilitación previa del PCA implica la imposición de barreras de acceso al mercado, que además depende de la decisión de un tercero particular. Esta subordinación operativa no solo restringe injustificadamente la libre entrada de nuevos competidores, sino que carece de control estatal directo, lo que incrementa el riesgo de conductas discriminatorias. Al condicionar la viabilidad comercial de un PCA a la discrecionalidad de un tercero independiente, se desincentiva la inversión en el sector y se ralentiza la adopción de innovaciones tecnológicas, perjudicando la eficiencia general del mercado de mensajería A2P.

Adicionalmente, afirma que es necesario evaluar la proporcionalidad de condicionar la asignación del SENDER ID a una certificación de KYC emitida dentro de un modelo centralizado. El proyecto establece que el KYC es condición necesaria para que el validador centralizado expida la certificación requerida para la asignación del SENDER ID. Este diseño puede convertirse en una barrera para el acceso al mercado, especialmente para pequeñas empresas, desarrolladores, comercios electrónicos, startups y proveedores globales que operan con múltiples intermediarios o modelos de mensajería transaccional.

Finalmente, indica que la redacción actual del artículo 6.13.3.1.7 resulta excesivamente amplia porque exige conservar la totalidad de la información KYC por cinco años después de la terminación del contrato, sin diferenciar entre tipos de datos, niveles de riesgo, existencia de incidentes, obligaciones legales específicas o necesidad probatoria. Ello puede implicar la retención prolongada de datos personales y empresariales sensibles, incluyendo información de representantes legales, documentos de identidad, beneficiarios finales, antecedentes, perfil de riesgo, información contractual y datos comerciales. Esta retención generalizada incrementa los riesgos de seguridad, acceso no autorizado, usos secundarios, duplicidad de bases de datos y exposición innecesaria de titulares y empresas a riesgos de seguridad.

COLOMBIA FINTECH

Indica que el artículo 6.13.3.1 replica controles que la SFC ya exige y supervisa sobre las entidades vigiladas (existencia jurídica, beneficiario final, perfil de riesgo), por lo que genera una carga administrativa redundante para entidades sometidas a SARLAFT, y que el numeral 19.1.2.5 reconoce la situación al priorizar a las entidades vigiladas, pero no simplifica el KYC. Solicita un régimen simplificado de KYC para las entidades vigiladas por la SFC que reconozca la supervisión existente como equivalente y evite la duplicación de cargas.

INALAMBRIA

Indica que utilizar el registro obligatorio de empresas que envían mensajes como la única dimensión para control de fraude es insuficiente e ineficaz. Señala que otras dimensiones de control de fraude como el origen de los mensajes (sin son generados por clientes local fácilmente identificables o clientes internacional difícilmente rastreables) o las particularidades de sus contenidos (contienen características específicas propias de fraude) podrían alinearse con la propuesta de Asobancaria, en donde resulta primordial contar con un compendio consolidado de las casuísticas más recurrentes que permitan analizar los principales patrones de fraude reportados.

NEXVIA

Manifiesta que los numerales 6.4.2.1.1 y 6.4.2.1.3 trasladan al PCA cargas que, por definición regulatoria, corresponden al Integrador Tecnológico. Afirma que la Resolución CRC 6522 es inequívoca, al señalar que el PCA «puede o no estar directamente conectado» con los PRST, y el IT es el agente «responsable de la provisión de infraestructura de conexión y de soporte entre los PRST y los PCA sin conexión directa». Argumenta que exigir al PCA la descripción de infraestructura técnica de conexión propia equivale a exigirle convertirse en IT, eliminando por vía de requisitos la categoría regulatoria del PCA sin conexión directa.

Adiciona que la exigencia constituye además un requisito adicional para el ejercicio de una actividad ya reglamentada, en tensión con el artículo 84 de la Constitución Política y una barrera de entrada nueva en un mercado donde el acceso ya es históricamente obstaculizado por los operadores, como lo acreditan los procesos de servidumbre tramitados por la propia Comisión. Frente a lo expuesto, propone la siguiente redacción:

> «6.4.2.1.1. Constancia de inscripción previa en el RPCAI, con indicación de la calidad en la que actúa el solicitante (PCA, IT, o ambas). 6.4.2.1.3. Descripción detallada del servicio o función que desempeñará como asignatario del código corto A2P. Cuando el solicitante actúe como Integrador Tecnológico o como PCA con conexión directa, incluirá la descripción de la infraestructura técnica de conexión con el o los PRST; cuando actúe como PCA sin conexión directa, indicará el o los Integradores Tecnológicos a través de los cuales cursará su tráfico y las relaciones de acceso de estos con los PRST.»

SAEM

Explica que el proyecto obliga al IT (asignatario de código corto A2P) a adelantar el KYC de cada PCA —identificación del agente y del beneficiario final, verificación del objeto social, perfil de riesgo, formalización contractual y conservación por cinco años, con debida diligencia continua (artículos 6.13.3.1 y 6.13.3.2)— y advierte que, aunque ya realiza debida diligencia, el proyecto eleva el estándar al del régimen de prevención del lavado de activos, duplicando información que ya reposa en el RPCAI, el RUES y el RUT, y superponiendo el KYC del IT con la verificación del validador.

Propone aprovechar e interoperar con el RPCAI, el RUES y el RUT para no duplicar verificaciones; delimitar el alcance del «beneficiario final» a umbrales razonables y a fuentes oficiales; precisar que el IT cumple su deber con la diligencia documental definida, sin convertirse en garante del comportamiento futuro del PCA; y escalonar la entrada en vigencia de la debida diligencia continua.

SEGUROS BOLÍVAR

Afirma que la obligación de señalar únicamente las plantillas aprobadas y vigentes implica que se deben fortalecer los acuerdos con los proveedores de BPO mediante otrosíes que incluyan ANS más exigentes, así como mecanismos de auditoria tecnológica y sanciones para garantizar su cumplimiento.

SINCH

Sostiene que la propia exigencia de crear y asignar un SENDER ID ya opera como un mecanismo robusto de autenticación, pues el solo hecho de que un cliente empresarial logre registrar y obtener ese identificador alfanumérico da certeza de que el originador es legítimo; por ello, exigir un KYC adicional sobre una empresa que ya cuenta con un identificador unívoco y regulado duplica esfuerzos sin añadir una capa proporcional de seguridad y contribuye a destruir el dinamismo del servicio SMS.

CLARO

Indica que es necesario que el proceso de conocimiento del cliente verifique también la existencia jurídica, vigencia y estado operativo activo de la persona jurídica, constatando que no se encuentre en estado de disolución, liquidación o inactividad pues se ha observado que estas empresas que están en estos estados envían tráfico presuntamente fraudulento.

Adicionalmente, señala que la medida supone un Onboarding más lento (KYC + validación + plantillas) y dependencia de un tercero (validador), de modo que la activación de un código o el proceso de venta se puede ralentizar por estas dependencias.

PTC

Afirma que, frente a las disposiciones contenidas en el artículo 6.13.3.1. por el cual se dispone el proceso de debida diligencia que deben surtir los asignatarios del código corto A2P respecto de cada agente con

quien celebren contratos para cursar tráfico A2P, con carácter previo al inicio de la relación contractual y de manera continua durante su vigencia, esta medida es indispensable en la reducción de eventos de fraude.

Agrega que es necesario que el responsable de la emisión de los contenidos realice un procedimiento de conocimiento del cliente, la identificación de tal persona es la única herramienta posible para determinar en grado de responsabilidad e investigación penal la persecución de aquellos delitos asociados con el fraude.

Sobre el particular, señala que doctrina especializada ha documentado que en los casos de estafas bajo modalidad de delito informático en su mayoría terminan con orden de archivo por parte de la Fiscalía General de la Nación, Carrizosa señala que: «*la Fiscalía General de la Nación afronta sus propios desafíos técnicos y de personal para investigar los delitos informáticos frente a la alta demanda investigativa cuyo resultado es que cerca del 95% de las denuncias de delitos informáticos hoy estén en la impunidad*» En ese sentido, agrega, identificar un posible responsable es objetivamente la forma de determinar la cadena final del presunto autor de conductas delictivas.

BLIPBLIP, NEXVIA E INALAMBRIA

Consideran que el KYC es, por naturaleza, una vinculación privada entre dos personas jurídicas sujeta a la libre contratación, y que dejar su fiscalización en manos de un centralizador —un tercero sin control legítimo sobre la información confidencial de los clientes— es conflictivo y mina los modelos de enrolamiento en línea. Concluyen que las medidas antifraude que requieren intervención sobre la relación comercial deberían recaer en las autoridades y, en lo operativo, articularse con esquemas basados en el comportamiento y la calidad del tráfico de cada agente, y no en una capa burocrática adicional de costo incierto.

Respuesta CRC:

Sobre esta temática se pronunciaron **ANDI**, **ANDESCO**, **ASOBANCARIA**, **BLIPBLIP**, **CCIT**, **CLARO**, **COLOMBIA FINTECH**, **INALAMBRIA**, **NEXVIA**, **PTC**, **SAEM**, **SEGUROS BOLÍVAR**, **SINCH** y, de manera conjunta, **BLIPBLIP**, **NEXVIA** e **INALAMBRIA**. Revisadas las intervenciones, la Comisión identifica las siguientes tendencias: (i) la caracterización del KYC como un trámite de habilitación previa ante un particular, que impondría barreras de acceso al mercado y duplicaría revisiones entre el asignatario del código corto A2P y el validador centralizado (**ANDI** y **CCIT**, en términos idénticos; **BLIP BLIP**; **ANDESCO**; y el escrito conjunto); (ii) los cuestionamientos a la identificación del beneficiario final y a la remisión a criterios de prevención del lavado de activos y de la financiación del terrorismo (**ANDI**, **CCIT**, **SAEM** y **COLOMBIA FINTECH**); (iii) las solicitudes de un tratamiento simplificado para las entidades vigiladas por la Superintendencia Financiera de Colombia (**ASOBANCARIA** y **COLOMBIA FINTECH**); (iv) las objeciones al plazo de conservación de la información previsto en el numeral 6.13.3.1.7 (**ANDI** y **CCIT**); (v) las solicitudes de interoperación con registros públicos, de delimitación del alcance del deber de diligencia y de escalonamiento de la debida diligencia continua (**SAEM**); (vi)

la tesis según la cual el KYC sería innecesario o inefectivo frente al fraude (**SINCH**, **BLIP BLIP** e **INALAMBRIA**); y (vii) comentarios individuales de **NEXVIA**, **CLARO**, **SEGUROS BOLÍVAR** y **PTC** que se responden de manera independiente.

La Comisión responde cada tendencia a continuación, no sin antes fijar el entendimiento general de la medida, que orienta todas las respuestas de este capítulo.

2.5.1 Naturaleza jurídica del proceso de conocimiento del cliente: precisión general

En el documento soporte, la Comisión justificó el proceso de conocimiento del cliente como el mecanismo mediante el cual el asignatario del código corto A2P verifica que los agentes cuyos contenidos cursa son personas jurídicas válidamente constituidas y legalmente identificables, de modo que solo empresas verificadas puedan originar campañas de mensajería, cerrando preventivamente la puerta al uso del canal por empresas fantasma o estructuras de fachada. El artículo 6.13.3.1 propuesto materializa esa finalidad exigiendo, con carácter previo al inicio de la relación contractual y de manera continua durante su vigencia, la identificación del agente y de su beneficiario final, la verificación del objeto social, la acreditación del derecho al uso del identificador, la evaluación del perfil de riesgo, la formalización contractual y la conservación de la información.

A partir de este marco, la Comisión precisa el entendimiento correcto de la medida, pues buena parte de las objeciones recibidas parte de una premisa que no corresponde a su diseño. Así, el KYC no es una habilitación previa para el ejercicio de una actividad económica, ni un trámite de autorización ante un particular. Se trata de una carga de debida diligencia que las partes de una relación contractual privada (el asignatario del código corto A2P y el agente que pretende cursar tráfico a través de él) deben satisfacer en la etapa precontractual, como presupuesto para formalizar la relación, y durante su ejecución, como condición para continuarla. Dicha carga no difiere, en su estructura, de los deberes de verificación que la buena fe precontractual impone en cualquier relación negocial en la que una parte pone a disposición de otra un recurso cuya utilización puede comprometer su propia responsabilidad; su particularidad consiste, únicamente, en que la regulación estandariza su contenido mínimo, en atención al interés público comprometido en el uso de los recursos de identificación administrados por el Estado. El asignatario del código corto A2P no «habilita» al PCA ni ejerce discrecionalidad administrativa alguna. Por el contrario, verifica documentalmente una identidad, celebra un contrato y conserva los soportes. Correlativamente, ninguna de las verificaciones del artículo 6.13.3.1 comporta juicios de conveniencia comercial librados a la discrecionalidad del verificador: sus elementos son objetivos, tasados y documentales.

En cuanto a su finalidad, la Comisión reitera que el KYC persigue un único propósito que es identificar de manera confiable a la persona jurídica, y a la persona natural que en última instancia la controla, que se encuentra detrás de cada generador de contenido, para dar transparencia y trazabilidad a la cadena de valor ante una eventual asignación de responsabilidad administrativa o judicial. Como lo destaca **PTC** en su intervención, cuya posición la Comisión comparte, la identificación cierta del

responsable de los contenidos es la herramienta que permite que las conductas fraudulentas no queden en la impunidad. Sin ella, la trazabilidad técnica del tráfico conduce a un extremo de la cadena en el que no hay nadie identificable a quien imputar la conducta.

2.5.2 Sobre la supuesta habilitación previa, las barreras de acceso y la duplicidad de revisiones (ANDI, CCIT, BLIPBLIP, ANDESCO y escrito conjunto)

ANDI y **CCIT** sostienen, en términos idénticos, que el PCA queda sujeto a un trámite de habilitación ante un particular y a la obtención de una certificación, que el asignatario del código corto examina al PCA y el validador vuelve a revisar ese examen, y que la subordinación de la viabilidad comercial del PCA a la decisión discrecional de un tercero sin control estatal restringe la libre entrada, incrementa el riesgo de conductas discriminatorias y desincentiva la inversión. **BLIPBLIP** y el escrito conjunto agregan que el KYC corresponde a una relación contractual privada regida por la libre contratación, cuya fiscalización por un centralizador designado por los PRST resulta conflictiva y mina los modelos de enrolamiento en línea. **ANDESCO**, por su parte, propone sustituir el modelo por uno en el que cada asignatario de código corto realice el KYC bajo estándares mínimos definidos por la CRC, con auditorías periódicas de la Comisión.

La Comisión no acepta estas solicitudes, con fundamento en la precisión general que ya se hizo y en las siguientes consideraciones adicionales. Primera, la premisa de la doble revisión es inexacta. El diseño del proyecto distribuye funciones que no se superponen. El asignatario del código corto A2P adelanta el KYC, esto es, ejecuta la verificación documental y celebra el contrato, mientras que el validador centralizado no rehace ese examen, sino que constata su realización como presupuesto para expedir la certificación requerida para la asignación del SENDER ID, conforme a los artículos 6.13.3.1 y 6.12.2.1.8. Se trata de una única diligencia con un único ejecutor, sujeta a una constatación de existencia por parte del validador, cuya razón de ser es dotar de uniformidad y confiabilidad al insumo con el que la CRC, no el validador, asigna el recurso. Segunda, la asignación del SENDER ID es y sigue siendo una decisión de la CRC como Administrador de los Recursos de Identificación, en ejercicio de los numerales 12 y 13 del artículo 22 de la Ley 1341 de 2009; ni el asignatario del código corto ni el validador deciden el acceso al recurso, de modo que no existe la subordinación de la viabilidad comercial del PCA a la voluntad de un particular que alegan los agentes.

Los desacuerdos que surjan en la ejecución del KYC son controversias contractuales entre privados, y las inconformidades frente a la actuación del validador cuentan con los mecanismos de supervisión descritos en el proyecto de resolución. Tercera, en cuanto a la propuesta de **ANDESCO**, la Comisión advierte que el modelo que describe (KYC ejecutado por cada asignatario de código corto bajo estándares mínimos definidos por la CRC) es, en lo sustancial, el modelo adoptado por el proyecto. En efecto, el artículo 6.13.3.1 radica la ejecución del KYC en los asignatarios y estandariza su contenido mínimo; la diferencia se reduce al rol de constatación del validador, que ya fue explicado. Cuarta, la afirmación de que la carga mina los modelos de enrolamiento en línea no se compadece con el contenido de la obligación, que es compatible con procesos de verificación digital. Ninguna disposición del proyecto exige presencialidad, soportes físicos ni tiempos muertos, y los documentos requeridos, certificado de

existencia y representación, documento de identidad, RUT, constancia RPCAI, son verificables por medios electrónicos.

2.5.3 Sobre la identificación del beneficiario final y la remisión a criterios de prevención del lavado de activos (ANDI, CCIT, SAEM y COLOMBIA FINTECH)

ANDI y **CCIT** expresan preocupación porque el numeral 6.13.3.1.2 exige la identificación del beneficiario final mediante un formato elaborado por el validador «con base en criterios de identificación del beneficiario en materia de prevención del lavado de activos y financiación del terrorismo», lo que a su juicio incorporaría estándares LA/FT en una regulación de fraude por SMS, generando ambigüedad, duplicidad regulatoria y cargas desproporcionadas para empresas que no son sujetos obligados de ese régimen. **SAEM** afirma que el proyecto eleva el estándar del KYC al nivel del régimen de prevención de lavado de activos y solicita delimitar el alcance del beneficiario final a umbrales razonables y fuentes oficiales. **COLOMBIA FINTECH** solicita aclarar el estándar aplicable y reconocer las declaraciones ya presentadas ante la UIAF.

La Comisión precisa que el proyecto no incorpora, extiende ni replica el régimen de prevención del lavado de activos y de la financiación del terrorismo, ni convierte a los agentes del ecosistema A2P en sujetos obligados de dicho régimen. La remisión del numeral 6.13.3.1.2 tiene un alcance estrictamente instrumental y acotado: el concepto de beneficiario final, la persona natural que en última instancia ejerce el control sobre la persona jurídica, es una noción cuya técnica de identificación ha sido desarrollada con mayor madurez en ese ámbito, y el proyecto se limita a ordenar que el formato de declaración se construya tomando como referencia esos criterios de identificación, no que se apliquen las metodologías, los sistemas de administración de riesgo, los reportes ni las consecuencias propias del régimen LA/FT. La finalidad, como se precisó en líneas precedentes, es una sola: que detrás de cada generador de contenido exista una persona natural identificada e identificable, de modo que las estructuras societarias no puedan utilizarse como pantalla para diluir la responsabilidad por el uso fraudulento del canal. El estándar exigido es, por tanto, el de una declaración documental de titularidad y control, sustancialmente menos intenso que la debida diligencia LA/FT, y no comporta evaluación de fuente de fondos, monitoreo transaccional financiero ni reporte a la UIAF.

No obstante, la Comisión acepta parcialmente estos comentarios en cuanto evidencian que la redacción del numeral 6.13.3.1.2 puede inducir el equívoco que los agentes señalan. En consecuencia, se ajusta dicho numeral para precisar: (i) que la identificación del beneficiario final tiene como única finalidad la individualización de la persona natural que ejerce el control sobre el agente contratante, para efectos de la transparencia y trazabilidad de la cadena de valor del tráfico A2P; (ii) que la referencia a los criterios de identificación del beneficiario final desarrollados en materia de prevención del lavado de activos opera exclusivamente como parámetro técnico para la elaboración del formato de declaración, sin que ello convierta a los agentes en sujetos obligados de dicho régimen ni les imponga obligaciones adicionales a la declaración; y (iii) que el formato podrá aceptar como soporte la información de beneficiario final que el agente ya haya reportado ante autoridades competentes en virtud de otros regímenes, cuando aquella se encuentre vigente, precisión con la cual queda atendida la solicitud de

COLOMBIA FINTECH sin necesidad de remitir la regulación sectorial a los registros de un régimen ajeno.

2.5.4 Sobre el tratamiento de las entidades vigiladas por la Superintendencia Financiera de Colombia (ASOBANCARIA y COLOMBIA FINTECH)

ASOBANCARIA respalda la incorporación de la debida diligencia como control necesario para la integridad del ecosistema, pero advierte que las entidades vigiladas por la SFC son objeto de comprobación permanente de su existencia, representación, estructura de propiedad, beneficiario final y perfil de riesgo en el marco de la supervisión estatal, por lo que exigir que un agente privado rehaga esa verificación impone una carga redundante y multiplica la circulación de información sensible; solicita que, respecto de dichas entidades, el KYC pueda satisfacerse mediante la acreditación de la condición de vigilada y de la titularidad del signo distintivo. **COLOMBIA FINTECH** coincide y solicita un régimen simplificado que reconozca la supervisión existente como equivalente, anotando que el numeral 19.1.2.5 del régimen de transición prioriza a las vigiladas, pero no simplifica el proceso.

La Comisión acepta este comentario pues la observación es técnica y jurídicamente fundada. Los elementos que el artículo 6.13.3.1 ordena verificar (existencia jurídica, representación, beneficiario final y perfil de riesgo) son objeto de comprobación permanente por parte del supervisor estatal respecto de las entidades sometidas a su inspección y vigilancia, de modo que la repetición íntegra de esas diligencias por un agente privado no añade seguridad al esquema y sí genera una carga redundante y una circulación innecesaria de información sensible, en tensión con el principio de proporcionalidad. El propio proyecto reconoce la condición de entidad vigilada como criterio de graduación del control, como lo evidencia el tratamiento de las plantillas de autenticación y transaccionales del artículo 6.13.4.2.7 y la priorización del numeral 19.1.2.5 del régimen de transición (ahora numeral 18.1.2.5).

En consecuencia, se adiciona un parágrafo al artículo 6.13.3.1 conforme al cual, tratándose de agentes contratantes que acrediten su condición de entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia, el validador centralizado y los asignatarios de código corto A2P podrán aplicar un proceso de conocimiento del cliente simplificado y más flexible, en el cual las obligaciones de los numerales 6.13.3.1.1, 6.13.3.1.2, 6.13.3.1.3 y 6.13.3.1.5 se entenderán satisfechas con la acreditación de dicha condición de vigilada, de la existencia y representación legal, y de la titularidad del signo distintivo cuyo registro como SENDER ID se pretende, apoyándose en la información ya verificada en el marco de la supervisión estatal. En todo caso, se mantendrán respecto de estas entidades la formalización contractual del numeral 6.13.3.1.6, la conservación de la información del numeral 6.13.3.1.7 y la debida diligencia continua del artículo 6.13.3.2, en lo que resulte compatible con el esquema simplificado, pues dichas obligaciones no duplican verificación alguna del supervisor y son necesarias para la operación del régimen de plantillas y monitoreo.

2.5.5 Sobre el plazo de conservación de la información del numeral 6.13.3.1.7 (ANDI y CCIT)

ANDI y **CCIT** consideran que la obligación de conservar la totalidad de la información del KYC por cinco años contados desde la terminación del contrato es excesivamente amplia, al no diferenciar tipos de datos, niveles de riesgo, existencia de incidentes o necesidad probatoria, y que la retención prolongada de datos sensibles incrementa los riesgos de seguridad, accesos no autorizados y usos secundarios.

La Comisión no acepta este comentario en la medida en que la conservación de la información del KYC no es una retención caprichosa ni indeterminada. Su finalidad, expresamente funcional, es garantizar que la información de identificación de la cadena de valor esté disponible para las autoridades administrativas y judiciales que la requieran en eventuales procesos futuros (actuaciones de recuperación de recursos, investigaciones administrativas o procesos penales asociados a fraudes), procesos que, por su naturaleza, se inician y desarrollan con posterioridad a los hechos y, con frecuencia, con posterioridad a la terminación de la relación contractual bajo cuyo amparo se cursó el tráfico investigado. Una regla que autorizara la depuración anticipada de los soportes según valoraciones del propio obligado sobre el nivel de riesgo o la existencia de incidentes vaciaría la utilidad probatoria del esquema, pues precisamente los eventos que interesan a las autoridades son aquellos que no fueron detectados como incidentes en su momento. El plazo de cinco años es, además, razonable y proporcionado frente al horizonte temporal de las acciones administrativas y judiciales que pueden requerir la información, y coincide con el término definido en el documento soporte al justificar la medida. Finalmente, la preocupación por la seguridad de la información conservada encuentra respuesta en el régimen de protección de datos personales de la Ley 1581 de 2012, de aplicación imperativa y directa a los responsables y encargados del tratamiento, cuyos principios de seguridad, confidencialidad, acceso y circulación restringida gobiernan la custodia de estos soportes, sin necesidad de reproducción en la regulación sectorial, conforme se explicó en la sección de respuesta a comentarios generales. La información conservada solo puede suministrarse al validador y al Administrador de los Recursos de Identificación cuando sea requerida, como lo dispone el propio numeral 6.13.3.1.7, lo que delimita el círculo de acceso.

2.5.6 Sobre la interoperación con registros públicos, el alcance del deber de diligencia y el escalonamiento de la debida diligencia continua (SAEM)

SAEM solicita: (i) permitir el aprovechamiento e interoperación con el RPCAI, el RUES y el RUT para no duplicar verificaciones; (ii) delimitar el alcance del beneficiario final a umbrales razonables y fuentes oficiales; (iii) precisar que el integrador tecnológico cumple su deber con la diligencia documental definida, sin convertirse en garante del comportamiento futuro del PCA; y (iv) escalonar la entrada en vigencia de la debida diligencia continua.

Frente al punto (i), la Comisión precisa que no existe la duplicación alegada: los documentos que el numeral 6.13.3.1.1 ordena verificar son, justamente, los expedidos por o inscritos en los registros que menciona el agente, de modo que el KYC no exige recaudar información paralela a la de dichos registros, sino apoyarse en ellos como fuentes oficiales de verificación. Nada en el articulado impide que la consulta se realice por medios electrónicos e interoperables, y así se entiende. El punto (ii) queda resuelto con el ajuste aclarativo del numeral 6.13.3.1.2 descrito en este capítulo. Frente al punto (iii),

la Comisión acoge el entendimiento propuesto, que corresponde al diseño del proyecto: las obligaciones del artículo 6.13.3.1 son deberes de diligencia de contenido determinado (verificación documental, formalización contractual, conservación), no obligaciones de garantía sobre la conducta futura del agente contratante; la responsabilidad del asignatario del código corto A2P frente al uso indebido posterior se rige por las reglas de imputación del régimen de atribución de responsabilidad, que exigen valorar el cumplimiento de sus propios deberes, tal como se explicó en el capítulo denominado «Atribución de responsabilidad», al cual se remite. Dado que este entendimiento se desprende del texto propuesto, no se requiere modificación del articulado, sin perjuicio de que la presente respuesta fije su interpretación auténtica para efectos de la aplicación del régimen. Finalmente, el punto (iv), relativo al escalonamiento temporal de la debida diligencia continua, corresponde a la secuencia de implementación del nuevo régimen y se aborda en el capítulo denominado «Régimen de transición», al cual se remite.

2.5.7 Sobre la supuesta falta de necesidad o inefectividad del KYC (SINCH, BLIPBLIP e INALAMBRIA)

SINCH sostiene que la asignación del SENDER ID ya operaría como mecanismo robusto de autenticación del originador, de modo que exigir adicionalmente un KYC duplicaría esfuerzos sin añadir seguridad proporcional. **BLIPBLIP** considera que conocer al cliente no necesariamente mejora la calidad del tráfico ni reduce el fraude. **INALAMBRIA** plantea que el registro de las empresas remitentes es insuficiente como única dimensión de control y que deben privilegiarse dimensiones como el origen del tráfico y las características del contenido, junto con un compendio consolidado de casuísticas de fraude.

La Comisión no acepta la tesis de **SINCH** ya que la confiabilidad del SENDER ID como identificador del originador depende, precisamente, de que la identidad declarada haya sido verificada. En el diseño del proyecto, la certificación que el validador expide para la asignación del SENDER ID tiene como condición necesaria la realización del KYC (artículos 6.13.3.1 y 6.12.2.1.8); suprimido este, el SENDER ID se reduciría a una autodeclaración de identidad sin verificación subyacente, que es exactamente la vulnerabilidad que las modalidades de suplantación explotan. El recurso identifica; el KYC es lo que garantiza que la identificación sea veraz. Por la misma razón se rechaza la apreciación de **BLIPBLIP**: el KYC no pretende, por sí solo, mejorar la calidad del tráfico (función que cumplen el monitoreo y el régimen de plantillas), sino asegurar que exista un responsable identificado detrás de cada flujo de tráfico, presupuesto de toda asignación de responsabilidad y disuasivo directo del uso del canal por estructuras anónimas. En cuanto a **INALAMBRIA**, la Comisión coincide en que la identificación del remitente no es la única dimensión del control, y por ello el proyecto la articula con el monitoreo de tráfico, el régimen de plantillas, las medidas sobre tráfico P2P y los mecanismos de coordinación, pero rechaza que ello reste necesidad al KYC. Las dimensiones son complementarias y no sustitutivas. La propuesta de construir un compendio consolidado de las casuísticas de fraude más recurrentes es valorada positivamente y encuentra su cauce institucional en las funciones de intercambio de información e inteligencia del CTLFSM, instancia a cuya consideración la Comisión la llevará, conforme a lo expuesto en el capítulo correspondiente.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.5.8 Comentarios individuales

NEXVIA sostiene que los numerales 6.4.2.1.1 y 6.4.2.1.3, al exigir al solicitante del código corto A2P la descripción de su infraestructura técnica de conexión, trasladan al PCA cargas propias del integrador tecnológico, eliminan por vía de requisitos la categoría del PCA sin conexión directa y configuran un requisito adicional para el ejercicio de una actividad reglamentada, en tensión con el artículo 84 de la Constitución Política, para lo cual propone una redacción alternativa que distinga según la calidad en la que actúe el solicitante. Así planteada, esta Comisión no acepta la referida propuesta, por partir de una premisa que no corresponde al diseño del proyecto. En el nuevo régimen, el código corto A2P se concibe como el recurso de identificación del agente que cuenta con conexión directa a las redes de los PRSTM, sea integrador tecnológico o PCA con conexión directa, mientras que el PCA sin conexión directa no requiere ser asignatario de código corto A2P, pues accede al canal a través de un asignatario de dicho recurso y se identifica mediante su SENDER ID. En consecuencia, la exigencia de describir la infraestructura de conexión no elimina la categoría del PCA sin conexión directa ni le impone convertirse en integrador: simplemente no le resulta aplicable, porque dicho agente no es destinatario del trámite de asignación del código corto A2P. La hipótesis que la redacción alternativa pretende regular (un PCA sin conexión directa solicitando código corto A2P) es ajena a la arquitectura del nuevo régimen. Tampoco se configura la tensión alegada con el artículo 84 constitucional, pues no se trata de requisitos adicionales para el ejercicio de una actividad, sino de los requisitos de asignación de un recurso escaso administrado por el Estado, cuya definición corresponde a la CRC en ejercicio de los numerales 12 y 13 del artículo 22 de la Ley 1341 de 2009.

CLARO solicita que el proceso de conocimiento del cliente verifique también la existencia jurídica, vigencia y estado operativo activo de la persona jurídica, constatando que no se encuentre en estado de disolución, liquidación o inactividad, pues se ha observado tráfico presuntamente fraudulento originado en empresas en tales estados; y advierte que la secuencia KYC–validación–plantillas puede ralentizar la activación de códigos y los procesos de venta. Frente a lo primero, la Comisión acepta el comentario, cuya finalidad es coherente con el diseño del régimen. Si bien el certificado de existencia y representación legal con vigencia no superior a noventa días, exigido por el numeral 6.13.3.1.1, da cuenta del estado de la persona jurídica, y el proyecto contempla como causal de recuperación la imposibilidad del asignatario de continuar ejerciendo su objeto social, resulta pertinente eliminar cualquier duda interpretativa. En consecuencia, se ajusta el numeral 6.13.3.1.1 para señalar expresamente que la verificación de identidad comprende la constatación de que la persona jurídica contratante se encuentra activa y no incursa en estado de disolución o liquidación. Frente a lo segundo, la preocupación por los tiempos de activación corresponde a los plazos y niveles de servicio del validador y del régimen de plantillas, abordados en los capítulos denominados «Validador centralizado: forma de selección, competencias y funciones» y «Plantillas (Template ID)», a los cuales se remite.

SEGUROS BOLÍVAR señala que la obligación de cursar tráfico únicamente mediante plantillas aprobadas y vigentes implicará fortalecer los acuerdos con sus proveedores de BPO mediante otrosíes con acuerdos de niveles de servicio más exigentes, auditoría tecnológica y sanciones. La Comisión toma

nota de la observación, que no contiene una solicitud de modificación sino la descripción del cauce natural de cumplimiento del régimen. Precisamente el numeral 6.13.3.1.6 concibe la formalización contractual como el instrumento mediante el cual las obligaciones regulatorias se proyectan sobre las relaciones entre los agentes de la cadena, incluidos los terceros tecnológicos que estos contraten.

Finalmente, **PTC** considera indispensable la medida de debida diligencia del artículo 6.13.3.1 y destaca que la identificación del responsable de los contenidos es la herramienta que permite la persecución efectiva de los delitos asociados al fraude, frente a los altos índices de archivo de las denuncias por delitos informáticos. La Comisión comparte la posición del agente, que coincide con la finalidad de transparencia y trazabilidad de la cadena de valor expuesta en el numeral 2.4.1 de este capítulo, y la registra como respaldo a la medida, que se mantiene con los ajustes de precisión y flexibilización descritos en los numerales precedentes

2.6 Plantillas (Template ID)

AMCHAM

Señala que el proyecto de resolución, al estructurar parte de su arquitectura de seguridad sobre un esquema de plantillas rígidas y aprobación previa de contenido, particularmente en los artículos 6.13.4.1 a 6.13.4.3, introduce un modelo de control estático que puede resultar incompatible con las herramientas más avanzadas de protección al usuario.

Adiciona que el fraude cibernético evoluciona de manera constante y utiliza técnicas de ingeniería social, suplantación y manipulación de mensajes que cambian en tiempo real. Por esta razón, dice, la industria global ha venido migrando hacia sistemas de Inteligencia Artificial y aprendizaje automático que permiten analizar patrones de tráfico, identificar comportamientos sospechosos, activar alertas dinámicas y ajustar mecanismos de autenticación de acuerdo con el riesgo detectado. Estas soluciones, a juicio de **AMCHAM**, no dependen necesariamente de textos previamente aprobados, sino de la capacidad de reacción inmediata frente a señales de amenaza.

En este contexto, **AMCHAM** sostiene que la exigencia de una plantilla previamente aprobada puede limitar la posibilidad de que los sistemas de seguridad globales adapten los mensajes de alerta, los factores de autenticación o las respuestas automatizadas ante incidentes detectados por Inteligencia Artificial.

A su juicio, esto podría dejar a los usuarios expuestos frente a ataques que no encajen en las plantillas vigentes o que requieran una reacción inmediata, distinta a la previamente validada por el esquema regulatorio.

Por lo anterior, **AMCHAM** considera que una regulación orientada a combatir el fraude debe promover la adopción de tecnologías avanzadas, no restringirlas mediante modelos excesivamente rígidos. En

consecuencia, **AMCHAM** sugiere que la CRC revise el alcance de las obligaciones asociadas a plantillas y validación previa, de manera que se permita el uso de soluciones dinámicas, automatizadas y basadas en riesgo, siempre que estas cumplan con estándares verificables de seguridad, trazabilidad y protección al usuario. Así mismo, **AMCHAM** advierte que rigidizar los canales SMS y USSD bajo un esquema centralizado de validación de contenido puede desincentivar la transición hacia métodos de autenticación más robustos y adaptativos, en contravía del principio de neutralidad tecnológica. La regulación debería habilitar, a su juicio, distintos modelos técnicos de prevención y detección de fraude, permitiendo que los proveedores adopten las mejores herramientas disponibles según la evolución de los riesgos y las capacidades de sus sistemas.

ANDESCO

En el marco del régimen de plantillas de contenido A2P y obligaciones de los actores, **ANDESCO** dice que el artículo 6.13.4.7.2 obliga a los PRST a verificar, 'previo al enrutamiento de CADA mensaje A2P', que este cuente con código corto A2P válido, Sender ID asignado e implementado y plantilla aprobada y vigente en el sistema del validador. **ANDESCO** sostiene que esta exigencia de validación síncrona por mensaje individual es técnicamente incompatible con la arquitectura y capacidad de procesamiento de los SMSC de los operadores móviles colombianos.

A su juicio, desde el punto de vista técnico, la propuesta presenta los siguientes problemas: (i) Los SMSC de los operadores procesan entre 2,000 y 3,000 mensajes por segundo en hora pico. (ii) La validación síncrona al validador introduce una latencia adicional mínima de 200 ms por mensaje (tiempo de respuesta normal según Art. 6.13.2.1.2). (iii) Con 2,000 msg/seg y 200 ms de latencia adicional, el throughput efectivo se reduciría a aproximadamente 340- 510 msg/seg: pérdida del 83% de capacidad. (iv) En condiciones de alta demanda del validador (500 ms según la norma), la latencia total superaría 610-890 ms por mensaje, violando los SLA de mensajería transaccional (OTP bancarios exigen entrega < 500 ms). (v) El validador centralizado debe atender simultáneamente las consultas de todos los operadores del país: 6,000 a 12,000 consultas/segundo. Ningún sistema de un único nodo puede sostener ese volumen con los tiempos exigidos. (vi) Los mensajes que no se procesen en tiempo real se acumularán en cola, generando timeouts SMPP y colapso del servicio en horas pico. Los más afectados serían los mensajes OTP de autenticación bancaria, que son los más críticos para el usuario final.

Para **ANDESCO**, la propuesta de norma crea una obligación de resultado (validación previa a cada mensaje) sin valorar la viabilidad técnica de su cumplimiento. El artículo 19 de la Ley 1341 de 2009 exige que la regulación sea técnica y económicamente viable. Una obligación cuyo cumplimiento literal hace colapsar el servicio no cumple ese requisito. En su opinión, la CRC no realizó análisis de impacto sobre la viabilidad técnica de esta exigencia en plataformas de alto throughput, incumpliendo la metodología AIN. Dice que la degradación del servicio SMS A2P generaría: (i) pérdida de ingresos para PRST y asignatarios de código corto durante los períodos de colapso; (ii) responsabilidades contractuales de los operadores frente a clientes corporativos cuyos SLA se incumplan; (iii) costos de rediseño arquitectural profundo de los SMSC, no incluidos en el AIN. (iv) Incumplimiento de SLA de OTP

bancarios. (v) Afectación de mensajería crítica de IoT (rastreo vehicular, alarmas, sensores industriales). (vi) Costos de rediseño arquitectural no cuantificados. (vii). Responsabilidades contractuales de los operadores.

Para **ANDESCO**, más que descartar de plano la validación centralizada, solicita que la CRC defina su arquitectura técnica antes de imponer la obligación. La resolución debe precisar el flujo operativo de validación, las especificaciones de las APIs, los mecanismos de autenticación, los tiempos máximos de respuesta, los niveles de disponibilidad, los criterios de capacidad en transacciones por segundo (TPS), los esquemas de caché o validación local permitidos, las reglas aplicables al tráfico bidireccional y los protocolos de contingencia ante indisponibilidad o degradación del validador. Sin esas especificaciones, los PRST y demás agentes no pueden dimensionar adecuadamente las inversiones requeridas, evaluar impactos sobre SMSC y motores de enrutamiento, ni garantizar la continuidad de mensajes legítimos.

En consecuencia, **ANDESCO** dice que la regulación debe evitar que la validación centralizada se traduzca en un cuello de botella operacional y debe permitir soluciones técnicas que preserven la continuidad del servicio, reduzcan latencias, eviten acumulación de colas, prevengan timeouts y aseguren que una falla del validador no bloquee injustificadamente tráfico legítimo, en especial el asociado a autenticación, seguridad, salud, servicios públicos, alertas transaccionales y comunicaciones críticas.

En complemento de lo anterior, **ANDESCO** dice que el régimen de plantillas establece que ningún mensaje A2P puede ser cursado si no está respaldado por una plantilla previamente aprobada y vigente. Las plantillas tienen vigencia mensual con renovación automática. El procedimiento de aprobación toma hasta 48 horas; sin embargo, para **ANDESCO**, el Proyecto no define la estructura, contenido mínimo, campos de información, reglas de intercambio ni especificaciones técnicas de la plantilla o formato mediante el cual se realizarían las consultas y respuestas entre los proveedores y dicho mecanismo. Esta ausencia, a su juicio, limita la capacidad de los PRST para evaluar de manera integral la viabilidad técnica, operativa y económica de la medida propuesta, así como para identificar los desarrollos tecnológicos, adecuaciones de sistemas, tiempos de implementación y eventuales impactos sobre sus procesos.

En consecuencia, dice que es necesario que la CRC incorpore dentro de la propuesta regulatoria un modelo de plantilla o especificación funcional detallada y la someta a comentarios de la industria, con el fin de garantizar un análisis adecuado de su factibilidad y de los costos asociados a su implementación.

Dice que, sin conocer la información que deberá intercambiarse, los tiempos de respuesta exigidos y los mecanismos de integración, resulta imposible estimar con precisión los impactos regulatorios y la carga operativa que asumirían los PRST. Lo anterior, en atención a los principios de transparencia, participación y análisis de impacto normativo. Adicionalmente, la obligación de que 'ningún mensaje A2P podrá ser cursado sin plantilla aprobada y vigente' (Art. 6.13.4.1) es una restricción absoluta sin excepciones para situaciones de emergencia o falla del validador. El Código de Procedimiento Administrativo establece que las restricciones absolutas sobre actividades lícitas requieren justificación

de proporcionalidad. La norma tampoco establece qué ocurre si el validador demora más de 48 horas en resolver una solicitud de plantilla urgente: el agente queda bloqueado sin recurso inmediato.

Finalmente, solicita que la regulación establezca que la validación y aprobación de plantillas por parte del validador centralizado se realice en un plazo máximo de veinticuatro (24) horas. Un término superior podría generar impactos significativos sobre la operación de los agentes que utilizan servicios de mensajería para el desarrollo de su actividad económica, especialmente en aquellos casos en los que la creación o modificación de plantillas responde a necesidades comerciales, operativas o de atención a los usuarios que requieren una implementación ágil.

En efecto, dice, numerosos sectores económicos, entre ellos el financiero, asegurador, comercio electrónico, transporte, salud y telecomunicaciones, utilizan la mensajería para enviar comunicaciones asociadas a procesos transaccionales, campañas temporales, validaciones de identidad, recuperación de credenciales, notificaciones de seguridad y atención de contingencias operativas. En estos escenarios, imponer tiempos de aprobación superiores a veinticuatro (24) horas podría retrasar la puesta en marcha de nuevos servicios, afectar la continuidad de procesos críticos y generar perjuicios económicos tanto para los remitentes como para los usuarios finales. Por esta razón, cualquier esquema de validación debe procurar un equilibrio entre los controles destinados a prevenir el fraude y la necesidad de garantizar la agilidad que demandan las dinámicas propias del mercado y de los servicios digitales.

ANDI

Afirma que los artículos 6.13.4.1 a 6.13.4.3, junto con la definición de Plantilla de contenido A2P, disponen que ningún mensaje A2P puede cursarse sin una plantilla aprobada y vigente; que el validador revisa el contenido estático y el sentido del contenido dinámico; que las plantillas tienen vigencia mensual renovable; y que la aprobación o el rechazo se resuelven en plazos de 24 a 48 horas.

Indica que el Proyecto instaura un mecanismo de aprobación previa de plantillas como condición para cursar comunicaciones A2P. Este esquema debe analizarse con especial cuidado, pues puede operar como un control previo sobre comunicaciones legítimas y generar restricciones desproporcionadas a la libertad de empresa, la libre competencia y la continuidad de servicios digitales. Aunque la renovación sea automática, mantener una vigencia mensual y causales amplias de desactivación introduce incertidumbre operativa para servicios críticos.

En particular, sostiene que, si la plantilla puede ser suspendida, rechazada o desactivada por criterios amplios o poco determinados, como los establece el Proyecto de Resolución, los remitentes legítimos enfrentan un riesgo operativo permanente que puede afectar comunicaciones de seguridad, autenticación, alertas de fraude o mensajes transaccionales necesarios para la prestación de servicios digitales.

Añade que los servicios digitales modifican textos, idiomas, variables y enlaces de manera continua y a gran escala. Exigir una plantilla aprobada por mensaje o campaña, con vigencia mensual y revisión del contenido dinámico, es incompatible con flujos automatizados y con la personalización legítima. En el caso de los OTP, el contenido dinámico es, por diseño, impredecible. El esquema introduce latencia, costos y fragilidad operativa, y traslada al validador decisiones que afectan la entrega de mensajes legítimos, con un incentivo estructural a la sobre-restricción para evitar responsabilidad.

En complemento de lo anterior, la **ANDI** dice que el artículo 6.13.4.7.2 obliga al PRST a verificar, antes de enrutar cada mensaje A2P, la existencia de código corto A2P, SENDER ID y plantilla vigente en el sistema validador, y dispone que, en ausencia de alguno de estos elementos, el PRST deberá bloquear el mensaje impidiendo su entrega al usuario final o, alternativamente, a su elección, marcarlo con la etiqueta de no verificado.

Al respecto, la **ANDI** dice que condicionar el enrutamiento de cada comunicación a una consulta de verificación genera una dependencia operativa y añade una latencia inadmisible a la red. Bajo esta arquitectura, cualquier retraso técnico en la consulta o un falso negativo en el sistema central se traducirá en el bloqueo automático de interacciones críticas que requieren inmediatez, tales como las alertas de fraude o los códigos de autenticación, lo cual perjudicará gravemente a los usuarios y a los remitentes globales.

Además, dice que la alternativa de marcar un mensaje de seguridad legítimo con la etiqueta de «sin verificar» resulta ser una medida equívoca y contraproducente. En lugar de alertar eficazmente, esta señalización induce a error al usuario y mina su confianza en las comunicaciones que son, precisamente, las que buscan proteger su identidad y su patrimonio.

Añade que el costo económico y reputacional de un falso bloqueo o de una mala catalogación sobre una comunicación crítica es desproporcionadamente elevado y asimétrico frente al beneficio marginal que el Proyecto pretende obtener mediante una exigencia procedimental. Asimismo, debe considerarse que el etiquetado erróneo de comunicaciones legítimas como «sin verificar» puede generar un efecto adverso sobre la confianza del usuario en los canales oficiales. En particular, si un mensaje de autenticación, una alerta de seguridad o una comunicación transaccional legítima aparece asociada a una advertencia de falta de verificación, el usuario puede ser inducido a desconfiar de los canales formales y a acudir a canales alternativos menos seguros. Este escenario podría ser aprovechado por defraudadores mediante esquemas de ingeniería social, en los que se explote la confusión generada por inconsistencias en el etiquetado para redirigir al usuario hacia comunicaciones fraudulentas.

CCIT

Indica que los artículos 6.13.4.1 a 6.13.4.3, junto con la definición de Plantilla de contenido A2P, disponen que ningún mensaje A2P puede cursarse sin una plantilla aprobada y vigente; que el validador revisa el contenido estático y el sentido del contenido dinámico; que las plantillas tienen vigencia mensual renovable; y que la aprobación o el rechazo se resuelven en plazos de 24 a 48 horas. El

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Proyecto instaura un mecanismo de aprobación previa de plantillas como condición para cursar comunicaciones A2P.

Alega que este esquema debe analizarse con especial cuidado, pues puede operar como un control previo sobre comunicaciones legítimas y generar restricciones desproporcionadas a la libertad de empresa, la libre competencia y la continuidad de servicios digitales. Aunque la renovación sea automática, mantener una vigencia mensual y causales amplias de desactivación introduce incertidumbre operativa para servicios críticos.

En particular, dice que, si la plantilla puede ser suspendida, rechazada o desactivada por criterios amplios o poco determinados, como los establece el Proyecto de Resolución, los remitentes legítimos enfrentan un riesgo operativo permanente que puede afectar comunicaciones de seguridad, autenticación, alertas de fraude o mensajes transaccionales necesarios para la prestación de servicios digitales. Además, sostiene que los servicios digitales modifican textos, idiomas, variables y enlaces de manera continua y a gran escala.

Afirma que exigir una plantilla aprobada por mensaje o campaña, con vigencia mensual y revisión del contenido dinámico, es incompatible con flujos automatizados y con la personalización legítima. En el caso de los OTP, el contenido dinámico es, por diseño, impredecible. El esquema introduce latencia, costos y fragilidad operativa, y traslada al validador decisiones que afectan la entrega de mensajes legítimos, con un incentivo estructural a la sobrerestricción para evitar responsabilidad.

En complemento de lo anterior, dice que el artículo 6.13.4.7.2 obliga al PRST a verificar, antes de enrutar cada mensaje A2P, la existencia de código corto A2P, SENDER ID y plantillas vigentes en el sistema validador, y dispone que, en ausencia de alguno de estos elementos, el PRST deberá bloquear el mensaje impidiendo su entrega al usuario final o, alternativamente, a su elección, marcarlo con la etiqueta de no verificado. Al respecto, afirma que condicionar el enrutamiento de cada comunicación a una consulta de verificación genera una dependencia operativa y añade una latencia inadmisible a la red. Bajo esta arquitectura, cualquier retraso técnico en la consulta o un falso negativo en el sistema central se traducirá en el bloqueo automático de interacciones críticas que requieren inmediatez, tales como las alertas de fraude o los códigos de autenticación, lo cual perjudicará gravemente a los usuarios y a los remitentes globales.

Además, dice que la alternativa de marcar un mensaje de seguridad legítimo con la etiqueta de «sin verificar» resulta ser una medida equívoca y contraproducente. En lugar de alertar eficazmente, esta señalización induce a error al usuario y mina su confianza en las comunicaciones que son, precisamente, las que buscan proteger su identidad y su patrimonio. El costo económico y reputacional de un falso bloqueo o de una mala catalogación sobre una comunicación crítica es desproporcionadamente elevado y asimétrico frente al beneficio marginal que el Proyecto pretende obtener mediante una exigencia procedimental.

COLOMBIA FINTECH

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Manifiesta que el artículo 6.13.4.3.1 establece que el validador puede rechazar una plantilla mediante comunicación motivada, pero la norma no contempla ningún procedimiento formal de revisión o segunda instancia para el asignatario que considere injustificado ese rechazo. Por su parte el artículo 6.13.1.6.5 prohíbe los rechazos injustificados, pero no define consecuencias ni quién los determina. Advierte que, para una entidad financiera, el rechazo de una plantilla de OTP equivale a una interrupción del servicio.

En este sentido, solicita que la CRC establezca un procedimiento expedito de revisión de rechazos ante el Administrador de Recursos de Identificación, con un plazo máximo de resolución de veinticuatro (24) horas para las plantillas de autenticación y seguridad.

Por otro lado, indica que el plazo de hasta 48 horas para procesar modificaciones de plantillas ya aprobadas no distingue entre cambios sustantivos (nueva modalidad, nuevas URLs, cambios de modalidad) y cambios menores (ajustes de copy, longitud del texto, reformulaciones que conservan la modalidad y el tipo de variables). Señala que, para productos de mensajería operados por entidades financieras, los ajustes menores son continuos (optimización por métricas de conversión, ajustes de tono, pruebas A/B).

Advierte que el plazo único bloquea el ciclo de mejora del producto sin justificación regulatoria proporcional al riesgo. Por tanto, solicita que la CRC introduzca en el artículo 6.13.4.3.2 una distinción entre modificaciones sustantivas (que mantienen el plazo de 48 horas) y modificaciones menores (entendidas como cambios al texto que preservan la modalidad, las URLs y los campos variables aprobados), con un plazo máximo de 24 horas. Alternativamente, que el validador esté facultado para aprobar tácitamente las modificaciones menores no rechazadas dentro de las primeras 12 horas.

Adicionalmente, indica que el artículo 6.13.4.2.4. reconoce la existencia de campos variables en las plantillas y exige declarar el tipo de información insertable, pero no establece una sintaxis estándar de marcado (placeholders), ni una tipología cerrada de tipos de variable (numérico, alfanumérico, monetario, fecha, identificador), ni define si los placeholders deben publicarse como especificación técnica del validador antes de su entrada en operación. La ausencia de esa estandarización genera ambigüedad operativa en la integración con proveedores internacionales de mensajería y obstaculiza la migración desde sistemas que ya operan con sintaxis propias.

Solicita que la CRC adicione al artículo 6.13.4.2.4 un parágrafo que establezca que el validador publicará, con al menos noventa (90) días de antelación a su entrada en operación, una especificación técnica que defina:

(i) la sintaxis estándar de placeholders de campos variables (por ejemplo, notación con dobles llaves {{variable}});
(ii) una tipología cerrada y reconocida de tipos de variable que no requiera aprobación caso a caso de cada valor concreto; y

(iii) las reglas de validación del contenido insertable.

Adicionalmente, indica que la obligación de que todo mensaje SMS A2P deba pasar por un validador centralizado y corresponder a una plantilla preaprobada antes de que el operador autorice su entrega al usuario final genera un cuello de botella para la inmediatez de las campañas de marketing, promociones limitadas u ofertas relámpago, que por su naturaleza dependen de ventanas de oportunidad muy cortas.

Solicita a la CRC que:

(i) evalúe excluir la categoría «Comercial/Marketing» de la validación previa;
(ii) en caso de mantenerse la validación previa, garantice que las plantillas comerciales permitan un porcentaje amplio de texto variable, del orden del 70%; y
(iii) establezca que, si el sistema del validador falla, se congestiona o no entrega respuesta dentro del plazo definido (por ejemplo, quince (15) minutos), el mensaje se entienda aprobado de manera automática.

CRISTIAN CANTILLO

Expone las siguientes preguntas:

¿Estarán las comunicaciones operativas, regulatorias y de servicio al cliente de los propios operadores (PRM y OMV) sujetas a la aprobación previa de plantillas ante el validador centralizado? De ser así, ¿cómo planea la CRC mitigar el impacto en la inmediatez de las comunicaciones de emergencia, alertas de fraude en tiempo real para el usuario o suspensiones de servicio, si estas dependen de un proceso de aprobación ex ante por parte de un tercero?

Frente al principio de neutralidad de red y la naturaleza del negocio OMV: Si un OMV utiliza la infraestructura de mensajería de su operador anfitrión para enviar notificaciones de red a sus usuarios desde números móviles ordinarios, ¿el operador anfitrión tendrá la facultad regulatoria de inspeccionar, filtrar o rechazar este contenido bajo el argumento de «mitigación de fraude», afectando la relación comercial directa del OMV con su cliente?

INALAMBRIA

Manifiesta que el régimen de plantillas propuesto podría incorporar criterios de gestión de riesgo asociados tanto al contenido como al origen del mensaje. En particular, la obligación de registro, aprobación o validación previa de plantillas podría concentrarse en aquellos mensajes que incluyan exclusivamente elementos que históricamente han estado asociados a campañas de fraude, tales como:

- La originación de mensajes a través de mayoristas internacionales o empresas que facilitan la interconexión de Colombia con proveedores de servicios de internet globales debido a que

la gran mayoría de actores maliciosos buscan «esconderse» detrás de cadenas internacionales largas de interconexión SMS, evitando su trazabilidad.
- La presencia de URLs o enlaces externos como se menciona anteriormente.

Mensajes cuyo contenido corresponda exclusivamente a comunicaciones transaccionales, operativas, informativas o de interés público podrían estar sujetos a un régimen simplificado o incluso exentos de controles asociados a plantillas.

Este enfoque permitiría focalizar los esfuerzos regulatorios sobre los segmentos de mayor riesgo (mensajes originados por agregadores internacionales y mensajes con URLs) reduciendo simultáneamente los costos de cumplimiento para los remitentes legítimos y disminuyendo los efectos no deseados sobre servicios esenciales y comunicaciones de interés general.

En este sentido, **INALAMBRIA** propone que se implemente un esquema de gestión de riesgo basado en el contenido y origen de los mensajes. Contemplando eventualmente un régimen simplificado de validación, o incluso la exclusión de determinadas obligaciones asociadas al registro y aprobación previa de plantillas.

JULIO NULDEMAR

Expone que el proyecto establece que ningún mensaje A2P podrá ser cursado a través de las redes de los PRST sin contar con una plantilla de contenido aprobada y vigente (Template ID) en el validador centralizado.

Esta medida podría vulnerar el Principio de Neutralidad Tecnológica del artículo 2 de la Ley 1341 de 2009, al imponer restricciones sobre mecanismos tecnológicos utilizados por los operadores para comunicarse con sus usuarios, como notificaciones push en aplicaciones propias, canales web o soluciones basadas en Applets/STK, los cuales corresponden a entornos cerrados y controlados donde el riesgo de suplantación o spoofing es reducido.

Plantea una posible extralimitación de competencias, al someter canales internos y desarrollos tecnológicos propios de los operadores a una validación previa por parte del sistema centralizado, así como al atribuir al validador funciones relacionadas con la verificación de condiciones de consentimiento, competencia que correspondería a la Superintendencia de Industria y Comercio (SIC) como autoridad de protección de datos personales**.**

De otra parte, señala que el proyecto podría generar una exposición adicional de los operadores a responsabilidad civil al exigir bloqueos o filtrados de tráfico legítimo basados en la detección de patrones atípicos o inconsistencias en plantillas, sin contemplar escenarios de falsos positivos.

Esto resulta relevante debido a que el tráfico A2P puede incluir comunicaciones críticas como alertas bancarias, códigos OTP, notificaciones de servicios de emergencia y comunicaciones médicas, por lo

que un error del algoritmo o del validador centralizado podría generar afectaciones económicas y operativas a terceros.

Adicionalmente, se señala que el proyecto no contempla una cláusula de protección o salvaguarda para los operadores que actúen de buena fe en cumplimiento de la obligación regulatoria de bloqueo, exponiéndolos a posibles demandas multimillonarias por lucro cesante y pérdida de la oportunidad derivadas de los fallos del sistema automatizado, rompiendo el principio de confianza legítima.

Concluye que el texto, debería modificarse a lo siguiente « **PARÁGRAFO NUEVO:** Exclúyase del ámbito de aplicación de la presente resolución, y por ende de las obligaciones de registro de SENDER ID y validación previa de plantillas ante el validador centralizado, a las comunicaciones de naturaleza informativa, operativa, regulatoria o de atención al cliente emitidas directamente por los PRST (incluyendo Operadores Móviles Virtuales - OMV) hacia sus propios usuarios finales, bien sea que se utilicen recursos de numeración móvil convencional (MSISDN) o canales digitales propietarios independientes del canal SMS tradicional (notificaciones Push, Applets SIM u homólogos)»

NEXVIA

Señala que el condicionamiento absoluto del tráfico a la aprobación previa de plantillas, administrada por un validador privado sin recurso contra sus decisiones, instala un régimen de autorización previa de contenidos cuya demora o rechazo paraliza servicios críticos (OTP, alertas transaccionales, citas de salud). En mensajería transaccional, minutos de indisponibilidad generan afectaciones directas al usuario final.

Afirma que el modelo proporcionado y probado internacionalmente es el de doble vía, análogo al tratamiento del CLI en voz, tráfico con plantilla verificada cursa con plena confianza; tráfico sin verificar cursa con etiquetado que advierte al usuario, sin bloqueo previo. Así se preserva la finalidad antifraude (transparencia frente al usuario) sin instituir un poder de veto privado sobre las comunicaciones. Frente a este caso, presenta la siguiente propuesta de redacción:

> «A través del código corto A2P podrá cursarse tráfico A2P de personas naturales o jurídicas que cuenten con un SENDER ID asignado y vigente vinculado al mismo. El tráfico respaldado por una plantilla de contenido verificada y vigente se cursará como tráfico verificado. El tráfico sin plantilla verificada podrá cursarse con la marcación «sin verificar» visible para el usuario receptor, sin perjuicio de las medidas que la CRC ordene dentro de las actuaciones administrativas a que haya lugar.»

SAEM

Afirma que ningún mensaje A2P podrá enrutarse si no está respaldado por una plantilla aprobada y vigente (art. 6.13.4.1). Las plantillas tienen vigencia mensual con renovación automática (art.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6.13.4.3.3), deben aprobarse en 24–48 horas (art. 6.13.4.3.1) y el PRST debe validarlas en tiempo real, mensaje por mensaje, antes del enrutamiento (art. 6.13.4.7).

Indica que el tráfico A2P real es de altísimo volumen y, en gran parte, dinámico (OTP, alertas, notificaciones transaccionales con campos variables). Un régimen de plantillas rígido, con campos variables limitados y vigencia mensual, genera un riesgo permanente de divergencia entre el contenido aprobado y el cursado, lo que —por la vía del artículo 6.13.4.4 y de las causales 6.4.3.2.6 y 6.12.3.2.12— puede derivar en la recuperación del código corto A2P del IT por conductas que no controla.

Menciona que India implementó en 2018–2021, mediante la TCCCPR de la TRAI, un sistema de registro obligatorio de entidades, cabeceras (headers) y plantillas de contenido sobre blockchain/DLT, conceptualmente idéntico al aquí propuesto. Cuando entró en operación el «scrubbing» de plantillas (marzo de 2021), se bloquearon masivamente mensajes legítimos —incluidos OTP bancarios y notificaciones transaccionales—, al punto que el regulador tuvo que suspender temporalmente la verificación. El cronograma se aplazó en repetidas ocasiones durante años, el onboarding de empresas se congestionó y el desajuste entre contenido dinámico y plantillas rígidas resultó estructural. Pese a todo ello, señala que el fraude continuó por rutas no registradas, tal como OTT y spoofing.

Propone lo siguiente: (i) Diferenciar por modalidad: exigir preaprobación de plantilla únicamente para contenido comercial/publicitario, y aplicar un régimen liviano (registro categórico, sin aprobación previa mensaje a mensaje) a OTP/autenticación, transaccional e informativo y regulatorio, por su carácter crítico y sensible al tiempo; (ii) admitir plantillas con campos variables amplios y reglas de coincidencia tolerantes; (iii) sustituir la vigencia mensual por una vigencia anual o indefinida sujeta a revisión periódica; (iv) prever, durante una rampa inicial prolongada, que la falta de coincidencia genere etiquetado «sin verificar» y no bloqueo; y (v) fijar un mecanismo expreso de plantillas de emergencia para campañas urgentes de interés público.

En complemento de lo anterior, en relación con la validación en tiempo real, mensaje a mensaje, por el PRST (art. 6.13.4.7 y 6.13.2.1), expone que el PRST debe consultar al validador, antes de enrutar cada mensaje A2P, la validez del código corto A2P, del SENDER ID y de la plantilla (art. 6.13.4.7.1). El validador debe responder en ≤200 ms (≤500 ms en alta demanda) con disponibilidad del 99,5% mensual (art. 6.13.2.1). Al respecto, señala que una disponibilidad del 99,5% admite hasta ~3,6 horas de indisponibilidad mensual; durante esos lapsos, si el PRST opta por bloquear (opción que el art. 6.13.4.7.2 le permite), se interrumpe la entrega de OTP y notificaciones críticas que cursa el IT, con afectación directa a sus clientes y a los usuarios finales. La latencia añadida también degrada throughput en picos.

Por lo tanto, propone lo siguiente: (i) Elevar la disponibilidad exigida a ≥99,95% y robustecer las exigencias de redundancia geográfica; (ii) que ante indisponibilidad la conducta por defecto sea «fail-open» con etiqueta «sin verificar» —nunca bloqueo de tráfico previamente validado—; (iii) admitir verificación por listas sincronizadas en caché local del PRST (en lugar de consulta sincrónica mensaje a

mensaje) para reducir latencia y dependencia del enlace; y (iv) someter los SLA y el plan de contingencia (art. 6.13.2.2) a prueba conjunta con los IT antes de su entrada en vigencia.

Concretamente, solicita diferenciar el régimen de plantillas por modalidad —régimen liviano para OTP, transaccional, informativo y regulatorio; preaprobación solo para comercial—, con campos variables amplios, vigencia anual o indefinida y etiquetado «sin verificar» (no bloqueo) durante una rampa inicial prolongada.

SINCH

Señala que la obligatoriedad de pre-aprobar plantillas de texto (Template IDs) limita la agilidad de los comercios. Por ejemplo, si una marca necesita lanzar una oferta relámpago basada en una coyuntura del día, no podrá hacerlo de inmediato si tiene que esperar el visto bueno de la plantilla por parte del validador.

SUMA

No considera adecuado, conveniente, ni necesario, que se ejerza por ninguna instancia algún modo de control sobre el contenido o la estructura del contenido de los mensajes A2P. Considera innecesariamente intrusivo ejercer una fiscalización de ese nivel, siendo que la CRC dispone de otros mecanismos coercitivos para evitar usos incorrectos o abusivos, y disciplinar a las empresas de tipo IT y/o PCA o a sus potenciales clientes, en el supuesto de que se identificara alguna mala práctica concreta. Este nivel de fiscalización puede incurrir en una limitación innecesaria de la libertad de actuación empresarial.

CLARO

Señala que el proyecto regulatorio contempla la implementación de una Plantilla de contenido A2P; sin embargo, no define la estructura, contenido mínimo, campos de información, reglas de intercambio ni especificaciones técnicas de la plantilla o formato mediante el cual se realizarían las consultas y respuestas entre los proveedores y dicho mecanismo.

Esta ausencia limita la capacidad de los PRSTM para evaluar de manera integral la viabilidad técnica, operativa y económica de la medida propuesta, así como para identificar los desarrollos tecnológicos, adecuaciones de sistemas, tiempos de implementación y eventuales impactos sobre sus procesos.

En consecuencia, considera que es necesario que la CRC incorpore dentro de la propuesta regulatoria un modelo de plantilla o especificación funcional detallada y la someta a comentarios de la industria, con el fin de garantizar un análisis adecuado de su factibilidad y de los costos asociados a su implementación.

Sin conocer la información que deberá intercambiarse, los tiempos de respuesta exigidos y los mecanismos de integración, resulta imposible estimar con precisión los impactos regulatorios y la carga operativa que asumirían los PRST. Lo anterior, en atención a los principios de transparencia, participación y análisis de impacto normativo.

Finalmente, solicita que la regulación establezca que la validación y aprobación de plantillas por parte del validador centralizado se realice en un plazo máximo de veinticuatro (24) horas. Un término superior podría generar impactos significativos sobre la operación de los agentes que utilizan servicios de mensajería para el desarrollo de su actividad económica, especialmente en aquellos casos en los que la creación o modificación de plantillas responde a necesidades comerciales, operativas o de atención a los usuarios que requieren una implementación ágil.

En efecto, expone que numerosos sectores económicos, entre ellos el financiero, asegurador, comercio electrónico, transporte, salud y telecomunicaciones, utilizan la mensajería para enviar comunicaciones asociadas a procesos transaccionales, campañas temporales, validaciones de identidad, recuperación de credenciales, notificaciones de seguridad y atención de contingencias operativas. En estos escenarios, señala que imponer tiempos de aprobación superiores a veinticuatro (24) horas podría retrasar la puesta en marcha de nuevos servicios, afectar la continuidad de procesos críticos y generar perjuicios económicos tanto para los remitentes como para los usuarios finales. Por esta razón, señala que cualquier esquema de validación debe procurar un equilibrio entre los controles destinados a prevenir el fraude y la necesidad de garantizar la agilidad que demandan las dinámicas propias del mercado y de los servicios digitales.

PTC

Manifiesta que los servicios A2P pueden incorporar información de naturaleza comercial, estratégica o incluso confidencial de los generadores de contenido, la obligación de registrar y reportar las plantillas de mensajería propuesta en el proyecto regulatorio podría generar riesgos asociados a la protección de información sensible y a la preservación de secretos empresariales, especialmente si no se establecen mecanismos regulatorios expresos que garanticen su adecuado tratamiento, custodia y confidencialidad.

En este sentido, expone que es necesario que la CRC precise las condiciones bajo las cuales dicha información será administrada, así como las medidas destinadas a evitar accesos no autorizados, filtraciones o cualquier situación que pueda derivar en una afectación a la competencia o a los intereses comerciales legítimos de los agentes involucrados.

No obstante, **PTC** considera que el objetivo perseguido por la Comisión podría alcanzarse mediante mecanismos alternativos menos intrusivos. En particular, expone que una certificación emitida por el Integrador Tecnológico respecto del cumplimiento de las condiciones regulatorias aplicables a las plantillas registradas permitiría gestionar adecuadamente los riesgos asociados al uso indebido de la mensajería A2P, sin requerir la revelación detallada del contenido de las comunicaciones.

Concluye que lo anterior, resulta razonable en la medida en que los Integradores Tecnológicos, en su calidad de actores directamente involucrados en la cadena de valor del servicio, pueden asumir un deber de gestión y mitigación del riesgo de fraude, suplantación o uso indebido de la mensajería, quedando sujetos a las consecuencias regulatorias y sancionatorias previstas en la regulación en caso de incumplimiento. De esta forma, señala que se logra un equilibrio entre los objetivos de supervisión y control perseguidos por la CRC y la protección de la información comercial sensible de los distintos agentes del ecosistema.

Aunado a lo anterior, solicita que la Comisión determine de manera clara y expresa la periodicidad con la que deberán actualizarse las plantillas registradas, con el fin de brindar certeza regulatoria a los agentes obligados y con ello evitar interpretaciones divergentes respecto de esta obligación.

Asimismo, resalta que es necesario que el plazo de actualización responda a criterios de razonabilidad y proporcionalidad, de forma tal que no genere cargas operativas excesivas derivadas de actualizaciones recurrentes e innecesarias, pero que tampoco permita que la información registrada permanezca desactualizada por periodos prolongados que puedan afectar los objetivos de trazabilidad y control perseguidos por la medida regulatoria.

BLIPBLIP, NEXVIA E INALAMBRIA

Afirman en su escrito conjunto que, la exigencia de que ningún mensaje A2P pueda cursarse sin una plantilla previamente aprobada y vigente en el sistema del validador (numerales 6.4.3.1.7 y 6.13.4.7.2, entre otros) instala un régimen de autorización previa de contenidos que es incompatible con la naturaleza dinámica del negocio de mensajería. Lo anterior lo sustentan en los siguientes puntos:

• Paraliza servicios críticos y campañas urgentes: un comercio que necesita enviar una promoción de inmediato, o una entidad de salud que debe alertar sobre un riesgo sanitario urgente, quedan sujetos a un trámite de aprobación. En mensajería transaccional, minutos de indisponibilidad se traducen en afectación directa al usuario final.
• Vulnera la libertad de comunicación e introduce riesgos de privacidad: someter el contenido de las comunicaciones empresariales a la aprobación de un tercero limita la libertad de empresas e individuos para comunicarse con sus usuarios y expone información sensible.
• Genera sobrecostos recurrentes: la vigencia y renovación mensual de las plantillas impone una carga operativa permanente a toda la cadena, reduce la productividad y encarece el canal.
• Es un reto técnico de gran escala: implementar la validación previa de plantillas manteniendo los volúmenes actuales —del orden de miles de millones de SMS al mes— supone un desafío técnico cuya viabilidad el proyecto no acredita.
• Duplica obligaciones ya existentes: la identificación del remitente vía SENDER ID ya es exigible bajo la Ley 2300; el proyecto la reproduce con un nuevo recurso y un nuevo costo.

HABLAME

Afirma que el esquema de plantillas es una censura previa del contenido y debe sustituirse por la identificación del originador, teniendo en cuenta que los artículos 6.13.4.1, 6.13.4.3 y 6.13.4.7.2 condicionan el envío de cada mensaje a que su contenido cuente con una plantilla previamente aprobada, y obligan al operador a bloquear el mensaje que no la tenga lo que categorizan como una censura previa.

Expone que, el artículo 20 de la Constitución Política garantiza a toda persona el derecho a recibir información, y ese derecho no admite autorización ni revisión previa por parte del Estado o de un particular, por lo que afirma que, en un servicio básico de telecomunicaciones, impedir que el usuario reciba un mensaje por el solo hecho de que su contenido no fue aprobado de antemano es una restricción que la Constitución no permite.

En suma, señala que la Corte ha sostenido que sobre la información solo caben controles posteriores y nunca previos (Sentencia C-488 de 1993), y que los intermediarios no tienen el deber ni la facultad de revisar el contenido antes de su difusión, porque hacerlo equivaldría a una censura proscrita (Sentencia T-121 de 2018), y a ello suma el bloque de constitucionalidad: el artículo 13 de la Convención Americana sobre Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos prohíben la censura previa y protegen tanto el derecho a difundir como el derecho a recibir información.

Expone que la CRC no puede convertirse en validador previo del contenido de los mensajes, ni puede trasladar esa función a los operadores o a los validadores privados ya que su finalidad legítima es otra y más sencilla: lograr que el usuario sepa quién le está escribiendo, para que decida por sí mismo si confía en lo que recibe. Por ello precisa que la regulación debe enfocarse en identificar al originador, no en aprobar el contenido.

Propone un esquema de identificación y marcación en el cual el validador, bajo la denominación que adopte el proyecto, realiza el conocimiento y la verificación del cliente. Cuando el originador, PCA o remitente ha sido validado, sus mensajes se entregan con un Sender ID certificado, que permite al usuario identificar que provienen de una fuente verificada. En caso contrario, el mensaje no se bloquea ni su tratamiento queda a discreción del operador, sino que se entrega con una marcación obligatoria, visible y clara que advierte al usuario que el originador no ha sido validado.

De esta manera, señala que el usuario siempre recibe la información necesaria y decide con base en ella, de forma análoga a lo que ocurre en los servicios de voz, en los que la llamada sospechosa se cursa y se presenta en pantalla con la etiqueta correspondiente. Asimismo, afirma que este modelo resuelve la situación de las aplicaciones extranjeras sin sede en el país, pues les permitiría cursar su tráfico bajo la marcación de «originador no validado» mientras completan el proceso de verificación, en lugar de quedar totalmente excluidas. En consecuencia, solicita eliminar la aprobación previa de plantillas como condición para el envío de mensajes y sustituirla por el esquema propuesto, mediante la modificación de los artículos 6.13.4.1 y 6.13.4.7.2.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Respuesta CRC:

La CRC analizó los comentarios presentados frente al régimen de Plantillas de Contenido A2P —Template ID—, en particular aquellos formulados por **ANDI**, **CCIT**, **AMCHAM**, **COLOMBIA FINTECH**, **BLIPBLIP**, **NEXVIA**, **INALAMBRIA** y **HABLAME**, relacionados con la exigencia de que los mensajes A2P estén asociados a una plantilla aprobada y vigente, la revisión del contenido estático y del sentido del contenido dinámico, la vigencia mensual de las plantillas, la posibilidad de rechazo por parte del validador, el tratamiento de mensajes críticos, la privacidad de la información y la eventual duplicidad con otros mecanismos de identificación como el SENDER ID. La **ANDI** y la **CCIT** señalan que los artículos 6.13.4.1 a 6.13.4.3, junto con la definición de plantilla de contenido A2P, establecen que ningún mensaje A2P puede cursarse sin una plantilla aprobada y vigente; que el validador revisa el contenido estático y el sentido del contenido dinámico; que las plantillas tienen vigencia mensual renovable; y que la aprobación o rechazo se resuelve en plazos de 24 a 48 horas.

De manera general, los agentes cuestionan que el esquema de plantillas pueda operar como una autorización previa de contenidos, generar rigideces operativas frente a servicios digitales dinámicos, afectar mensajes de autenticación o seguridad, introducir costos recurrentes, restringir la innovación, exponer información sensible o duplicar controles ya previstos a través del SENDER ID. La CRC reconoce la relevancia de estas preocupaciones, pero considera que el régimen de plantillas constituye un elemento esencial del modelo preventivo propuesto, en la medida en que permite fortalecer la trazabilidad, verificar la consistencia entre la modalidad declarada y la comunicación cursada, y reducir el riesgo de que los recursos de identificación sean utilizados para enviar mensajes engañosos o fraudulentos.

A continuación, la CRC se pronuncia sobre cada uno de los aspectos comentados.

2.6.1 Naturaleza del esquema de plantillas: trazabilidad operativa y no autorización previa de contenidos

ANDI y **CCIT** sostienen que el proyecto instaura un mecanismo de aprobación previa de plantillas como condición para cursar comunicaciones A2P, lo que, a su juicio, podría operar como un control previo sobre comunicaciones legítimas y generar restricciones desproporcionadas a la libertad de empresa, la libre competencia y la continuidad de servicios digitales.

Por su parte, **BLIPBLIP**, **NEXVIA** e **INALAMBRIA** manifiestan en su escrito que exigir que ningún mensaje A2P pueda cursarse sin una plantilla previamente aprobada y vigente instala un régimen de autorización previa de contenidos incompatible con la naturaleza dinámica del negocio. En la misma línea, **HABLAME** califica el esquema de plantillas como una forma de censura previa del contenido y propone sustituirlo por mecanismos centrados en la identificación del originador.

La CRC no comparte la interpretación según la cual el régimen de plantillas constituya censura previa o autorización material del contenido de las comunicaciones. La finalidad del esquema no es controlar

opiniones, mensajes comerciales legítimos o comunicaciones empresariales en abstracto, sino verificar que el tráfico A2P que se cursa mediante recursos de identificación administrados por la CRC corresponda a una estructura, modalidad y finalidad previamente declaradas.

La plantilla cumple una función instrumental dentro del sistema de trazabilidad. Mientras el código corto A2P identifica el canal técnico mediante el cual se cursa el tráfico y el SENDER ID identifica al responsable del contenido frente al usuario, la plantilla permite verificar que el mensaje enviado corresponde a una modalidad declarada y a una estructura previamente conocida dentro del sistema de validación. Esta función resulta especialmente relevante para evitar que un remitente legítimamente identificado utilice posteriormente sus recursos para enviar comunicaciones con finalidades distintas a las registradas o con elementos que puedan facilitar la comisión de fraudes.
Uno de los elementos fundamentales de la plantilla es la declaración sobre si los mensajes incluyen o no URL. La CRC considera indispensable que el sistema de validación pueda identificar y controlar este elemento, teniendo en cuenta que una parte relevante de las conductas fraudulentas que se materializan a través de SMS se ejecutan mediante la inducción al usuario a acceder a enlaces indebidos, a través de los cuales se capturan datos personales, credenciales, claves, factores de autenticación o se facilita la suplantación de identidad. Por ello, un esquema preventivo que no permita conocer si una comunicación incorpora URL —y bajo qué estructura o finalidad se incluyen— resultaría insuficiente para mitigar eficazmente el riesgo de smishing.

En este sentido, la verificación de plantillas no puede entenderse como una autorización previa del contenido, sino como una condición de trazabilidad del tráfico A2P. La revisión permite comprobar la coherencia entre el remitente, la modalidad del mensaje, la finalidad declarada, la estructura del contenido y la eventual inclusión de elementos de riesgo, como enlaces. El proyecto de resolución y el documento soporte prevén precisamente un régimen de plantillas de contenido A2P y obligaciones de revisión de plantillas activas para verificar que el contenido cursado corresponda a las plantillas aprobadas.

En este orden de ideas, la CRC no acepta la solicitud de eliminar el régimen de plantillas ni comparte la afirmación según la cual este constituya censura previa o autorización material de contenidos, por lo que se mantiene la estructura propuesta en la medida en que la plantilla es una herramienta necesaria para la trazabilidad, la prevención del fraude y el control de elementos de riesgo, particularmente la inclusión de URL en mensajes A2P.

2.6.2 Rigidez del modelo frente a servicios digitales dinámicos, inteligencia artificial y respuestas automatizadas

AMCHAM señala que el proyecto estructura parte de su arquitectura de seguridad sobre un esquema de plantillas rígidas y aprobación previa de contenido, lo que podría resultar incompatible con herramientas avanzadas de protección al usuario basadas en inteligencia artificial, aprendizaje automático, análisis de patrones de tráfico, alertas dinámicas y mecanismos de autenticación ajustados al riesgo detectado. Según este planteamiento, los sistemas globales de seguridad requieren adaptar

mensajes, alertas o factores de autenticación ante incidentes detectados en tiempo real, sin depender necesariamente de textos previamente aprobados.

ANDI y **CCIT** también sostienen que los servicios digitales modifican textos, idiomas, variables y enlaces de manera continua y a gran escala, por lo que exigir una plantilla aprobada por mensaje o campaña podría ser incompatible con flujos automatizados y con la personalización legítima.

Al respecto, la CRC reconoce que los servicios digitales utilizan cada vez más mecanismos automatizados, inteligencia artificial, analítica de datos y herramientas dinámicas para prevenir incidentes de seguridad. No obstante, la existencia de estos mecanismos no elimina la necesidad de adoptar reglas regulatorias específicas cuando la evidencia demuestra que las medidas generales vigentes no han sido suficientes para contener el crecimiento del fraude que afecta a los usuarios.

En efecto, la regulación vigente contempla reglas amplias y flexibles para que los distintos actores de la cadena de valor implementen mecanismos de mitigación del fraude. Sin embargo, la realidad observada evidencia que las afectaciones a los usuarios continúan aumentando y que las modalidades de fraude se adaptan de manera constante a los controles existentes. Precisamente por esa razón se justificó el inicio del presente proyecto regulatorio, orientado a fortalecer la trazabilidad, la identificación del remitente, los controles sobre intermediarios y la validación de las comunicaciones A2P.

El hecho de que existan herramientas dinámicas no impide que las comunicaciones cursadas por el canal SMS A2P deban contar con una estructura verificable. La CRC considera que la plantilla no impone un texto rígido e inmodificable para cada mensaje, sino una referencia estructural que permite verificar que el mensaje corresponde a una finalidad, modalidad y patrón declarado. En esa medida, el uso de campos variables, parámetros dinámicos o mensajes automatizados puede coexistir con el régimen de plantillas, siempre que se mantenga la coherencia con la modalidad declarada y se preserve la trazabilidad del tráfico.

Adicionalmente, el modelo propuesto no se agota en reglas estáticas. El proyecto prevé espacios de coordinación, intercambio de información y seguimiento técnico, incluyendo el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles —CTLFSM—, dentro del cual los diferentes actores podrán compartir información, analizar nuevas modalidades de fraude y diseñar estrategias de respuesta más ágiles que el tránsito propio de una modificación regulatoria. Este espacio permite flexibilizar el sistema y adaptar las medidas preventivas a la evolución de las amenazas, sin renunciar a los elementos mínimos de trazabilidad exigibles en el canal A2P.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de sustituir el régimen de plantillas por modelos dinámicos no sujetos a validación previa y, en consecuencia, se mantiene la obligación de que los mensajes A2P estén asociados a plantillas aprobadas y vigentes, sin perjuicio de que los agentes puedan utilizar campos variables, mecanismos automatizados y estrategias coordinadas en el marco del CTLFSM, siempre que se respete la estructura, finalidad y modalidad declarada.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.6.3 Revisión del contenido estático y dinámico de las plantillas, privacidad y confidencialidad de la información

ANDI y **CCIT** señalan que el proyecto prevé que el validador revise el contenido estático y el sentido del contenido dinámico de la plantilla, lo cual podría resultar incompatible con servicios que modifican textos, variables, enlaces, idiomas o campos personalizados de manera continua y a gran escala. En particular, advierten que en mensajes como OTP, autenticación o confirmaciones transaccionales, el contenido dinámico es por definición variable e impredecible. El documento base recoge que estos agentes cuestionan que el validador revise el contenido estático y el sentido del contenido dinámico, así como que ningún mensaje A2P pueda cursarse sin plantilla aprobada y vigente.

BLIPBLIP, **NEXVIA** e **INALAMBRIA**, por su parte, sostienen que someter el contenido de las comunicaciones empresariales a la aprobación de un tercero podría limitar la libertad de comunicación de empresas e individuos, exponer información sensible y generar riesgos de privacidad. En línea similar, **ANDI** recomienda limitar los procesos de validación a metadatos o elementos estructurales, evitando el acceso al contenido completo cuando no sea necesario, y prohibir el almacenamiento de datos sensibles como códigos OTP u otros factores de autenticación.

La tendencia de los comentarios es coincidente en pedir claridad sobre el alcance real de la revisión que realiza el validador, especialmente para evitar que se entienda como una revisión material del contenido final del mensaje o como acceso a información confidencial, personalizada o sensible del usuario.

Al respecto, la CRC considera pertinente precisar el alcance de la revisión prevista en el proyecto. El artículo 6.13.1.5.4 dispone que el validador centralizado debe:

> «Recibir, revisar y aprobar o rechazar las plantillas de contenido A2P que los asignatarios de SENDER ID sometan a su consideración conforme a la Sección 4 del presente capítulo. La revisión implica la validación del contenido estático y el sentido del contenido dinámico de la plantilla, para que corresponda con la modalidad declarada de los mensajes.»

Esta disposición no debe entenderse como una habilitación para que el validador revise, controle o apruebe el contenido final de cada mensaje individual que será enviado al usuario. Tampoco implica que el validador acceda al valor concreto de los campos dinámicos, tales como códigos OTP, referencias transaccionales, identificadores de operación, montos, nombres, claves, credenciales o cualquier otro dato personalizado que sea incorporado al momento efectivo del envío del mensaje.

La revisión prevista en el proyecto corresponde a un control de coherencia estructural y funcional entre la plantilla, los campos variables, la modalidad declarada y la finalidad del mensaje. En otras palabras, el validador debe verificar que la estructura de la plantilla sea compatible con la categoría declarada —por ejemplo, autenticación, transaccional, comercial, regulatoria o de seguridad— y que los campos dinámicos no permitan alterar sustancialmente esa finalidad.

Así, cuando la disposición se refiere al «sentido del contenido dinámico», la CRC aclara que no se trata de validar el significado específico de cada mensaje individual, sino de verificar que los campos variables declarados sean coherentes con la modalidad de la plantilla. Por ejemplo, en una plantilla de autenticación, un campo dinámico puede corresponder al código OTP o a una referencia de operación; lo que debe verificar el validador es que dicho campo sea funcionalmente compatible con una comunicación de autenticación, y no que el código específico o la información personalizada sean revisados, almacenados o aprobados por el validador.

En este sentido, la CRC no comparte la afirmación según la cual el régimen de plantillas implique acceso del validador al contenido final que se entrega a los usuarios. Las plantillas son estructuras genéricas de mensaje y no deberían contener información confidencial del usuario final ni datos sensibles. Si bien el validador es el encargado de aprobar las plantillas genéricas, en ningún momento tiene acceso al contenido concreto finalmente enviado a cada usuario.

Esto es especialmente relevante en el caso de mensajes OTP o similares. Bajo la estructura propuesta, el OTP hace parte de un campo dinámico de la plantilla. El validador puede conocer que la plantilla contiene un campo dinámico destinado a incorporar un código de autenticación, pero no accede al valor específico de ese código, ni lo almacena, ni lo valida individualmente. Por tanto, no existe, bajo el diseño regulatorio propuesto, un escenario en el que el validador tenga acceso al OTP concreto recibido por el usuario.

La CRC considera que esta precisión permite armonizar dos objetivos regulatorios: por una parte, preservar la trazabilidad del tráfico A2P y verificar que los mensajes correspondan a la modalidad declarada; y, por otra, evitar interpretaciones según las cuales el validador realiza un control material del contenido final o accede a información personalizada, confidencial o sensible. Adicionalmente, el proyecto contempla prohibiciones y obligaciones aplicables al validador centralizado en materia de uso de información, incluyendo restricciones a la divulgación o comercialización de información de los agentes registrados.

Teniendo en cuenta lo anterior, la CRC acepta parcialmente los comentarios, en el sentido de precisar el alcance de la revisión del contenido estático y del sentido del contenido dinámico de las plantillas. En consecuencia, se aclara en los artículos 6.13.4.2.4 y 6.13.4.3.1 que los originadores de contenido deben declarar la información asociada a códigos OTP, referencias transaccionales, identificadores de operación u otros datos personalizados como variables dentro de la plantilla para garantizar la confidencialidad de la información, y adicionalmente se indica que la revisión por el validador corresponde a un control de coherencia entre la estructura de la plantilla, la modalidad declarada y los campos variables, y no a una revisión material del contenido final de cada mensaje ni al acceso a valores específicos de campos dinámicos.

No obstante, la CRC no acepta la solicitud de eliminar o modificar el régimen de plantillas por razones de privacidad o confidencialidad, en la medida en que el diseño propuesto no supone que el validador acceda al contenido final enviado al usuario ni a información sensible como códigos OTP, credenciales,

claves, factores de autenticación o datos personalizados. La validación se limita a la plantilla genérica, a su estructura y a la coherencia de los campos variables con la modalidad declarada.

2.6.4 Vigencia mensual, renovación automática y desactivación de plantillas

ANDI y **CCIT** manifiestan que la vigencia mensual renovable y las causales de desactivación podrían introducir incertidumbre operativa para servicios críticos. **BLIPBLIP**, **NEXVIA** e **INALAMBRIA** sostienen que la vigencia y renovación mensual de las plantillas impone una carga operativa permanente a toda la cadena, reduce la productividad y encarece el canal.

Al respecto, el proyecto de resolución dispone que las plantillas aprobadas tendrán vigencia mensual, pero también establece que dicha vigencia se renovará automáticamente al vencimiento de cada periodo, salvo que el asignatario solicite expresamente su desactivación cuando la campaña o servicio haya concluido, o que el validador detecte un escenario de mal uso de la plantilla.

Por tanto, la vigencia mensual no debe entenderse como una obligación de presentar mensualmente una nueva solicitud de aprobación ni como un trámite recurrente para las plantillas que mantienen sus condiciones y no presentan escenarios de mal uso. La renovación automática permite mantener actualizado el control sobre plantillas activas, sin imponer cargas desproporcionadas a quienes utilizan correctamente el recurso.

La CRC considera que la vigencia mensual renovable cumple una función preventiva razonable, pues permite mantener un mecanismo de seguimiento periódico sobre plantillas activas, especialmente en un entorno en el que las modalidades de fraude cambian rápidamente y las campañas pueden ser utilizadas indebidamente una vez aprobadas. Sustituir este esquema por una vigencia indefinida reduciría la capacidad de control y seguimiento, mientras que la renovación automática mitiga las cargas administrativas que preocupan a los agentes.

Teniendo en cuenta lo anterior, la CRC no acepta la solicitud de sustituir la vigencia mensual por una vigencia anual o indefinida. Se mantiene la regla propuesta de vigencia mensual con renovación automática, en los términos previstos en el proyecto de resolución.

2.6.5 Procedimiento de rechazo de plantillas y mecanismo de revisión o segunda instancia

COLOMBIA FINTECH sostiene que el artículo 6.13.4.3.1 permite que el validador rechace una plantilla mediante comunicación motivada, pero no contempla un procedimiento formal de revisión o segunda instancia para el asignatario que considere injustificado ese rechazo. **BLIPBLIP**, **NEXVIA** e **INALAMBRIA** también advierten que el rechazo de una plantilla puede paralizar la operación sin que exista recurso de reposición ni apelación, lo que, en su criterio, afecta el debido proceso.

Frente a este punto, la CRC no acoge la solicitud de incorporar una segunda instancia o recurso formal frente a cada decisión técnica de rechazo de plantillas. El proyecto ya exige que el rechazo sea comunicado de manera motivada, lo cual permite al solicitante conocer las razones técnicas o regulatorias que impiden la aprobación de la plantilla y proceder a presentar una nueva solicitud.

Adicionalmente, debe tenerse en cuenta que la revisión de plantillas es una actuación técnica dentro del sistema de validación, no una actuación administrativa sancionatoria ni una decisión definitiva de recuperación, suspensión o revocatoria de recursos de identificación. Convertir cada rechazo técnico en un procedimiento de doble instancia podría generar cargas operativas incompatibles con los tiempos de respuesta requeridos por el ecosistema A2P y con la finalidad preventiva del sistema.

Lo anterior no impide que el solicitante subsane la plantilla, presente una nueva versión o ajuste los elementos que dieron lugar al rechazo. En efecto, el diseño del proyecto permite que las plantillas sean modificadas y procesadas nuevamente por el validador, y prevé que durante el trámite de modificación la plantilla original continúe vigente cuando corresponda.

En este orden de ideas, la CRC no acepta la solicitud de incorporar un procedimiento formal de segunda instancia o recurso frente al rechazo de plantillas. Se mantiene la regla según la cual el rechazo debe ser motivado, sin perjuicio de que el solicitante pueda presentar una nueva plantilla o ajustar la información conforme a las razones comunicadas por el validador.

2.6.6 Plantillas de emergencia o campañas urgentes de interés público

En el documento de respuesta a comentarios se identifica una propuesta para crear un mecanismo expreso de plantillas de emergencia para campañas urgentes de interés público. **BLIPBLIP**, **NEXVIA** e **INALAMBRIA** también advierten que un comercio que necesite enviar una promoción inmediata o una entidad de salud que deba alertar sobre un riesgo sanitario urgente quedarían sujetos a un trámite de aprobación, lo que podría afectar la oportunidad de la comunicación.

Al respecto, la CRC no considera procedente crear una categoría autónoma de plantillas de emergencia. El régimen propuesto ya permite registrar plantillas, modificar plantillas existentes y mantener vigente la plantilla original durante el trámite de modificación, lo que brinda un margen operativo suficiente para gestionar ajustes o comunicaciones asociadas a servicios previamente registrados.

Crear una vía excepcional para plantillas de emergencia podría abrir espacios de uso indebido, generar incentivos para clasificar campañas ordinarias como urgentes y debilitar la eficacia preventiva del sistema. Además, en el caso de campañas comerciales, la necesidad de oportunidad no justifica exceptuar los controles de trazabilidad, especialmente cuando el canal A2P ha sido utilizado para fraudes que aprovechan precisamente mensajes urgentes, promociones falsas o alertas engañosas.

En el caso de comunicaciones de interés público, salud, seguridad o gestión de riesgos, los agentes podrán estructurar plantillas previamente registradas con campos variables que permitan adaptar la

información específica al evento correspondiente, sin necesidad de crear una excepción general al régimen.

Por lo anterior, la CRC no acepta la solicitud de crear un mecanismo autónomo de plantillas de emergencia. Se mantiene el esquema general de registro, modificación y validación de plantillas previsto en el proyecto.

2.6.7 Costos, cargas operativas y productividad del canal

BLIPBLIP, **NEXVIA** e **INALAMBRIA** afirman que la vigencia y renovación mensual de plantillas impone una carga operativa permanente a toda la cadena, reduce la productividad y encarece el canal. **ANDI** y **CCIT** también señalan que el esquema introduce latencia, costos y fragilidad operativa, especialmente frente a servicios digitales que modifican textos, variables y enlaces a gran escala.

Al respecto, es preciso mencionar que la CRC no desconoce que el régimen de plantillas implica cargas operativas para los agentes que cursan tráfico A2P. Sin embargo, dichas cargas resultan proporcionales frente al riesgo que se busca mitigar y a la necesidad de proteger a los usuarios frente a modalidades de fraude cada vez más sofisticadas.

El canal SMS A2P es utilizado para comunicaciones de alto impacto, incluyendo mensajes transaccionales, alertas de seguridad, autenticación, comunicaciones comerciales y notificaciones operativas. La falta de controles sobre la estructura y finalidad de los mensajes puede facilitar el uso de identificadores legítimos para enviar comunicaciones engañosas, incluyendo aquellas que incorporan enlaces maliciosos o instrucciones orientadas a capturar información del usuario.

Además, como se indicó, la vigencia mensual se renueva automáticamente cuando no se configura una causal de desactivación, por lo que no implica necesariamente una carga recurrente de aprobación para cada periodo. La carga regulatoria debe evaluarse frente al beneficio de contar con un sistema preventivo capaz de identificar desviaciones en el uso de plantillas, controlar la inclusión de elementos de riesgo y fortalecer la trazabilidad de las comunicaciones.

Así las cosas, la CRC no acepta la solicitud de modificar o eliminar el régimen de plantillas por razones de costo, carga operativa o productividad del canal y, en consecuencia, se mantiene el esquema propuesto por considerarse necesario, idóneo y proporcional frente a los riesgos identificados en el proyecto regulatorio.

2.6.8 Duplicidad con SENDER ID, Ley 2300 y otros controles

BLIPBLIP, **NEXVIA** e **INALAMBRIA** sostienen que el régimen de plantillas duplica obligaciones ya existentes, en particular aquellas asociadas a la identificación del remitente mediante SENDER ID y a otros controles normativos.

La CRC no comparte la afirmación de que el régimen de plantillas duplique el SENDER ID u otros mecanismos de control. Cada elemento del esquema cumple una función diferenciada y complementaria. El código corto A2P identifica el canal técnico mediante el cual se cursa el tráfico. El SENDER ID identifica al responsable del contenido frente al usuario. La plantilla permite verificar que el mensaje enviado corresponde a una finalidad, modalidad y estructura previamente declaradas.

El SENDER ID por sí solo permite conocer quién aparece como remitente, pero no permite controlar si el contenido enviado corresponde a la finalidad declarada, si incluye URL no previstas, si modifica la modalidad autorizada o si incorpora elementos que puedan facilitar fraudes. De la misma manera, la existencia de reglas sobre contacto comercial o protección de datos no reemplaza la necesidad de contar con mecanismos técnicos de trazabilidad sobre el contenido estructural de los mensajes A2P.

Por tanto, el régimen propuesto no reproduce controles existentes, sino que articula distintos niveles de verificación para cerrar brechas identificadas en el ecosistema de mensajería: identificación del canal, identificación del remitente y consistencia estructural del mensaje.

En este sentido, la CRC no comparte la afirmación de que el régimen de plantillas duplique el SENDER ID, la Ley 2300 u otros controles y, en consecuencia, se mantiene el esquema de código corto A2P, SENDER ID y plantilla como elementos complementarios del sistema de validación y trazabilidad del tráfico A2P.

2.6.9 Especificaciones técnicas de la plantilla, plazos de validación y comentarios individuales adicionales

ANDESCO y **CLARO** señalaron que el proyecto contempla la implementación de una plantilla de contenido A2P sin definir su estructura, contenido mínimo, campos de información, reglas de intercambio ni especificaciones técnicas del formato mediante el cual se realizarían las consultas y respuestas, y solicitaron que la CRC incorpore un modelo de plantilla o especificación funcional detallada y la someta a comentarios de la industria. Ambos agentes solicitaron, además, que la validación y aprobación de plantillas por parte del validador centralizado se realice en un plazo máximo de veinticuatro (24) horas. **ANDESCO** cuestionó adicionalmente que la verificación previa al enrutamiento de cada mensaje A2P, prevista en el artículo 6.13.4.7.2, resulte compatible con la arquitectura y la capacidad de procesamiento de los SMSC de los operadores móviles.

Por su parte, **JULIO NULDEMAR** propuso adicionar un parágrafo que excluya del ámbito de aplicación de la resolución, y por ende de las obligaciones de registro de SENDER ID y de validación previa de plantillas, las comunicaciones de naturaleza informativa, operativa, regulatoria o de atención al cliente emitidas por los PRSTM —incluidos los operadores móviles virtuales— hacia sus propios usuarios finales, tanto cuando se utilice numeración móvil convencional como cuando se empleen canales digitales propietarios. **SAEM**, a su turno, invocó la experiencia de la India, donde la entrada en operación de la verificación de plantillas habría producido el bloqueo masivo de mensajes legítimos, incluidos OTP bancarios, al punto de exigir su suspensión temporal por el regulador.

La tendencia de estos comentarios es propositiva en lo relativo a las especificaciones técnicas y a los plazos, y disidente en cuanto al ámbito de aplicación del régimen de plantillas.

Frente a la solicitud de definir en la resolución la estructura, los campos y las especificaciones técnicas de la plantilla, la CRC no la acoge. El artículo 6.13.4.2 del proyecto establece la información que debe contener la plantilla de contenido A2P, con el nivel de detalle propio de un acto administrativo de carácter general. La definición de formatos de intercambio, reglas de integración, especificaciones de las APIs y demás elementos de implementación no debe incorporarse en el texto regulatorio, pues corresponde a materia técnica sujeta a evolución permanente, cuya rigidez en la resolución dificultaría su adaptación frente a los cambios del ecosistema y a las nuevas modalidades de fraude. Como se indicó en otros apartes de este documento, dichos aspectos serán desarrollados en el marco del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles —CTLFSM—, con la participación del validador centralizado y de los agentes del ecosistema, escenario en el cual los PRSTM y los asignatarios de recursos podrán incidir en su definición.

En cuanto a la solicitud de reducir a veinticuatro (24) horas el plazo de validación y aprobación de plantillas, la Comisión tampoco la acoge. El plazo previsto en el numeral 6.13.4.3.1 constituye ya un término breve y su reducción uniforme comprometería la calidad de la verificación en un procedimiento cuya finalidad es precisamente identificar estructuras de contenido susceptibles de uso fraudulento, particularmente en lo relativo a la declaración de URL. A ello se suma que el régimen adoptado mitiga el impacto operativo del plazo mediante la renovación automática de las plantillas vigentes, la permanencia de la plantilla original durante el trámite de modificación y el registro simplificado, categórico o parametrizado de las modalidades sensibles al tiempo. Sin perjuicio de lo anterior, el seguimiento a los tiempos efectivos de respuesta del validador centralizado hace parte de las funciones de las instancias de coordinación previstas en la resolución.

Respecto de la observación de **ANDESCO** sobre la validación previa al enrutamiento de cada mensaje, la Comisión precisa que el artículo 6.13.4.7.2 no impone una arquitectura específica ni exige necesariamente una consulta unitaria y en línea al validador centralizado por cada mensaje cursado. La obligación consiste en integrar las plataformas de mensajería con el sistema de información del validador a través de las APIs disponibles y en verificar, antes del enrutamiento, la validez del código corto A2P, del SENDER ID y de la plantilla asociados al mensaje, finalidad que puede alcanzarse mediante mecanismos de sincronización, réplica local de los registros y actualizaciones incrementales, según se desarrolla en el capítulo denominado «Validador centralizado: forma de selección, competencias y funciones». Los parámetros de desempeño, latencia y sincronización serán objeto de definición técnica en el CTLFSM. En consecuencia, no se acepta la solicitud de modificar la obligación prevista en el artículo 6.13.4.7.2.

En relación con la propuesta de **JULIO NULDEMAR**, la Comisión reitera lo expuesto en el capítulo denominado «Sender ID», en el sentido de que el ámbito de aplicación del proyecto se circunscribe a las comunicaciones cursadas mediante los servicios y recursos regulados, de manera que los canales

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

propietarios o cerrados del operador —notificaciones push integradas en aplicaciones, servicios basados en applets o STK y mecanismos análogos— no quedan comprendidos en las obligaciones de registro de SENDER ID y de validación de plantillas. No ocurre lo mismo, en cambio, con las comunicaciones que los PRSTM y los operadores móviles virtuales cursen hacia sus usuarios mediante SMS, las cuales corresponden a tráfico A2P y no pueden exceptuarse del esquema de trazabilidad sin abrir una vía de elusión que comprometería la eficacia del conjunto de las medidas, máxime cuando la suplantación de la identidad de los propios proveedores es una de las modalidades de fraude identificadas en el diagnóstico. La continuidad de las comunicaciones asociadas al cumplimiento de obligaciones regulatorias se encuentra atendida mediante la asignación de oficio del SENDER ID prevista en el capítulo denominado «Régimen de transición». Por lo anterior, no se acepta la adición del parágrafo propuesto.

Frente a la referencia de **SAEM** a la experiencia de la India, la Comisión advierte que dicha experiencia fue analizada en el capítulo denominado «Tratamiento de mensajes OTP, autenticación, seguridad y comunicaciones críticas», del cual se desprende que el regulador indio no eliminó el esquema de registro de plantillas sino que ajustó su implementación, y que los mensajes de autenticación se gestionan mediante plantillas transaccionales con campos variables. Las dificultades de despliegue invocadas por el agente se atienden en el diseño adoptado mediante el registro simplificado, categórico o parametrizado de plantillas, la ampliación del período de transición decidida en el capítulo denominado «Régimen de transición» y las pruebas de interoperabilidad que se adelantarán en el marco del CTLFSM. En consecuencia, no se acepta la solicitud de eliminar o flexibilizar el régimen de plantillas con fundamento en dicha experiencia comparada.

Finalmente, en relación con los comentarios individuales restantes, la Comisión precisa lo siguiente. La preocupación de **PTC** sobre la protección de la información comercial sensible de los generadores de contenido fue atendida en el aparte relativo a la revisión del contenido estático y dinámico de las plantillas, en el cual se precisó que la verificación no recae sobre el contenido final del mensaje; su propuesta de sustituir el registro de plantillas por una certificación emitida por el integrador tecnológico no se acepta, por cuanto trasladaría la verificación al agente vigilado y eliminaría la trazabilidad centralizada que constituye el núcleo del esquema; y su solicitud sobre la periodicidad de actualización se encuentra resuelta mediante la regla de vigencia mensual con renovación automática. La solicitud de **SUMA** de eliminar toda disposición que habilite la evaluación del contenido de los mensajes no se acepta, en los términos expuestos en el aparte sobre la naturaleza del esquema de plantillas, sin perjuicio del ajuste adoptado respecto de la homogeneidad del contenido en el tráfico P2P, explicado en el capítulo denominado «Tráfico P2P». La observación de **SINCH** sobre la pérdida de agilidad para el lanzamiento de campañas coyunturales se responde en el aparte relativo a la rigidez del modelo frente a servicios digitales dinámicos. Y las preguntas de **CRISTIAN CANTILLO** sobre el tratamiento de las comunicaciones operativas, regulatorias y de servicio al cliente de los propios operadores y sobre los canales utilizados por los operadores móviles virtuales fueron resueltas en el capítulo denominado «Sender ID», en el aparte relativo al ámbito de aplicación frente a canales distintos de SMS y USSD.

Con fundamento en lo anterior, la CRC no acepta las solicitudes analizadas en el presente aparte y, en consecuencia, se mantiene el régimen de plantillas de contenido A2P en los términos propuestos, con los ajustes expresamente señalados en los apartes precedentes de este capítulo.

2.7 Obligación de constituir una sucursal en Colombia y cargas para sociedades internacionales

ANDI

Dice que el Parágrafo 2 del artículo 6.12.1.2 dispone que «a cada persona natural o jurídica le será asignado un único SENDER ID»; solo se asignará «un SENDER ID por NIT o por cédula»; y los solicitantes extranjeros podrán ser asignatarios «siempre que hayan establecido una sucursal en Colombia». La exigencia de sucursal se reitera en el numeral 6.12.2.1.1 del Proyecto de Resolución.

Sostiene que la exigencia de establecer una sucursal en el país como condición para enviar mensajes de autenticación y seguridad a usuarios en Colombia resulta desproporcionada y potencialmente discriminatoria frente a los proveedores extranjeros. En su opinión, obligar a una presencia local permanente para el ejercicio de una función puramente técnica de identificación no es una medida proporcional y, de hecho, impone una carga estructural gravosa que no guarda relación de necesidad ni con el fin de identificar al remitente.

Adicionalmente, dice que esta obligación puede generar tensiones con los compromisos internacionales asumidos por Colombia en materia de comercio transfronterizo de servicios. En particular, el TLC con Estados Unidos contempla disciplinas orientadas a evitar que la prestación transfronteriza de servicios sea condicionada a la obligación de establecer presencia local en el territorio de la otra parte. Por ello, una medida que exige a proveedores extranjeros constituir una sucursal en Colombia como condición para acceder al SENDER ID y cursar mensajes A2P podría ser incompatible con dichos compromisos.

Finalmente, dice que la exigencia de una sucursal obligatoria puede desincentivar la prestación de servicios de seguridad desde el exterior y podría impedir o desincentivar que ciertos proveedores globales mantengan el SMS como canal de autenticación en Colombia, llevando a los usuarios a alternativas menos seguras o reduciendo la disponibilidad de mecanismos de autenticación robusta en el país lo que afectaría la seguridad del ecosistema digital, que el propio Proyecto pretende proteger.

AMCHAM

Considera indispensable evaluar el impacto de las cargas operativas derivadas del modelo propuesto, especialmente para proveedores de servicios digitales transfronterizos que operan bajo esquemas globales de soporte, seguridad y autenticación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Dice que el proyecto, al exigir la validación periódica de plantillas y la resolución de rechazos en plazos reducidos, de 24 a 48 horas, puede imponer de facto la necesidad de contar con una estructura operativa local, en idioma español y con disponibilidad permanente para interactuar con el Validador.

A su juicio, si bien la atención oportuna de incidentes es relevante, el diseño de estas obligaciones debe ser proporcional y considerar las diferencias entre operadores locales de telecomunicaciones, agregadores, proveedores de contenido, plataformas digitales y servicios globales de autenticación.

Adiciona que, para los proveedores de servicios digitales transfronterizos, estas exigencias pueden generar cargas desproporcionadas cuando se combinan con requisitos adicionales, como la eventual obligación de establecer una sucursal en Colombia para acceder al SENDER ID. En la práctica, dice **AMCHAM**, esto podría obligar a las empresas a crear estructuras operativas dedicadas exclusivamente al cumplimiento de un proceso local de validación de plantillas, sin que exista una relación clara entre esa carga y una mejora técnica efectiva en la seguridad del usuario.

Advierte que una carga operativa excesiva puede producir efectos no deseados. Dice que algunos proveedores podrían limitar o descontinuar el uso de canales SMS o USSD para autenticación en Colombia, restringir la disponibilidad de ciertos servicios digitales, demorar procesos de verificación o migrar hacia mecanismos menos accesibles para determinados usuarios. Sostiene que, en lugar de fortalecer la seguridad, estas consecuencias podrían aislar a los usuarios colombianos de estándares globales de autenticación y protección.

AMCHAM dice que la disponibilidad de servicios digitales 24/7 depende de arquitecturas globales altamente automatizadas, con equipos distribuidos, sistemas de monitoreo continuo y protocolos de respuesta inmediata. En su opinión, imponer procesos manuales, locales o dependientes de validaciones previas puede afectar la eficiencia de estos modelos y reducir la capacidad de reacción frente a incidentes de seguridad. Por ello, sugiere que la CRC incorpore criterios de proporcionalidad, gradualidad y reconocimiento de modelos operativos globales en la definición de las obligaciones aplicables.

En este sentido, **AMCHAM** recomienda que las obligaciones asociadas a plantillas, validaciones, soporte y tiempos de respuesta sean revisadas para permitir esquemas automatizados, integraciones técnicas directas y mecanismos de cumplimiento basados en riesgo. Esto permitiría, a su juicio, preservar la protección del usuario sin imponer cargas que puedan afectar la disponibilidad de servicios digitales seguros en el país.

CCIT

Formula, en términos idénticos a la ANDI, que la exigencia de sucursal para los solicitantes extranjeros (Parágrafo 2 del artículo 6.12.1.2 y numeral 6.12.2.1.1) es desproporcionada y potencialmente discriminatoria, puede ser incompatible con los compromisos del TLC con Estados Unidos en materia de comercio transfronterizo de servicios y puede desincentivar que los proveedores globales mantengan el SMS como canal de autenticación en Colombia, afectando la seguridad del ecosistema digital.

SAEM

Señala que la exigencia de sucursal a los extranjeros, sin un régimen claro de representación, puede excluir a anunciantes legítimos del exterior y trasladar su tráfico a agregadores grises. Propone prever un procedimiento expedito y un canal de representación para anunciantes extranjeros que no implique necesariamente sucursal (por ejemplo, un representante o responsable local solidario).

CLARO

En cuanto a los A2P internacionales, afirma que queda la duda sobre la identificación del originador para asignarle un SENDER ID, dado que al operador o carrier al que se le asigna el código corto, este lo use para el envío de todos los clientes que tenga. Señala que, si para mensajería internacional se requiere un Sender ID dedicado para cada uno, se debe tener en cuenta que no se tiene acceso a los clientes de los integradores y que estos no están domiciliados en Colombia para que hagan solicitud del Sender ID directamente a la CRC. Expone que es preciso que la CRC indique la forma en que se va a asignar un Sender ID en estos casos, sabiendo además que en los tramos internacionales puede haber varios carriers o integradores como sucede con las llamadas, de manera que identificar el comercio como tal, no es posible en su condición de operador de telefonía.

Indica que la lista DNO también exigirá integración con sistemas de voz y numeración para bloquear CLI no válidos y que se deberá tener en cuenta el desarrollo de procesos internos, ajustes de sistemas, validaciones documentales, lo que también puede aumentar los tiempos de activación de servicios y los costos de cumplimiento asociados a revisiones KYC y trazabilidad, por lo que expone que el nuevo modelo puede exigir ajustes contractuales y operativos con integradores y clientes que actualmente utilizan códigos cortos bajo esquemas comerciales existentes.

Expone que implementar la prevención del fraude sobre las plataformas existentes, generará un sobrecosto e incremento de actividades al interior de su compañía, por lo que es inminente que se revise el mercado de A2P, previo a cualquier modificación.

En resumen, plantea, respecto de los A2P internacionales, la duda sobre cómo identificar al originador para asignarle un SENDER ID, dado que el operador o carrier al que se le asigna el código corto lo usa para el envío de todos sus clientes; advierte que, si para los internacionales se requiere un SENDER ID dedicado por cliente, debe tenerse en cuenta que no se tiene acceso a los clientes finales de los agregadores internacionales.

Respuesta CRC:

Revisadas las intervenciones, la Comisión identifica una tendencia mayoritaria y convergente, integrada por **ANDI**, **CCIT** y **SAEM**, y respaldada en lo esencial por **AMCHAM**, que cuestiona la exigencia, contenida en el Parágrafo 2 del artículo 6.12.1.2 y reiterada en el numeral 6.12.2.1.1, de que los

solicitantes extranjeros hayan establecido una sucursal en Colombia como condición para ser asignatarios de un SENDER ID. Dentro de esa tendencia se distinguen tres líneas argumentativas: (i) la que reprocha la desproporción y el eventual carácter discriminatorio de la medida frente a proveedores extranjeros y su posible tensión con los compromisos de comercio transfronterizo de servicios (**ANDI** y **CCIT**, en términos idénticos); (ii) la que, sin oponerse al fondo, propone una alternativa menos gravosa consistente en un canal de representación local que no implique necesariamente sucursal (**SAEM**); y (iii) la que, desde la perspectiva de las cargas operativas de los modelos globales, advierte que la combinación de la exigencia de sucursal con las obligaciones de validación de plantillas puede forzar estructuras locales desproporcionadas (**AMCHAM**).

De manera separada, **CLARO** formula una inquietud operativa específica sobre la identificación del originador y la asignación del SENDER ID en el tráfico A2P internacional cursado a través de múltiples carriers e integradores, que por su naturaleza recibe respuesta independiente. La Comisión responde a continuación.

2.7.1 Sobre la identificación del originador y la asignación del SENDER ID en el tráfico A2P internacional (CLARO)

CLARO plantea una inquietud de orden operativo: en el tráfico A2P internacional, el código corto se asigna al operador o carrier, quien lo utiliza para cursar el tráfico de todos sus clientes; por ello, pregunta cómo se asignará el SENDER ID cuando el originador esté en el exterior, considerando que el operador no tiene acceso a los clientes de los integradores, que estos no están domiciliados en Colombia para solicitar directamente el recurso a la CRC, y que en los tramos internacionales pueden intervenir varios carriers o integradores, de modo que identificar al comercio originador no siempre le resulta posible.

Adicionalmente, **CLARO** advierte sobre los sobrecostos de implementación —integración de la lista DNO con los sistemas de voz y numeración, ajustes de sistemas, validaciones documentales, tiempos de activación y adecuaciones contractuales con integradores y clientes— y solicita que se revise el mercado de A2P previamente a cualquier modificación.

La Comisión precisa, en primer lugar, que la arquitectura del nuevo régimen ofrece respuesta a la inquietud sobre la identificación del originador internacional, y que dicha respuesta se articula, justamente, con la flexibilización adoptada en este capítulo. En el modelo propuesto, todo mensaje A2P dirigido a usuarios en Colombia —de origen nacional o internacional— debe estar identificado con un SENDER ID cuyo asignatario es el responsable de la producción del contenido, y ese SENDER ID se cursa a través del código corto A2P del agente con el que el asignatario mantiene relación contractual. Para el originador domiciliado en el exterior, la vía de asignación implica la solicitud y titularidad del recurso a través de un responsable local —sucursal o representante o mandatario domiciliado en Colombia— que responde por su uso. De este modo, el régimen no traslada al PRSTM ni al carrier la carga de identificar individualmente al comercio originador en el exterior: esa identificación se resuelve en el momento de la asignación del SENDER ID al responsable, de manera previa al cursado del tráfico,

y se preserva a lo largo de la cadena mediante el propio recurso de identificación que acompaña al mensaje.

2.8 Tratamiento de mensajes OTP, autenticación, seguridad y comunicaciones críticas

ANDI

Dice que el Proyecto establece obligaciones sobre quienes generan mensajes de autenticación (OTP), segundo factor (2FA), verificación de identidad, alertas de seguridad y comunicaciones transaccionales. Añade que estas comunicaciones son, en muchos casos, parte intrínseca de servicios digitales prestados por actores distintos a los proveedores de redes y servicios de telecomunicaciones, e incluso de desde fuera del país.

Frente a lo anterior, indica que la autenticación multifactor mediante OTP y 2FA es una de las medidas de seguridad más utilizadas para mitigar la apropiación de cuentas, la suplantación y el fraude en internet. El Proyecto somete estos mensajes al mismo aparato de plantillas obligatorias, aprobación previa, validación anual y eventual bloqueo aplicable a otras modalidades de mensajería A2P.

Aunque el Proyecto reconoce que los mensajes de autenticación y seguridad tienen una naturaleza especial y no requieren consentimiento adicional, dicha diferenciación pierde eficacia si, en la práctica, estos mensajes quedan sujetos al mismo esquema de validación previa y bloqueo operativo que las comunicaciones comerciales o publicitarias.

En este sentido, la **ANDI** sostiene que el Proyecto de Resolución desconoce que cada uno de esos pasos introduce latencia, costos y puntos de falla en una cadena que debe ser instantánea y de altísima disponibilidad, especialmente teniendo en cuenta que su finalidad es proteger las cuentas de los usuarios. Si un OTP no se entrega por falta de plantilla vigente, por una desactivación, por una caída del validador o por un bloqueo del PRST, el usuario no podrá iniciar sesión, recuperar su cuenta ni autenticar el uso de su cuenta.

Dice que el efecto previsible podría ser no menos fraude, sino más exposición a usuarios bloqueados, migración a factores menos seguros y mayor superficie para el fraude de cuentas. Una medida concebida para mitigar el fraude no debe perjudicar la herramienta que más lo previene y afectar desproporcionadamente medidas de seguridad reconocidas como eficaces internacionalmente.

En ese sentido, la **ANDI** sostiene que es esencial distinguir con precisión entre (i) las comunicaciones legítimas de autenticación y seguridad, solicitadas por el propio usuario o derivadas de un servicio contratado, y (ii) las prácticas fraudulentas de phishing, smishing, suplantación de marca, ingeniería social, malware, SIM swapping, granjas de SIM. El OTP y el 2FA son mecanismos reconocidos de respuesta al fraude, no su causa. Por lo tanto, imponerles barreras podría generar riesgos de seguridad adicionales para el ecosistema digital.

Adicionalmente, considera necesario que el Proyecto incorpore un tratamiento diferenciado para las comunicaciones críticas asociadas a servicios financieros, especialmente aquellas utilizadas para autenticación reforzada, códigos OTP, alertas transaccionales, confirmación de identidad, bloqueo preventivo de productos y notificaciones de seguridad. Estas comunicaciones cumplen una función distinta a la mensajería comercial o publicitaria, pues hacen parte de la arquitectura de prevención del fraude y permiten reaccionar oportunamente frente a operaciones sospechosas, apropiación de cuentas o intentos de suplantación. Por ello, la **ANDI** dice que no deberían quedar sometidas, sin distinción, a reglas que puedan introducir latencia, indisponibilidad, bloqueos automáticos o etiquetados negativos que afecten su entrega oportuna.

En complemento de lo anterior, la **ANDI** dice que el artículo 6.12.1.3.1 establece que los mensajes de autenticación y seguridad (OTP, alertas de inicio de sesión, confirmaciones) se generan a solicitud del usuario y no requieren consentimiento adicional. No obstante, señala que los artículos 6.13.4.1 y 6.13.4.7.2 exigen que todo mensaje A2P (incluida la autenticación) cuente con plantilla aprobada y vigente, y disponen que en su ausencia el PRST podrá bloquear el mensaje o marcarlo como «sin verificar». Al respecto, considera que el Proyecto incurre en una contradicción pues en principio reconoce la naturaleza especial de los mensajes de autenticación y luego los somete al mismo control previo de contenido y a la misma posibilidad de bloqueo que la mensajería comercial o publicitaria.

Indica que estos mensajes son generados a solicitud activa del propio usuario en un momento específico, lo que descarta que se trate de comunicaciones imprevistas o no deseadas que por sí solas puedan generar casos de fraude.

Añade que las características técnicas de estos mensajes hacen de difícil cumplimiento algunas de las medidas propuestas por la CRC. Los OTP contienen variables dinámicas, son sensibles al tiempo y se cursan en volúmenes elevados con exigencias de disponibilidad casi absoluta. Aunque el Proyecto no necesariamente exige aprobar el valor exacto de cada OTP, sí somete la plantilla, el contenido estático, el sentido del contenido dinámico y el enrutamiento del mensaje a un esquema de validación previa y consulta operativa que puede generar falsos bloqueos, latencia o indisponibilidad. La aprobación previa, la vigencia mensual de la plantilla (incluso si es de renovación automática) y la consulta en tiempo real al validador antes de enrutar cada mensaje añaden latencia y barreras para su adecuado funcionamiento.

De hecho, dice que cualquier interrupción en la entrega de un OTP impide, por ejemplo, el inicio de sesión o la recuperación de cuenta.

Entonces, señalada que el costo de un falso bloqueo de un mensaje de seguridad es muy superior al de un mensaje comercial no entregado. El efecto de la propuesta sería desconocer la importancia de la herramienta que mejor protege a los usuarios, en contra del propio objetivo del Proyecto de Resolución.

ASOBANCARIA

Sostiene que, sin perjuicio de los beneficios esperados, se encuentra que el Proyecto puede generar riesgos no intencionados que deben evaluarse de manera integral, entre ellos la interrupción de controles antifraude críticos como los OTP´s. Tales riesgos, a su juicio, no derivan necesariamente de fallas en la implementación, sino del diseño mismo de los mecanismos propuestos en el Proyecto, en particular cuando introducen dependencias centralizadas o restricciones operativas sobre canales que hoy cumplen funciones esenciales en la prevención del fraude. Desde el enfoque de gestión de riesgos, **ASOBANCARIA** sugiere especificar la operatividad de los mensajes OTP, de acuerdo a la definición expuesta en el Proyecto, ya que son mecanismos de autenticación y no deberían estar expuestos a interrupciones o demoras en la entrega de su información, con el fin de que las empresas habilitadas para el uso de este mecanismo cumplan con el objetivo de mitigar casos de suplantación, y transferencias no autorizadas, situación que deriva en la pérdida de confianza de los usuarios y la reputación de la entidad.

CCIT

Señala que el Proyecto establece obligaciones sobre quienes generan mensajes de autenticación (OTP), segundo factor (2FA), verificación de identidad, alertas de seguridad y comunicaciones transaccionales. Frente a lo anterior, indica que la autenticación multifactor mediante OTP y 2FA es una de las medidas de seguridad más utilizadas para mitigar la apropiación de cuentas, la suplantación y el fraude en internet. El Proyecto somete estos mensajes al mismo aparato de plantillas obligatorias, aprobación previa, validación anual y eventual bloqueo aplicable a otras modalidades de mensajería A2P. Aunque el Proyecto reconoce que los mensajes de autenticación y seguridad tienen una naturaleza especial y no requieren consentimiento adicional, dicha diferenciación pierde eficacia si, en la práctica, estos mensajes quedan sujetos al mismo esquema de validación previa y bloqueo operativo que las comunicaciones comerciales o publicitarias.

En este sentido, **CCIT** sostiene que el Proyecto de Resolución desconoce que cada uno de esos pasos introduce latencia, costos y puntos de falla en una cadena que debe ser instantánea y de altísima disponibilidad, especialmente teniendo en cuenta que su finalidad es proteger las cuentas de los usuarios. Añade que, si un OTP no se entrega por falta de plantilla vigente, por una desactivación, o por una caída del validador, el usuario no podrá iniciar sesión, recuperar su cuenta ni autenticar el uso de su cuenta.

Sostiene que el efecto previsible podría ser no menos fraude, sino más exposición a usuarios bloqueados, migración a factores menos seguros y mayor superficie para el fraude de cuentas. Una medida concebida para mitigar el fraude no debe perjudicar la herramienta que más lo previene y afectar desproporcionadamente medidas de seguridad reconocidas como eficaces internacionalmente.

Indica que es esencial distinguir con precisión entre: i) las comunicaciones legítimas de autenticación y seguridad, solicitadas por el propio usuario o derivadas de un servicio contratado, y ii) las prácticas fraudulentas de phishing, smishing, suplantación de marca, ingeniería social, malware, SIM swapping,

granjas de SIM. El OTP y el 2FA son mecanismos reconocidos de respuesta al fraude, no su causa. Por lo tanto, concluye que imponerles barreras podría generar riesgos de seguridad adicionales para el ecosistema digital.

En complemento de lo anterior, dice que el artículo 6.12.1.3.1 establece que los mensajes de autenticación y seguridad (OTP, alertas de inicio de sesión, confirmaciones) se generan a solicitud del usuario y no requieren consentimiento adicional. No obstante, los artículos 6.13.4.1 y 6.13.4.7.2 exigen que todo mensaje A2P (incluida la autenticación) cuente con plantilla aprobada y vigente.

Al respecto, **CCIT** dice que se considera que el Proyecto incurre en una contradicción pues en principio reconoce la naturaleza especial de los mensajes de autenticación y luego los somete al mismo control previo de contenido y a la misma posibilidad de bloqueo que la mensajería comercial o publicitaria. Sostiene que estos mensajes son generados a solicitud activa del propio usuario en un momento específico, lo que descarta que se trate de comunicaciones imprevistas o no deseadas que por sí solas puedan generar casos de fraude.

Añade que las características técnicas de estos mensajes hacen de difícil cumplimiento algunas de las medidas propuestas por la CRC. Los OTP contienen variables dinámicas, son sensibles al tiempo y se cursan en volúmenes elevados con exigencias de disponibilidad casi absoluta. Aunque el Proyecto no necesariamente exige aprobar el valor exacto de cada OTP, sí somete la plantilla, el contenido estático, el sentido del contenido dinámico y el enrutamiento del mensaje a un esquema de validación previa y consulta operativa que puede generar falsos bloqueos, latencia o indisponibilidad.

Concluye diciendo que la aprobación previa, la vigencia mensual de la plantilla (incluso si es de renovación automática) y la consulta en tiempo real al validador antes de enrutar cada mensaje añaden latencia y barreras para su adecuado funcionamiento. De hecho, cualquier interrupción en la entrega de un OTP impide, por ejemplo, el inicio de sesión o la recuperación de cuenta. Entonces, el costo de un falso bloqueo de un mensaje de seguridad es muy superior al de un mensaje comercial no entregado. El efecto de la propuesta sería desconocer la importancia de la herramienta que mejor protege a los usuarios, en contra del propio objetivo del Proyecto de Resolución.

COLOMBIA FINTECH

Señala que el artículo 6.13.2.1.2 fija tiempos de respuesta del sistema del validador de 200 ms en promedio. Sin embargo, el artículo 6.13.4.3.1 establece hasta 48 horas para aprobar una plantilla nueva. Concluye que ninguna disposición garantiza que los mensajes de autenticación y seguridad (OTP, alertas de inicio de sesión) lleguen en la ventana de segundos que su naturaleza exige. Advierte que un OTP con 30 segundos de retraso es inútil para el usuario y compromete la seguridad de las operaciones que pretende proteger.

De acuerdo con lo anterior solicita que la CRC establezca un carril prioritario de aprobación de plantillas para la modalidad de autenticación y seguridad (art. 6.12.1.3.1), con un SLA máximo de cuatro (4) horas, y que los PRST estén obligados a priorizar el enrutamiento de los mensajes de esa categoría.

PTC

Señala que el proyecto reconoce, en el artículo 6.12.1.3.1, la naturaleza especial de los mensajes de autenticación y seguridad —como OTP, 2FA, alertas de inicio de sesión, confirmaciones de operaciones y validaciones transaccionales— al indicar que estos se generan a solicitud del usuario y no requieren consentimiento adicional. Según el comentario, esta disposición parte de la premisa correcta de que dichos mensajes cumplen una finalidad funcional y de seguridad, distinta de la mensajería comercial, promocional o publicitaria, pues permiten el acceso seguro a servicios digitales, la confirmación de identidad y la protección de cuentas frente a accesos no autorizados.

No obstante, PTC advierte que los artículos 6.13.4.1 y 6.13.4.7.2 establecen que todo mensaje A2P, incluidos los mensajes de autenticación, debe contar con una plantilla aprobada y vigente, y que en ausencia de dicha aprobación el PRST podría bloquear el mensaje o marcarlo como «sin verificar». Expone que se genera una contradicción interna en el proyecto: por un lado, se reconoce la naturaleza especial de los mensajes de autenticación y seguridad, pero por otro se los somete al mismo régimen de validación previa, control operativo y eventual bloqueo aplicable a mensajes comerciales o publicitarios.

Sostiene que esta equiparación resulta problemática porque los mensajes de autenticación no son comunicaciones imprevistas, masivas o no deseadas, sino mensajes generados a partir de una acción activa e inmediata del usuario, como iniciar sesión, recuperar una contraseña, confirmar una transacción, validar un dispositivo o autorizar una operación. En esa medida, PTC considera que no deberían recibir el mismo tratamiento regulatorio que las campañas comerciales o publicitarias.

PTC enfatiza que estos mensajes cumplen una función esencial en ecosistemas digitales, financieros, comerciales, gubernamentales y de servicios en línea. Su finalidad no es promover productos o servicios, sino permitir que el usuario acceda de forma segura a plataformas, confirme su identidad o complete procesos iniciados por él mismo. Por ello, imponer controles previos de contenido, vigencias periódicas y validaciones operativas en tiempo real podría afectar la continuidad de servicios que dependen de la entrega inmediata y confiable de estos mensajes.

Desde el punto de vista técnico, resalta que los mensajes OTP, 2FA y demás mensajes de autenticación incorporan variables dinámicas, códigos únicos, datos transaccionales, referencias temporales, nombres de servicios, montos, identificadores parciales o instrucciones específicas que cambian en función de cada operación. Además, expone que son altamente sensibles al tiempo, pues un retraso de pocos segundos puede hacer que el código pierda vigencia, impedir que el usuario complete la operación o generar una experiencia fallida de autenticación.

PTC reconoce que el proyecto no necesariamente exige aprobar la configuración exacta de cada OTP, pero advierte que sí se somete la plantilla, el contenido estático, la lógica o sentido del contenido dinámico y el enrutamiento del mensaje a un esquema de validación previa y consulta operativa, podría generar incertidumbre sobre el alcance de la validación exigida y traducirse en cargas operativas relevantes para originadores, integradores, agregadores y PRST, especialmente cuando los mensajes deben adaptarse a múltiples casos de uso, canales, idiomas, marcas, servicios, niveles de riesgo o necesidades de seguridad.

Asimismo, identifica varios riesgos operativos asociados a aplicar el esquema propuesto a los mensajes de autenticación y seguridad. Entre ellos destaca el riesgo de latencia en la entrega, falsos bloqueos por diferencias menores entre la plantilla y el mensaje dinámico, indisponibilidad por fallas del validador, afectación de procesos esenciales del usuario, degradación de la experiencia, congestión operativa en eventos de alto tráfico, aumento de cargas administrativas y técnicas, afectación a la seguridad del usuario, interrupción de servicios digitales críticos e incertidumbre sobre la responsabilidad entre los distintos actores de la cadena.

Subraya que el costo de un falso bloqueo o retraso en un mensaje de autenticación es significativamente mayor que el de un mensaje comercial no entregado. Mientras la falta de entrega de un mensaje publicitario puede implicar la pérdida de una oportunidad comercial, la no entrega de un mensaje OTP puede impedir el acceso del usuario a su cuenta, bloquear una operación financiera, frustrar la recuperación de una contraseña, afectar la continuidad de un servicio o generar riesgos adicionales de seguridad.

Con base en lo anterior, PTC propone que la regulación reconozca una categoría diferenciada para los mensajes de autenticación y seguridad, con reglas proporcionales a su naturaleza funcional, transaccional y crítica. En particular, sugiere que estos mensajes no estén sujetos al mismo régimen de bloqueo previo aplicable a la mensajería comercial o que, al menos, se contemplen mecanismos especiales para garantizar su continuidad, tales como tratamientos prioritarios, reglas de excepción, validaciones ex post, esquemas de certificación de originadores confiables o controles orientados a patrones de abuso, en lugar de validaciones individuales previas de cada mensaje.

Finalmente, concluye que, en los términos planteados, la medida podría producir un efecto contrario al objetivo del proyecto. En vez de fortalecer la seguridad y prevenir el fraude, podría afectar una de las herramientas más eficaces para proteger a los usuarios frente a accesos indebidos, suplantaciones y operaciones no autorizadas. Por ello, recomienda revisar el tratamiento regulatorio aplicable a los mensajes de autenticación y seguridad, de manera que se preserve su disponibilidad, oportunidad y confiabilidad, sin perjuicio de adoptar medidas razonables y proporcionadas para prevenir su uso indebido.

Respuesta CRC:

La CRC analizó los comentarios presentados frente al tratamiento de los mensajes de autenticación, códigos de verificación de un solo uso —OTP—, segundo factor de autenticación —2FA—, verificación de identidad, alertas de seguridad y comunicaciones transaccionales críticas. En particular, **CCIT** señaló que el proyecto establece obligaciones sobre quienes generan este tipo de mensajes y advirtió que, aunque se reconoce su naturaleza especial, estos quedarían sometidos al mismo esquema de plantillas obligatorias, aprobación previa, validación anual y eventual bloqueo aplicable a otras modalidades de mensajería A2P. En una línea similar, se indica que los mensajes de autenticación y seguridad —incluidos OTP, alertas de inicio de sesión y confirmaciones— se generan a solicitud del usuario y son sensibles al tiempo, por lo que su sometimiento al mismo esquema de validación previa y bloqueo operativo podría generar falsos bloqueos, latencia o indisponibilidad.

De estos comentarios se identifica una tendencia coincidente en solicitar que los OTP y demás mensajes de autenticación, seguridad o comunicaciones críticas cuenten con un tratamiento diferencial frente a otras modalidades de mensajería A2P, especialmente frente a comunicaciones comerciales o publicitarias. Los agentes no cuestionan, en términos generales, la necesidad de identificar al remitente o preservar la trazabilidad del tráfico, sino que advierten que la aplicación indiferenciada de plantillas, validaciones y consecuencias operativas podría afectar la oportunidad y continuidad de mensajes que cumplen una función de seguridad para el usuario.

En el documento soporte, la CRC reconoció que una de las principales aplicaciones del SMS A2P corresponde a procesos de autenticación e identificación digital, incluyendo códigos de verificación —OTP—, mecanismos de autenticación multifactor —MFA— y alertas de seguridad asociadas al acceso o uso de cuentas digitales. También se indicó que estos mensajes son ampliamente utilizados en el sector financiero, las plataformas digitales, redes sociales y el comercio electrónico, donde el SMS funciona como mecanismo adicional de seguridad para validar la identidad del usuario y mitigar riesgos de fraude o accesos no autorizados.

Así mismo, el documento soporte clasificó los mensajes de autenticación y seguridad como aquellos destinados exclusivamente a verificar la identidad del usuario o proteger la seguridad de accesos y operaciones, incluidos los OTP, las alertas inmediatas de seguridad y las confirmaciones de activación o desbloqueo de servicios; y precisó que, por su naturaleza, estos mensajes se generan normalmente a solicitud explícita del usuario o como parte intrínseca de un servicio contratado, por lo que no requieren consentimiento adicional expreso.

Por su parte, el proyecto de resolución establece que los PRST deben integrar sus plataformas de mensajería con el sistema del validador centralizado a través de las APIs disponibles, de modo que puedan consultar, previo al enrutamiento de cada mensaje A2P, la validez del código corto A2P, del SENDER ID y de la plantilla de contenido asociados al mensaje. Igualmente, prevé que cada mensaje A2P debe contar con código corto A2P, SENDER ID en estado asignado e implementado en el SIGRI y una plantilla de contenido aprobada y vigente en el sistema del validador. En consecuencia, el diseño propuesto parte de que los OTP y demás comunicaciones de autenticación o seguridad hacen parte del

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

tráfico A2P y, por tanto, deben ser trazables dentro del sistema de validación, sin perjuicio de las particularidades propias de su modalidad.

Frente a este punto, resulta relevante mencionar que de la revisión de las experiencias internacionales se pudo constatar que no existe evidencia de que las autoridades regulatorias excluyan los mensajes OTP, de autenticación o seguridad de los sistemas de validación de remitentes SMS. En India, la fuente oficial de TRAI[5] indica expresamente que cualquier remitente de comunicaciones masivas —incluidos OTP, transactional messages, service messages o commercial messages— debe cumplir requisitos regulatorios como el registro como Principal Entity, la asignación de header, el registro de Content Template y la transmisión de PE ID, header y Content ID al ofrecer los mensajes para entrega a los proveedores de servicios. Además, las guías operativas[6] sobre el esquema DLT en India muestran que los OTP pueden ser tratados mediante plantillas transaccionales con campos variables, lo que permite validar la estructura del mensaje sin validar el valor específico del código OTP generado para cada usuario.

En Singapur, el SMS Sender ID Registry —SSIR— aplica a todas las organizaciones que pretendan usar Sender IDs alfanuméricos en SMS enviados a usuarios móviles de Singapur, y los Sender IDs no registrados son marcados como «Likely-SCAM». La fuente oficial revisada[7] no establece una exclusión específica para OTP o mensajes de autenticación; el criterio de aplicación es el uso de un Sender ID alfanumérico. IMDA[8] también explicó que el régimen obligatorio de registro y marcación de SMS no registrados forma parte de un enfoque de múltiples capas para fortalecer la protección frente a scams por SMS. Esta experiencia resulta relevante porque evidencia que la marcación de mensajes legítimos como «Likely-SCAM» puede generar confusión en el usuario, incluso en comunicaciones legítimas de autenticación, como se reportó en casos de OTP recibidos con dicha etiqueta durante la implementación inicial del esquema.

En España, la CNMC creó el Registro de Alias para verificar nombres o marcas que aparecen como remitentes en mensajes SMS, MMS o RCS enviados a números españoles, con el objetivo de restaurar la confianza de los usuarios y reforzar la protección frente a estafas de suplantación de identidad. La CNMC[9] señala que los proveedores de mensajería deben bloquear mensajes cuando se usen alias no registrados, cuando provengan de proveedores no registrados o cuando se envíen sin autorización del titular del alias, sin identificar una exclusión específica para OTP o mensajes de autenticación.

[5] https://trai.gov.in/advice-to-senders
[6] Guía de Infobip: https://www.infobip.com/docs/essentials/asia-registration/dlt-templates Guía de Fyno: https://fyno.io/docs/dlt-sms-templates.
[7] https://www.sgnic.sg/smsregistry/overview
[8] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/enhanced-measures-against-scam-sms
[9] https://www.cnmc.es/sectores-que-regulamos/telecomunicaciones/registro-alias

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En Australia, el documento de consulta[10] de ACMA sobre el SMS Sender ID Register define el alcance del registro respecto de mensajes SMS/MMS con sender ID alfanumérico enviados a números móviles australianos. ACMA señala que los sender IDs usados por entidades para enviar SMS/MMS deben registrarse y que, si los mensajes se envían con sender IDs no registrados, estos serían reemplazados por expresiones como «Likely SCAM»; además, precisa que las reglas del registro no requieren evaluar si los mensajes son o no scam, de manera que la disrupción opera por el estado del sender ID, no por una valoración individual del contenido del mensaje. La página oficial[11] de ACMA también indica que las nuevas reglas exigen el registro de los branded sender IDs utilizados para enviar textos con el nombre de una organización. Al igual que en Singapur y España, la fuente revisada no identifica una exclusión específica para OTP; el criterio relevante es el uso del identificador alfanumérico sujeto a registro.

Finalmente, en el Reino Unido, el SMS SenderID Protection Registry administrado por MEF se orienta a reducir el smishing y el spoofing mediante colaboración entre actores de la industria, permitiendo a las organizaciones registrar los headers utilizados para enviar mensajes a sus clientes y facilitando un sistema coordinado de bloqueo frente a intentos de suplantación. La fuente revisada[12] no contiene una regla específica sobre OTP, pero sí confirma que el modelo protege headers o Sender IDs frente a suplantación, especialmente en contextos de marcas, banca y gobierno.

A partir de lo anterior, la CRC encuentra que la experiencia comparada respalda una solución intermedia. Por una parte, no resulta técnicamente aconsejable excluir los OTP, mensajes de autenticación, seguridad o comunicaciones críticas del sistema de validación, pues estos mensajes generan alta confianza en los usuarios y pueden ser utilizados por actores maliciosos para suplantar entidades legítimas, inducir acciones urgentes o conducir a los usuarios hacia enlaces, números o instrucciones fraudulentas.

En particular, ACMA explica que una técnica común de los scammers consiste en usar Sender IDs falsos para imitar marcas o agencias conocidas, logrando que los mensajes fraudulentos aparezcan en el mismo hilo que comunicaciones legítimas, e induciendo al usuario a hacer clic en enlaces o llamar a números incluidos en el cuerpo del mensaje. Por otra parte, la CRC reconoce que los OTP y mensajes de autenticación tienen características operativas particulares: contienen campos dinámicos, son sensibles al tiempo, se originan normalmente por una acción del usuario y se cursan en volúmenes elevados con altos requerimientos de disponibilidad.

En consecuencia, la CRC considera que los OTP y mensajes de autenticación, seguridad y comunicaciones críticas no deben quedar excluidos del sistema de validación, pero sí pueden ser objeto de un tratamiento operacional simplificado, categórico o parametrizado. Esta aproximación permite preservar la trazabilidad del tráfico A2P y, al mismo tiempo, reducir cargas operativas y riesgos de

[10] https://www.acma.gov.au/sites/default/files/2025-03/ACMA%20SMS%20sender%20ID%20register_consultation%20paper.pdf
[11] https://www.acma.gov.au/sms-sender-id-register
[12] https://mobileecosystemforum.com/sms-senderid-protection-registry/

afectación a comunicaciones sensibles al tiempo. La validación debe recaer sobre la modalidad declarada, la estructura general de la plantilla, el SENDER ID asociado, el código corto A2P y los campos dinámicos definidos, pero no sobre el valor específico del OTP generado para cada usuario. Esta conclusión resulta coherente con la experiencia en India, en la cual los OTP están incluidos dentro del sistema de registro y plantillas, pero se gestionan mediante formatos con variables.

La CRC también considera necesario precisar que la ausencia de consentimiento adicional para el envío de OTP no equivale a una exclusión de los controles de trazabilidad. El documento soporte reconoce que los mensajes de autenticación y seguridad se generan normalmente a solicitud explícita del usuario o como parte intrínseca de un servicio contratado, por lo que su envío no requiere consentimiento adicional expreso. Sin embargo, esa característica se refiere al régimen de consentimiento, no a la obligación de identificar al remitente, validar la plantilla o asegurar la trazabilidad del tráfico. Por tanto, los OTP pueden estar exceptuados de una autorización adicional del usuario cuando se generan en el marco de una operación o servicio contratado, pero deben mantenerse dentro del esquema de validación para evitar su uso indebido en modalidades de suplantación o fraude.

Así mismo, cuando los mensajes OTP, de autenticación o seguridad incorporen URL, enlaces, dominios o instrucciones de acción para el usuario, la plantilla deberá declarar expresamente esa característica. Esta precisión es necesaria porque, como se indicó en la revisión del régimen de plantillas, el acceso a URL indebidas constituye uno de los mecanismos mediante los cuales se materializan conductas fraudulentas orientadas al robo de datos personales o credenciales, o la suplantación de identidad. La experiencia australiana también identifica que los mensajes fraudulentos con Sender IDs suplantados suelen inducir al usuario a hacer clic en enlaces o llamar a números incluidos en el cuerpo del mensaje. En consecuencia, permitir que los OTP queden por fuera de la declaración de URL o enlaces podría debilitar la eficacia preventiva del sistema.

Con fundamento en lo anterior, la CRC acepta parcialmente los comentarios relacionados con el manejo de los OTP, mensajes de autenticación, seguridad y comunicaciones críticas, en el sentido de acoger la necesidad de prever un tratamiento simplificado, categórico o parametrizado para estas modalidades, atendiendo su sensibilidad temporal y su función de seguridad. No obstante, la CRC no acepta la exclusión de estos mensajes del sistema de validación, dadas su alta criticidad y la confianza que deben generar en los usuarios. Adicionalmente, si se toma como criterio la experiencia internacional, no se evidencia una regla general de exclusión; por el contrario, se observa que los sistemas de validación de remitentes se aplican en función del uso de un Sender ID, alias, header o una plantilla sujeta a registro, sin exceptuar de manera general los mensajes críticos.

En consecuencia, la modificación en la resolución se introduce en el régimen de plantillas y validación de mensajes A2P, precisando que los mensajes de autenticación, códigos OTP, segundo factor de autenticación, verificación de identidad, alertas de seguridad, confirmaciones de operaciones, comunicaciones transaccionales críticas, regulatorias o de interés público podrán ser registrados mediante plantillas simplificadas, categóricas o parametrizadas, siempre que se garantice la identificación del remitente, la modalidad declarada, la finalidad de la comunicación, la trazabilidad del

tráfico y la declaración de elementos estructurales relevantes, incluida la presencia de URL, enlaces o instrucciones de acción cuando aplique.

De manera particular, estos ajustes se verán reflejados en el régimen de plantillas contenido en la Sección 4 del Capítulo 13 del Título VI de la Resolución CRC 5050 de 2016, específicamente en el artículo 6.13.4.2 (información de las plantillas, en conexión con el numeral 6.13.4.2.7 sobre autenticación) mediante un nuevo parágrafo que habilite el registro simplificado, y, en lo pertinente, en el artículo 6.13.4.3 (procedimiento). La estructuración técnica se coordina en el CTLFSM

En efecto, la CRC considera que la definición concreta del esquema simplificado, categórico o parametrizado aplicable a los mensajes OTP, de autenticación, seguridad y comunicaciones críticas debe ser desarrollada con un enfoque técnico y evolutivo. Para ello, la CRC considera que el CTLFSM deberá analizar, de la mano del validador centralizado y de los agentes que participan en el ecosistema A2P, la mejor forma de estructurar estos esquemas simplificados de plantillas, de manera que se garantice un equilibrio adecuado entre la oportunidad que requieren los mensajes de autenticación y seguridad, y la necesidad de mantener controles efectivos frente al fraude. Este análisis deberá considerar, entre otros aspectos, la definición de categorías de mensajes críticos, los campos dinámicos mínimos exigibles, los criterios para declarar URL o enlaces cuando existan, las condiciones de trazabilidad, los riesgos de uso indebido de plantillas genéricas y los mecanismos técnicos que permitan reducir cargas operativas sin debilitar el sistema de validación.

De esta manera, la CRC no traslada al CTLFSM la definición de nuevas obligaciones regulatorias sustantivas, sino que reconoce que la implementación técnica de las plantillas simplificadas, categóricas o parametrizadas requiere un espacio especializado de coordinación, seguimiento y ajuste operativo. Esta aproximación permite que el régimen conserve su finalidad preventiva, pero cuente con herramientas de adaptación más ágiles frente a la evolución del fraude y frente a las necesidades operativas de mensajes sensibles al tiempo.

Por último, la Comisión se pronuncia sobre las observaciones que, en el capítulo denominado «Comentarios generales», fueron remitidas a la presente temática.

En primer término, la solicitud de **ANDI** y **ASOBANCARIA** de prohibir el almacenamiento de datos sensibles como los códigos OTP u otros factores de autenticación se encuentra atendida en el capítulo denominado «Plantillas (Template ID)», en el cual se precisó que los originadores de contenido deben declarar la información asociada a códigos OTP, referencias transaccionales, identificadores de operación u otros datos personalizados como campos variables dentro de la plantilla, y que la revisión a cargo del validador centralizado corresponde a un control de coherencia entre la estructura de la plantilla, la modalidad declarada y los campos variables, y no a una revisión material del contenido final de cada mensaje ni al acceso a los valores específicos de los campos dinámicos. En consecuencia, el diseño adoptado excluye que el valor del código OTP sea conocido o almacenado por el validador, sin que resulte necesario incorporar una prohibición adicional en el texto de la resolución.

En segundo término, frente a la solicitud de **ASOBANCARIA** relativa a las salvaguardas de continuidad de las comunicaciones críticas, la Comisión reitera que el proyecto no habilita interrupciones automáticas ni indiscriminadas de este tipo de comunicaciones. Las medidas se adoptan en el marco de actuaciones administrativas o de obligaciones expresamente regladas, y se acompañan de mecanismos de continuidad tales como el registro simplificado, categórico o parametrizado de plantillas para mensajes de autenticación y seguridad reconocido en este capítulo, la vigencia de la plantilla original durante el trámite de modificación, y las obligaciones de disponibilidad, resiliencia y continuidad operacional exigibles al validador centralizado, desarrolladas en el capítulo denominado «Validador centralizado: forma de selección, competencias y funciones».

En tercer término, en cuanto a los plazos de la transición, la Comisión precisa que las observaciones sobre su suficiencia fueron analizadas y parcialmente acogidas en el capítulo denominado «Régimen de transición», en el cual se amplió el período de transición del nuevo régimen del ecosistema A2P, decisión que beneficia de manera directa a los agentes que cursan mensajería de autenticación y seguridad y que atiende la preocupación por la continuidad de estas comunicaciones durante la implementación.

En cuarto término, respecto de las garantías de debido proceso frente a las medidas de suspensión, la Comisión reitera que ninguna medida restrictiva sobre recursos de identificación opera de pleno derecho: su adopción exige acto administrativo motivado, dictado dentro de una actuación administrativa en la que se garantizan la contradicción y los recursos procedentes, conforme al artículo 29 de la Constitución Política. El desarrollo puntual de estas garantías frente a las consecuencias aplicables a los agentes reincidentes y frente a las medidas adoptadas por los PRSTM se realiza en los capítulos denominados «Consecuencia para reincidentes» y «Oposición a la interconexión».

Con fundamento en lo expuesto, la CRC no acepta las solicitudes de incorporar disposiciones adicionales sobre almacenamiento de códigos OTP, salvaguardas de continuidad o garantías de debido proceso en el régimen aplicable a los mensajes de autenticación, seguridad y comunicaciones críticas, por encontrarse dichas garantías ya previstas en el ordenamiento y en el diseño regulatorio adoptado, y en consecuencia se mantiene el texto propuesto con los ajustes ya señalados en este capítulo.

2.9 Atribución de responsabilidad

ANDI

Indica que el artículo 6.13.4.4 regula la atribución de responsabilidad por el mal uso de plantillas y que el numeral 6.12.3.2.12 establece como causal de recuperación del SENDER ID el envío de mensajes «potencialmente» atribuibles al mal uso de las plantillas e imputable al asignatario. Sostiene que un estándar basado en lo «potencialmente atribuible» es indeterminado y cercano a la responsabilidad objetiva —con la consecuencia gravísima de la pérdida del recurso y la desactivación de todas las plantillas— y que afecta la tipicidad, la seguridad jurídica y el debido proceso (artículo 29 de la

Constitución), por lo que la responsabilidad debe fundarse en conocimiento efectivo y control real y no en una simple potencialidad.

ASOBANCARIA

Valora el régimen de responsabilidad compartida y recuerda que el fraude no se origina en un único punto de la cadena, por lo que las obligaciones deben distribuirse según el rol, la capacidad de control y el acceso a la información de cada actor; cita como referente el Shared Responsibility Framework de Singapur (MAS e IMDA), que asigna responsabilidades a instituciones financieras, operadores y usuarios según su posición real en la cadena de riesgo.

Solicita reglas claras de atribución basadas en el control efectivo de cada actor y mecanismos de resolución de controversias, y advierte que, dado que en el proceso interviene el integrador tecnológico, existe el riesgo de que conductas no imputables a la entidad financiera terminen afectando su recurso (artículos 6.13.4.4, 6.12.2.2.3 y 6.12.3.2). Por ello pide que el mal uso atribuible al integrador no derive en la recuperación del SENDER ID de la entidad financiera y que se excluya del período de inhabilidad a las modalidades de autenticación y transaccionalidad de las entidades vigiladas —o se reduzca sustancialmente dicho plazo— con notificación inmediata a la entidad sobre el comportamiento de su proveedor.

SAEM

Dice que el artículo 6.13.4.4 atribuye consecuencias regulatorias —incluida la recuperación del recurso— al IT cuando el mal uso le sea «imputable» por haber permitido o facilitado tráfico no autorizado, y prevé recuperación concurrente cuando el mal uso sea imputable a ambos asignatarios.

Sostiene que el IT provee conectividad y trazabilidad, pero no genera ni controla el contenido, que es responsabilidad del PCA asignatario del SENDER ID. Afirma que una atribución amplia o basada en estándares difusos de «facilitación» expone al IT a perder su recurso esencial por conductas de terceros, pese a haber cumplido KYC, integración y reporte.

Informa que el derecho comparado reconoce un régimen de responsabilidad limitada para el intermediario que se limita a transmitir («mere conduit»): el artículo 12 de la Directiva 2000/31/CE de la Unión Europea y, hoy, el artículo 4 del Reglamento de Servicios Digitales (DSA, 2022/2065) eximen de responsabilidad por el contenido transmitido a quien no origina la transmisión, no selecciona al destinatario ni modifica la información, pues es el estándar que debería guiar la atribución al IT.

Propone lo siguiente: (i) Incorporar un puerto seguro expreso: el IT no responderá por el contenido cuando acredite haber cumplido el KYC, la integración con el validador, el bloqueo/suspensión oportuna ante orden o indicio, y el reporte dentro de los plazos; (ii) exigir, para imputar responsabilidad al IT, un estándar de conocimiento efectivo o negligencia grave, no la mera «facilitación»; (iii) graduar la

consecuencia (requerimiento, plan de corrección, suspensión parcial) antes de la recuperación del recurso esencial.

Concretamente, solicita incorporar un puerto seguro (mere conduit) para el IT, condicionando su responsabilidad al conocimiento efectivo o negligencia grave, y graduando las consecuencias antes de la recuperación del recurso esencial.

Respuesta CRC:

Revisadas las intervenciones, la Comisión identifica una tendencia convergente y dos énfasis particulares. La tendencia convergente, común a los tres agentes, cuestiona el estándar de imputación del régimen de atribución de responsabilidad por mal uso de plantillas del artículo 6.13.4.4 y de las causales de recuperación asociadas. En efecto, la **ANDI** y **SAEM** objetan, con fundamentos coincidentes, la indeterminación del estándar correspondiente a la expresión «potencialmente» del numeral 6.12.3.2.12 y la noción de «facilitación» del numeral 6.13.4.4.3, por su cercanía a un régimen de responsabilidad objetiva y su tensión con la tipicidad, la seguridad jurídica y el debido proceso del artículo 29 de la Constitución Política; y **ASOBANCARIA** plantea, desde la perspectiva del asignatario del SENDER ID, el riesgo de que conductas imputables a un tercero de la cadena, en particular el integrador tecnológico, terminen afectando el recurso de identificación de la entidad financiera. Como énfasis particulares, **SAEM** propone incorporar un «puerto seguro» para el integrador y graduar las consecuencias antes de la recuperación del recurso, y **ASOBANCARIA** solicita reglas de atribución basadas en el control efectivo, la exclusión o reducción del período de inhabilidad para las modalidades de autenticación y transaccionalidad de las entidades vigiladas, y la notificación inmediata a la entidad financiera sobre el comportamiento de su proveedor. Seguidamente la Comisión responde de manera integrada la tendencia convergente identificada y, posteriormente, cada solicitud particular.

2.9.1 Sobre el estándar de imputación: la expresión «potencialmente» del numeral 6.12.3.2.12 y la noción de «facilitación» (ANDI y SAEM)

La **ANDI** sostiene que la causal del numeral 6.12.3.2.12, que habilita la recuperación del SENDER ID por el envío de mensajes que «potencialmente pueden ser atribuibles al mal uso de las plantillas», introduce un estándar indeterminado y cercano a la responsabilidad objetiva, con la consecuencia gravísima de la pérdida del recurso y la desactivación de todas las plantillas del asignatario, lo que afecta la tipicidad, la seguridad jurídica y el debido proceso; concluye que la responsabilidad debe fundarse en conocimiento efectivo y control real, y no en una simple potencialidad. **SAEM**, en la misma dirección respecto del asignatario del código corto A2P, afirma que una atribución amplia o basada en estándares difusos de «facilitación» expone al integrador tecnológico a perder su recurso esencial por conductas de terceros, pese a haber cumplido el KYC, la integración y el reporte, y propone exigir, para imputarle responsabilidad, un estándar de conocimiento efectivo o negligencia grave.

En el documento soporte y en el proyecto de resolución, la Comisión diseñó el artículo 6.13.4.4 precisamente como una regla de atribución diferenciada y no objetiva. En efecto, el numeral 6.13.4.4.1

define de manera precisa y cerrada cuándo existe mal uso de una plantilla (divergencia entre el contenido cursado y el aprobado, inclusión de URLs o dominios no declarados, información que induce a error, o envío a usuarios inscritos en el RNE en contravención de la modalidad); y los numerales 6.13.4.4.2, 6.13.4.4.3 y 6.13.4.4.4 distribuyen las consecuencias según a quién sea «directamente imputable» el mal uso, distinguiendo tres escenarios: atribución exclusiva al asignatario del SENDER ID (sin intervención ni conocimiento del asignatario del código corto A2P), atribución exclusiva al asignatario del código corto A2P (por haber permitido o facilitado tráfico no autorizado sin conocimiento del asignatario del SENDER ID), y atribución concurrente. La arquitectura del régimen es, por tanto, subjetiva en la medida en que exige un análisis individual que considere el rol específico de cada agente, apoyado en los registros de auditoría que el validador conserve conforme al numeral 6.13.4.4.5, y se surte en el marco del procedimiento administrativo de recuperación, con plena observancia del derecho de defensa y del debido proceso, como lo reconoce expresamente el numeral 6.13.4.4.4. En este punto vale destacar que los procedimientos de recuperación desarrollados por la CRC en su rol de administrador de los recursos de identificación no corresponden a actuaciones administrativas de carácter sancionatorio en donde se busque acreditar la existencia de responsabilidad administrativa y que deriven en la consecuente imposición de una sanción.

No obstante, la Comisión acepta que la redacción de las causales que remiten a ese régimen puede debilitar, por su literalidad, el estándar de orden individual que el propio artículo 6.13.4.4 consagra, y que ello podría interpretarse como una fuente legítima de potencial inseguridad jurídica. En consecuencia, se aceptan parcialmente los comentarios de **ANDI** y **SAEM**, con el siguiente alcance:

Primero, se acepta la observación sobre la expresión «potencialmente» del numeral 6.12.3.2.12. La Comisión coincide en que un adverbio que sugiere la mera posibilidad del mal uso es incompatible con un régimen de recuperación de recursos que exige certeza sobre la conducta. En consecuencia, se modifica el numeral 6.12.3.2.12 para eliminar la expresión «potencialmente pueden ser atribuibles» y sustituirla por una formulación que exija la atribución efectiva del mal uso al asignatario, de modo que la causal quede redactada en el sentido de que procede la recuperación por el «envío de mensajes de texto (SMS) constitutivos de mal uso de las plantillas, cuando dicho mal uso sea imputable al asignatario del SENDER ID conforme al artículo 6.13.4.4 de la presente resolución». Con este ajuste, la causal se ancla íntegramente en un análisis que tenga en cuenta la condición específica de cada agente de conformidad con el artículo 6.13.4.4 y desaparece el estándar de mera potencialidad objetado.

Segundo, se acepta parcialmente la observación de **SAEM** sobre la noción de «facilitación» del numeral 6.13.4.4.3. La Comisión precisa que dicha expresión no consagra de ninguna manera una especie de régimen de responsabilidad objetiva. El numeral exige que el mal uso sea «directamente imputable» al asignatario del código corto A2P «por haber permitido o facilitado el envío de tráfico no autorizado sin conocimiento del asignatario del SENDER ID», fórmula que ya supone una conducta propia del asignatario y no la simple ocurrencia del mal uso en su infraestructura. No obstante, para eliminar la ambigüedad que el agente señala, se ajusta el numeral 6.13.4.4.3 para precisar que la atribución al asignatario del código corto A2P requiere que este haya permitido o facilitado el tráfico no autorizado con conocimiento de la irregularidad o por inobservancia de los deberes de diligencia a su cargo, de

modo que quede expresamente excluida la atribución de la consecuencia por el solo hecho de que el tráfico haya transitado por su infraestructura. No se acoge, en cambio, la fórmula exacta propuesta por **SAEM** de circunscribir la atribución al «conocimiento efectivo o negligencia grave» porque limitar la imputación al conocimiento efectivo vaciaría de contenido los deberes de diligencia, monitoreo y bloqueo que el propio régimen impone al asignatario del código corto A2P (artículos 6.13.3.1, 6.13.3.2 y 6.13.4.5), permitiendo que la desatención deliberada de esos controles operara como causal de exoneración. El estándar correcto es el del incumplimiento de los deberes de diligencia a cargo del asignatario, que supone el análisis sobre obligaciones de esa naturaleza y que resulta coherente con la posición de garante que cada asignatario asume respecto del recurso escaso que le fue confiado.

La Comisión precisa que la observación sobre la palabra «potencialmente» se replica en el numeral 6.4.3.2.6, relativo a la causal de recuperación del código corto A2P por mensajes atribuibles al mal uso de plantillas, según lo advierte **SAEM** en el capítulo correspondiente, por lo que se hace el respectivo ajuste ya explicado.

2.9.2 Sobre la propuesta de un «puerto seguro» (mere conduit) y la graduación de las consecuencias (SAEM)

SAEM propone incorporar un puerto seguro expreso conforme al cual el integrador tecnológico no responda por el contenido cuando acredite haber cumplido el KYC, la integración con el validador, el bloqueo o la suspensión oportuna ante orden o indicio, y el reporte dentro de los plazos; invoca como referente el régimen de responsabilidad limitada del intermediario que se limita a transmitir, reconocido en el artículo 12 de la Directiva 2000/31/CE de la Unión Europea y en el artículo 4 del Reglamento de Servicios Digitales (Reglamento 2022/2065). Adicionalmente, solicita graduar la consecuencia (requerimiento, plan de corrección, suspensión parcial) antes de la recuperación del recurso esencial.

En cuanto a la incorporación de un puerto seguro, la Comisión considera que la finalidad que persigue el agente (que el asignatario del código corto A2P diligente no responda por conductas de mal uso que no le son atribuibles) ya se encuentra satisfecha por la estructura del artículo 6.13.4.4, tal como quedó precisada en líneas precedentes de este capítulo. En el diseño del régimen, cuando el mal uso es directamente atribuible al asignatario del SENDER ID sin intervención ni conocimiento del asignatario del código corto A2P, las consecuencias recaen exclusivamente sobre el SENDER ID (numeral 6.13.4.4.2), de modo que el integrador diligente no pierde su recurso por el contenido que un tercero originó. La exoneración del asignatario del código corto A2P no depende, pues, de un puerto seguro adicional, sino de la ausencia de atribución conforme a las reglas ya previstas: si dicho asignatario cumplió sus deberes de diligencia y el mal uso obedeció exclusivamente a la conducta del originador, no se configurará respecto de él ninguna causal de recuperación. La Comisión estima, en todo caso, pertinente robustecer la certeza de este entendimiento y, por ello, adiciona al artículo 6.13.4.4 un numeral conforme al cual no habrá lugar a consecuencias regulatorias sobre el código corto A2P cuando su asignatario acredite el cumplimiento oportuno de los deberes de conocimiento del cliente, integración con el validador, monitoreo, suspensión del tráfico ante orden del Administrador de Recursos de Identificación o ante indicios de uso fraudulento, y reporte dentro de los plazos previstos, siempre que

el mal uso no le sea atribuible a título de conducta propia o de inobservancia de tales deberes. Con esta adición se acoge, en lo sustancial, la finalidad de la propuesta de **SAEM**.

En cuanto a la graduación de las consecuencias, la Comisión precisa que el régimen no consagra la recuperación como respuesta automática y única. La recuperación de un recurso de identificación es la consecuencia más gravosa y se reserva a la configuración de una causal precisa, verificada en el procedimiento administrativo de recuperación con plenas garantías; el régimen contempla, además, medidas de menor intensidad y de carácter previo o cautelar, entre ellas la suspensión inmediata del tráfico del SENDER ID por orden del Administrador (numeral 6.13.4.5.4), la desactivación de la plantilla objeto de mal uso (numeral 6.13.4.3.3) y la suspensión de plantillas al inicio del procedimiento (Parágrafo 1 del artículo 6.12.3.2), que operan sin necesidad de recuperar el recurso y que permiten contener el riesgo de manera proporcional. No se acoge, sin embargo, la incorporación de una secuencia rígida y obligatoria de requerimiento, plan de corrección y suspensión parcial como condición previa e ineludible de toda recuperación, por cuanto ello privaría a la autoridad de la posibilidad de actuar con la celeridad que exigen los casos más graves de instrumentalización del recurso para el fraude, en los que la protección inmediata de los usuarios ante el mal uso del recurso no admite la dilación de una escala de correctivos previos. La proporcionalidad se garantiza mediante la valoración que la Comisión efectúa en cada procedimiento, y no mediante el mecanismo propuesto por el agente.

2.9.3 Sobre la protección del recurso de la entidad financiera frente a conductas del integrador y el período de inhabilidad (ASOBANCARIA)

ASOBANCARIA, tras respaldar el enfoque de responsabilidad compartida del proyecto y citar como referente el modelo de responsabilidad distribuida de Singapur, plantea que, dado que en la cadena intervienen terceros, en particular el integrador tecnológico, existe el riesgo de que conductas no atribuibles a la entidad financiera terminen afectando su recurso de identificación y privándola por un plazo prolongado de un canal esencial de comunicación con sus clientes. Solicita, en concreto: (i) que el mal uso atribuible al integrador no pueda derivar en la recuperación, esto es, en la pérdida, del SENDER ID de la entidad financiera; (ii) que se excluyan del período de inhabilidad para la reasignación las modalidades de autenticación y transaccionalidad de las entidades vigiladas o, en su defecto, que se reduzca sustancialmente dicho plazo; y (iii) que se informe de manera inmediata a la entidad financiera sobre el comportamiento de su proveedor.

En cuanto a la solicitud (i), la Comisión coincide con ella porque esa es la lógica del artículo 6.13.4.4 tal como ha sido precisada. Si el mal uso es directamente atribuible al asignatario del código corto A2P (el integrador) sin conocimiento del asignatario del SENDER ID (la entidad financiera), las consecuencias recaen exclusivamente sobre el código corto A2P (numeral 6.13.4.4.3), y no sobre el SENDER ID de la entidad, que resulta indemne. La preocupación de **ASOBANCARIA** queda, por tanto, atendida por la regla de atribución diferenciada, cuya certeza se refuerza con los ajustes introducidos ya explicados en líneas precedentes. La entidad financiera solo puede ver afectado su SENDER ID cuando el mal uso le sea a ella atribuible (numeral 6.13.4.4.2) o cuando exista atribuible concurrente por conducta propia

(numeral 6.13.4.4.4), hipótesis en las cuales la afectación del recurso responde a su propia conducta y no a la de un tercero.

En cuanto a la solicitud (ii), relativa a la exclusión o reducción del período de inhabilidad para la reasignación del recurso respecto de las modalidades de autenticación y transaccionalidad de las entidades vigiladas, la Comisión reitera que la recuperación del SENDER ID de una entidad vigilada solo procede cuando el mal uso le sea atribuible a ella misma, de modo que la hipótesis de una inhabilidad derivada de conductas ajenas no se configura en el diseño del régimen.

En cuanto a la solicitud (iii), sobre la notificación inmediata a la entidad financiera del comportamiento de su proveedor, la Comisión la acepta parcialmente. El régimen ya prevé un flujo de información relevante ya que el numeral 6.13.4.5.3 obliga al asignatario del código corto A2P a notificar al asignatario del SENDER ID, al validador y al Administrador de Recursos de Identificación, dentro de las veinticuatro horas siguientes a su detección, cualquier incidente de uso indebido del tráfico A2P cursado a través de su infraestructura. En consecuencia, la finalidad de mantener informado al asignatario del SENDER ID, lo que incluye a la entidad financiera, sobre las incidencias que puedan afectar su recurso ya se encuentra incorporada. No obstante, para reforzar esta garantía, la Comisión precisa en el artículo 6.13.4.4 que, cuando se inicie un procedimiento de recuperación que pueda afectar un SENDER ID, el Administrador de Recursos de Identificación vinculará y comunicará oportunamente al asignatario del SENDER ID, garantizándole el ejercicio de sus derechos de contradicción y defensa, con lo cual se asegura que la entidad titular del recurso tenga conocimiento y participación en la actuación que pueda afectarlo. No se acoge, en cambio, la creación de una obligación adicional de reporte permanente del «comportamiento» del proveedor por fuera de los incidentes de uso indebido, por cuanto excedería la finalidad del régimen y las relaciones de información que este ordena, sin que ello obste para que las partes lo pacten contractualmente en el marco del numeral 6.13.3.1.6.

2.9.4 Consideración final sobre el enfoque de atribución compartida

La Comisión destaca que las tres intervenciones, pese a sus distintos énfasis, comparten y respaldan el enfoque de atribución diferenciada según el rol, la capacidad de control y el acceso a la información de cada agente de la cadena, que es precisamente el principio que informa el artículo 6.13.4.4 y el conjunto del régimen del ecosistema A2P. Los ajustes acogidos en este capítulo fortalecen ese enfoque, dotándolo de mayor tipicidad y seguridad jurídica sin desnaturalizar la corresponsabilidad que exige la efectividad de las medidas antifraude.

2.10 Tráfico P2P

ASOBANCARIA

Sostiene que el Proyecto incorpora obligaciones de etiquetado, validación y bloqueo que pueden incidir en servicios financieros críticos dependientes de los canales de SMS y voz (alertas transaccionales,

mensajes de seguridad, códigos OTP y confirmaciones de identidad, entre otros). A diferencia de la mensajería comercial, estas comunicaciones forman parte de la arquitectura de prevención del fraude, por lo que su interrupción, demora o clasificación errónea podría comprometer la seguridad de las transacciones, abrir ventanas de exposición o retrasar la reacción frente a operaciones sospechosas.

En ese contexto, **ASOBANCARIA** sugiere, frente al monitoreo y restricción del tráfico P2P, precisar el detalle operativo por el cual se va a tener seguimiento en el monitoreo de tráfico P2P. El numeral 2.1.10.7.2.1.1 exige a los PRST acreditar ante la CRC la detección de al menos seis patrones de uso atípico (volumen inusual, dispersión de destinatarios, homogeneidad del contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red), y en voz se exigen sistemas en tiempo real para robocalls y numeración fraudulenta.

Por lo anterior, **ASOBANCARIA** estima necesario prever procedimientos diferenciados y prioritarios para las comunicaciones de las entidades vigiladas por la SFC (especialmente mensajes transaccionales, alertas de seguridad y autenticación reforzada), de modo que no queden sujetas a restricciones que generen latencia o bloqueos.

ANDESCO

Indica que el artículo 2.1.10.7.2.1.5. señala que los PRST tienen tres meses a partir de la expedición de la resolución para implementar los sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P) orientados a identificar:

• La detección oportuna de patrones de uso atípico que sean indicativos de un posible uso fraudulento del servicio.
• Patrones asociados al uso masivo de planes con SMS ilimitados o con alto saldo para cursar el tráfico de naturaleza A2P simulado como P2P.
• el funcionamiento de granjas de SIM o a la comercialización del saldo de mensajes de texto entre usuarios.
• Volumen inusual de mensajes salientes por usuario.
• Alta dispersión de destinatarios.
• Homogeneidad del contenido.

Dice que, con independencia del plazo, las obligaciones de monitoreo de tráfico P2P y voz deben preservar la flexibilidad técnica de los PRST. La regulación puede definir criterios de referencia, pero no debería imponer una metodología cerrada ni exigir la concurrencia acumulativa de todos los patrones previstos al mismo tiempo para habilitar la actuación del operador. Cada PRST debe poder definir, según la arquitectura de su red, la información disponible y sus capacidades operativas, los criterios más adecuados para identificar riesgos, bastando contar con herramientas tecnológicas razonables y verificables basadas en al menos uno o varios criterios de análisis. Este enfoque conserva el objetivo de prevención del fraude, reduce el riesgo de falsos positivos, evita costos desproporcionados y permite que los operadores innoven en sus metodologías de detección.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Añade que el plazo de tres (3) meses previsto en el artículo mencionado, para la implementación de sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P), resulta insuficiente para garantizar una implementación adecuada, segura y efectiva de las capacidades exigidas por la regulación. Las funcionalidades requeridas por la propuesta regulatoria exceden la simple incorporación de herramientas de monitoreo, pues implican el diseño, desarrollo, adquisición o adaptación de sistemas especializados capaces de identificar patrones complejos de comportamiento asociados a fraude, tales como detección de tráfico A2P simulado como P2P, identificación de granjas de SIM, análisis de volúmenes inusuales de tráfico, dispersión de destinatarios y homogeneidad de contenido.

Dice que estas actividades requieren procesos de análisis, parametrización, integración con plataformas existentes, definición de reglas de negocio, pruebas técnicas y ajustes operativos que difícilmente pueden completarse dentro del plazo propuesto. Adicionalmente, la implementación de estos mecanismos demanda inversiones en infraestructura tecnológica, desarrollo de capacidades analíticas, procesamiento de grandes volúmenes de información y, en algunos casos, la contratación o adquisición de soluciones de terceros. Lo anterior debe estar acompañado de procesos internos de evaluación, contratación, desarrollo, pruebas de aceptación y puesta en producción, los cuales suelen requerir varios meses para su ejecución adecuada.

Afirma que debe considerarse además que la efectividad de los sistemas de detección depende de la construcción y calibración de modelos de comportamiento y umbrales de alerta, actividad que exige recopilar información histórica, analizar patrones de tráfico y validar la precisión de las alertas generadas con el fin de minimizar falsos positivos que puedan afectar usuarios legítimos o generar bloqueos injustificados.

Por otra parte, el proyecto regulatorio, a su juicio, no incorpora evidencia que demuestre que un plazo de tres meses sea técnica y operativamente suficiente para implementar las capacidades exigidas por todos los PRST, ni presenta un análisis de impacto que considere las diferencias existentes entre operadores en cuanto a infraestructura, arquitectura tecnológica y niveles de madurez de sus sistemas antifraude.

En consecuencia, solicita ampliar el plazo de implementación a un mínimo de seis (6) meses contados a partir de la entrada en vigencia de la resolución. Este término permitiría a los PRST desarrollar e implementar soluciones robustas, realizar las pruebas necesarias, capacitar al personal involucrado y garantizar que los mecanismos de monitoreo entren en operación con niveles adecuados de precisión, estabilidad y efectividad, contribuyendo así al cumplimiento de los objetivos perseguidos por la regulación sin comprometer la continuidad y calidad de los servicios. En consecuencia, el reporte del cumplimiento de dicha obligación debería realizarse a los doce (12) meses desde la expedición de la norma.

Insiste en que el artículo 2.1.10.7.2.1.5 otorga tres meses para implementar sistemas de monitoreo y control de tráfico P2P. El período de transición del artículo 19 es de seis meses contados desde la publicación de la resolución de remuneración A2P (Fase II), cuya fecha es incierta.

La implementación de sistemas de monitoreo P2P capaces de detectar los seis patrones descritos en el artículo 2.1.10.7.2.1.1 (volumen inusual, alta dispersión de destinatarios, homogeneidad de contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado, concentración geográfica) requiere: (i) diseño de la arquitectura del sistema; (ii) selección o desarrollo de modelos de machine learning; (iii) integración con los sistemas de gestión de red del PRST; (iv) calibración de umbrales con datos históricos de tráfico; (v) pruebas en entorno no productivo; (vi) ajustes y corrección de falsos positivos; (vii) capacitación del personal. Ese proceso toma entre 6 y 12 meses en operadores con infraestructura tecnológica madura, y potencialmente más en operadores con arquitecturas más antiguas.

Sostiene que el plazo de 3 meses es técnicamente inviable para implementar un sistema robusto; puede ser suficiente para implementar uno rudimentario que genere altas tasas de falsos positivos, afectando usuarios legítimos. La norma no presentó un análisis técnico de viabilidad del plazo de 3 meses. La imposición de plazos técnicamente insuficientes genera el riesgo de que los operadores implementen soluciones superficiales de cumplimiento formal sin efectividad real en la prevención del fraude. Ampliar el plazo de implementación de sistemas de monitoreo P2P a 6 meses desde la publicación en Diario Oficial, con el primer informe de acreditación a los 7 meses y el informe de resultados a los 13 meses.

CLARO

Dice que el protocolo de respuesta escalonado propuesto por la CRC adolece de una grave lentitud operativa que, de aplicarse tal como está redactado, anularía la efectividad de los sistemas antifraude.

Sostiene que, para la primera etapa, titulada «Alerta interna y análisis técnico», se propone que esta tendrá un carácter prioritario y no podrá exceder de dos (2) horas desde la detección del evento.

Adiciona que, respecto de la segunda etapa, titulada «Restricción preventiva inmediata y notificación», se debe permitir la restricción preventiva de la capacidad de envío de mensajes cortos de texto (SMS) de la línea o líneas en caso de que se concluya que existen méritos técnicos que descartan una falsa alarma. De forma simultánea al bloqueo, el PRST notificará al usuario titular sobre la medida preventiva aplicada por motivos de seguridad y sospecha de fraude, indicándole los canales habilitados para realizar una autenticación adicional. Durante esta etapa, la línea mantendrá restringido el envío de SMS, pero no se afectará la recepción de mensajes ni los servicios de voz.

Frente a la tercera etapa: «Autenticación adicional y reactivación», propone que el usuario, dentro de las veinticuatro (24) horas desde la notificación, manifieste la existencia de una causa legítima o complete una autenticación adicional por los canales disponibles. Una vez completada la validación, el PRST levantará la restricción preventiva de forma inmediata. Si vencido el plazo el usuario no se ha autenticado, o la validación resulta insatisfactoria, la restricción de envío de mensajes de texto se

mantendrá con carácter formal por un término de siete (7) días calendario, quedando el PRST habilitado para reportar el caso a la CRC e iniciar las acciones de terminación del contrato por violación a las condiciones de uso del servicio.

Afirma que dejar activa una línea sospechosa durante días, mientras se completan notificaciones y en espera de la autenticación o prueba de vida, viola el principio básico de la ciberseguridad: la mitigación inmediata del riesgo. Permitir que siga operando es una negligencia técnica que desprotege por completo a los usuarios. La restricción técnica debe ser inmediata una vez superado el análisis inicial.

A su juicio, este proceso garantiza la protección del usuario y está alineado con el objetivo del proyecto regulatorio.

COLOMBIA FINTECH

Manifiesta que el artículo 2.1.10.7.2.1.1. establece que los PRST deberán implementar sistemas de monitoreo y control del tráfico P2P, y acreditar ante la CRC que dichos sistemas tienen capacidad de detectar, como mínimo, seis patrones de tráfico atípico: volumen inusual de mensajes salientes, alta dispersión de destinatarios, homogeneidad del contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red.

Si bien la Asociación celebra la incorporación de esta obligación, considera que la norma puede precisarse en dos aspectos relevantes:

1. Ausencia de requisito de evaluación en tiempo real: El artículo no exige que la detección de los patrones descritos opere en tiempo real, sino que parece admitir sistemas de análisis retrospectivo o por lotes (batch). Esto es problemático, dado que el fraude en SMS P2P generalmente se ejecuta en ventanas de tiempo muy cortas (minutos u horas), lo que hace que la detección tardía sea ineficaz. Se sugiere que la CRC precise que los sistemas de monitoreo de tráfico P2P deben operar bajo una arquitectura de procesamiento en tiempo real (real-time o near-real-time), con latencias máximas de detección que la misma CRC podría parametrizar en el marco del CTLFSM. Un estándar razonable de la industria es una latencia de detección inferior a cinco (5) minutos desde el inicio del patrón atípico.

2. Ausencia de requisitos mínimos sobre la arquitectura tecnológica: El artículo deja a libre elección del PRST «las herramientas técnicas, los algoritmos y las metodologías de análisis». Si bien esto respeta el principio de neutralidad tecnológica, introduce el riesgo de que los PRST implementen soluciones insuficientes que cumplan formalmente con la norma sin alcanzar sus objetivos de fondo. Se propone que la CRC, en el marco del CTLFSM, establezca un conjunto mínimo de capacidades funcionales que cualquier solución de monitoreo deba acreditar, independientemente de la tecnología específica escogida. Entre estas capacidades mínimas se sugiere incluir:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

(i) análisis de series de tiempo con ventanas deslizantes de corto plazo;
(ii) detección de anomalías basada en líneas de base dinámicas (no solo umbrales fijos);
(iii) capacidad de correlación multivariada entre los seis patrones listados; y
(iv) generación automática de alertas con asignación de niveles de severidad.

Adicionalmente, manifiesta que el artículo 2.1.10.7.2.1.5. exige que los PRST acrediten la puesta en operación de sus sistemas de monitoreo mediante un informe técnico, y que seis meses después presenten un segundo informe con estadísticas de funcionamiento. Sugiere que la CRC complemente este mecanismo de acreditación con la exigencia de un reporte trimestral, considerando que la dinámica del fraude exige un monitoreo continuo de la efectividad de los sistemas implementados. El reporte debería incluir indicadores de desempeño mínimos, tales como: tasa de detección (verdaderos positivos sobre el total de patrones fraudulentos identificados), tasa de falsos positivos, tiempo promedio de detección y tiempo de respuesta entre la detección y la acción correctiva.

INETUM

Solicita que se aclare el alcance de las medidas de monitoreo y control previstas para el tráfico SMS P2P, particularmente si la detección de patrones asociados a posibles usos fraudulentos —como tráfico A2P simulado como P2P, granjas de SIM o comercialización de saldos de mensajes— implicará el bloqueo de terminales o líneas móviles.

En caso afirmativo, solicita precisar si estas medidas darán lugar a nuevas tipologías de bloqueo, diferentes a las actualmente previstas, así como los criterios, procedimientos y condiciones bajo los cuales se aplicarían dichas restricciones.

JULIO NULDEMAR

Expone que la medida de obligaciones presenta una contradicción técnica, dado que, una vez el PRST bloquea la capacidad de envío de SMS de una línea, el canal de originación queda cerrado y, por tanto, no es posible generar nuevos eventos de detección asociados a dicha línea. En consecuencia, si el levantamiento del bloqueo depende de la detección de nuevos eventos, la restricción finalizaría automáticamente al cumplirse el plazo establecido, reduciendo la efectividad de la medida.

Esto podría generar un incentivo para redes fraudulentas automatizadas, como las SIM-farms, que podrían esperar el vencimiento del bloqueo para reactivar nuevamente el tráfico fraudulento, convirtiendo la medida en una carga operativa sin un efecto preventivo real.

En la segunda etapa, referente a obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P artículo 2.1.10.7.2.1.2.- expone que esta disposición podría vulnerar el Principio de Finalidad del artículo 4 de la Ley 1581 de 2012 (Habeas Data), dado que los datos de contacto obtenidos en una PQR tienen como finalidad específica la notificación de la respuesta a dicha

reclamación, por lo que su uso para control de tráfico, detección de fraude o medidas preventivas requeriría autorización previa, expresa e informada del usuario.

Adicionalmente, al limitar la notificación exclusivamente a este canal, se desconoce la realidad del mercado, considerando que la mayoría de los usuarios no han presentado PQR, generando una imposibilidad material de notificación y pudiendo llevar a la aplicación de restricciones del servicio sin una advertencia efectiva al usuario, afectando las garantías del debido proceso del artículo 29 de la Constitución Política.

Concluye que debe modificarse el artículo 2.1.10.7.2.1.2. de la propuesta a «**CUARTA ETAPA** (...) La restricción tendrá una duración máxima de siete (7) días calendario, al vencimiento de los cuales se levantará temporalmente el bloqueo de envío. La medida se entenderá definitivamente superada si, dentro de los siete (7) días posteriores al levantamiento técnico de la restricción, no se registran nuevos patrones de tráfico atípicos asociados a la línea identificada.»

SCAMZERO

Expone que el artículo 2.1.10.7.2.1. establece que los PRST deben detectar patrones atípicos en SMS P2P -volumen inusual, alta dispersión de destinatarios, homogeneidad de contenido – aplicar un esquema escalonado de cinco etapas que puede tomar hasta varios días hábiles en completarse, pero no protege al usuario en tiempo real frente al mensaje o llamada individual que llegué a su dispositivo.

Propone complementar las medidas de control en la red con herramientas de protección para el usuario final, ya que el monitoreo de SMS P2P y el esquema escalonado de detección no ofrecen una respuesta en tiempo real frente a mensajes o llamadas fraudulentas, y además no cubren canales OTT como WhatsApp o Telegram.

SINCH

Dice que, a medida que se endurecen los controles en el tráfico empresarial (A2P), los estafadores suelen migrar al tráfico de persona a persona (P2P) usando planes de SMS ilimitados. Sostiene que implementar controles aquí es fundamental para no dejar una «puerta trasera» abierta al fraude.

Sostiene que la exigencia a los operadores de monitorear patrones atípicos es acertada, pero deberá aplicarse con cuidado para no vulnerar la privacidad de las comunicaciones. Los operadores deben enfocarse en monitorear metadatos (volumen, frecuencia) y ciertamente, el esquema de respuesta escalonada protege a los usuarios regulares de falsos positivos (bloqueos accidentales por uso legítimo intensivo).

En complemento de lo anterior, señala que la exigencia a los operadores de monitorear conductas «atípicas» en mensajes personales (P2P) camina sobre una línea muy delgada en términos de privacidad de datos. Aunque se aclara que es un análisis de patrones, existe el riesgo de un monitoreo intrusivo o

de la generación de falsos positivos (por ejemplo, bloquear a un usuario legítimo que simplemente está enviando invitaciones masivas para un evento personal).

Añade que el documento menciona el bloqueo temporal y la terminación de contratos para usuarios P2P con conductas atípicas, pero no especifica un mecanismo de defensa o reclamación rápida para el usuario. Si el algoritmo de un operador bloquea por error la línea de una persona, el ciudadano queda incomunicado sin un debido proceso claro para demostrar su inocencia de manera ágil. Dice que se debería establecer un canal de atención prioritario y directo con los operadores para la gestión operativa de quejas y reclamos. Esto permitirá, a su juicio, resolver las controversias de manera ágil en una primera instancia, sin la necesidad de escalar cada incidente directamente ante el regulador (CRC), evitando así la congestión administrativa y demoras innecesarias.

SIC

Sugiere la inclusión del siguiente numeral al proyecto resolución:

«2.1.10.7.13. Los operadores tienen la obligación de usar biometría y consultar las bases de datos de la Registraduría Nacional del Estado Civil cuando usen este factor de autenticación, en las solicitudes o trámites presenciales que requieran la verificación de la identidad del usuario y establecer mecanismos alternativos para ello cuando los trámites se puedan realizar por la línea de atención, la página web u otros canales digitales.»

Expone que la inclusión de esta obligación permitirá:

a. Que la verificación de identidad de los usuarios o titulares se realice por medio de mecanismos confiables, cuando el trámite lo requiera, en armonía con lo establecido en el artículo 2.1.25.1.3 de la Resolución CRC 5050 de 2016

b. Que los PRST tengan certeza de que quien se acerque a realizar un trámite en una oficina física o quien esté realizando la gestión por la línea gratuita, u otro medio de atención o canal digital, sea realmente el usuario o titular y no un tercero. Así como la garantía para los usuarios de que el operador debe hacer uso de herramientas o mecanismos fuertes de autenticación para verificar la identidad complementando con otros medios alternativos, para completar el proceso de autenticación.

Por otro lado, la SIC sugiere el siguiente cambio adicional:

«*ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES. Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude:*

(...)

2.1.10.7.2. Obligaciones particulares:

2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.

(...)

2.1.10.7.2.1.2. (...)

Segunda etapa - Notificación al usuario. (...), notificará al usuario titular de la línea o líneas afectadas, a través del correo electrónico que el usuario haya suministrado, (...)»

En relación con esta modificación, la SIC señala que establecer que esta notificación también se realice por medio del correo electrónico suministrado por el usuario resulta más claro para el usuario y permite una mejor trazabilidad por parte del PRST.

SUMA

Indica que el punto de homogeneidad del contenido no debería formar parte de la lista de capacidades exigidas que deben conformar los sistemas de monitoreo de un PRSTM. Un PRSTM no debe ejercer, de ninguna manera, funciones orientadas a la detección, inspección o evaluación del contenido de mensajes creados por o para los usuarios finales del servicio móvil, de ninguna manera o aproximación.

Sugiere que sean eliminadas todas las referencias a cualquier disposición, obligación o potestad de evaluación de los contenidos de los mensajes cursados tanto en el ámbito A2P como en el P2P, por parte de ningún agente sectorial o administrativo. **SUMA** considera que existiría, innecesariamente, un riesgo cierto de que estas disposiciones contravengan disposiciones legales preexistentes, siendo que ello podría conducir o derivar en invalidez de parte de las normas que se pretenden establecer de buena fe.

De igual forma, considera que el esquema de comportamiento por etapas para la detección y actuación de los PRSTM es adecuado, pero debe establecerse como una recomendación de actuación y buena práctica, no como una lista de obligaciones. Señala que convertirlo en una obligación podría generar riesgos, dado que las situaciones reales no están predeterminadas ni tienen plazos definidos, por lo que su aplicación automática podría generar inconsistencias y efectos no deseados. En este sentido, **SUMA** indica que este esquema debe ser adoptado por los PRSTM como una guía de buenas prácticas, conforme a la experiencia y criterios profesionales del sector.

Respuesta CRC:

La CRC analizó los comentarios presentados frente a las obligaciones particulares en materia de prevención del fraude asociadas al tráfico de mensajes cortos de texto P2P, particularmente aquellas

orientadas a la implementación de sistemas de monitoreo y control que permitan detectar patrones de uso atípico indicativos de posible fraude. El proyecto de resolución previó que los PRST deberán implementar sistemas de monitoreo y control del tráfico P2P orientados a detectar, entre otros, el uso masivo de planes con SMS ilimitados o con alto saldo para cursar tráfico de naturaleza A2P simulado como P2P, el funcionamiento de granjas de SIM y la comercialización del saldo de mensajes de texto entre usuarios. También estableció que cada PRST podrá seleccionar libremente las herramientas técnicas, algoritmos y metodologías que considere más eficientes, siempre que acredite ante la CRC la capacidad de detectar patrones como volumen inusual de mensajes salientes por usuario, alta dispersión de destinatarios, homogeneidad del contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red.

De los comentarios recibidos se identifica una tendencia coincidente en reconocer la importancia de contar con los mecanismos para detectar usos atípicos del tráfico P2P, pero también se evidencian preocupaciones sobre el alcance operativo de la obligación, la flexibilidad técnica de los PRST, la posible afectación de comunicaciones críticas, las medidas preventivas sobre líneas o terminales, los plazos de implementación, el tratamiento de datos personales y la delimitación entre tráfico P2P legítimo y tráfico A2P simulado como P2P.

A continuación, se responden cada una de las subtemáticas identificadas:

2.10.1 Alcance de la obligación de monitoreo y patrones mínimos de detección

ASOBANCARIA solicitó precisar el detalle operativo del seguimiento del tráfico P2P, señalando que el proyecto exige a los PRST acreditar la detección de patrones de uso atípico como volumen inusual, dispersión de destinatarios, homogeneidad del contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red.

ANDESCO indicó que la regulación puede definir criterios de referencia, pero no debería imponer una metodología cerrada ni exigir que todos los patrones se presenten acumulativamente para habilitar la actuación del operador. Según este agente, cada PRST debe poder definir, de acuerdo con la arquitectura de su red, la información disponible y sus capacidades operativas, los criterios más adecuados para identificar riesgos, bastando herramientas tecnológicas razonables y verificables basadas en uno o varios criterios de análisis.

COLOMBIA FINTECH, por su parte, sugirió precisar que la detección debería operar en tiempo real o casi real, debido a que el fraude en SMS P2P puede ejecutarse en ventanas cortas. También propuso que las latencias máximas de detección puedan parametrizarse en el marco del CTLFSM.

Frente a estos comentarios, es preciso mencionar que la CRC no acoge la solicitud de modificar el alcance de la obligación de monitoreo ni los patrones mínimos de detección previstos en el proyecto. La Comisión considera al respecto que la redacción propuesta ya preserva un equilibrio adecuado entre la necesidad de contar con capacidades mínimas verificables y el respeto por la neutralidad tecnológica.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En efecto, el proyecto no impone una herramienta, proveedor, arquitectura o algoritmo específico. Lo que establece es un estándar mínimo de resultado: que los PRST cuenten con sistemas capaces de identificar patrones objetivos de uso atípico asociados a fraude en tráfico P2P, particularmente cuando se utilicen planes o líneas P2P para simular tráfico A2P, operar granjas de SIM o comercializar saldos de mensajes.

En ese sentido, la CRC precisa que los patrones incluidos en el proyecto —volumen inusual, dispersión de destinatarios, homogeneidad de contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red— no constituyen una metodología cerrada ni una lista que deba concurrir simultáneamente en todos los casos para que el operador actúe. Dichos patrones corresponden a señales mínimas que los sistemas de monitoreo deben estar en capacidad de detectar, individual o conjuntamente, según el comportamiento observado, la arquitectura de red, la información disponible y el nivel de riesgo asociado.

Esta aproximación resulta coherente con el documento soporte, en el cual la CRC identificó como problemática específica la falta de control en SMS P2P y los riesgos asociados a planes con SMS ilimitados, particularmente por la posibilidad de que se generen mercados secundarios de saldos, envíos masivos no autorizados, phishing y suplantación de identidad.

Teniendo en cuenta lo anterior, la CRC no considera necesario modificar el alcance de la obligación de monitoreo ni los patrones mínimos de detección, por lo que se mantiene la redacción propuesta en la medida en que define capacidades mínimas de resultado sin imponer una metodología cerrada.

2.10.2 Homogeneidad del contenido como capacidad exigida en los sistemas de monitoreo P2P

SUMA manifestó que un PRSTM no debe ejercer funciones orientadas a la detección, inspección o evaluación del contenido de mensajes creados por o para los usuarios finales del servicio móvil. En ese sentido, solicitó eliminar las referencias a disposiciones, obligaciones o potestades de evaluación de contenidos de mensajes cursados tanto en el ámbito A2P como P2P, al considerar que estas podrían generar riesgos frente a disposiciones legales preexistentes. Adicionalmente, señaló que el esquema de comportamiento por etapas para la detección y actuación de los PRSTM puede ser adecuado como recomendación de actuación o buena práctica, pero no necesariamente como lista de obligaciones rígidas.

En el proyecto publicado para comentarios, la obligación de monitoreo del tráfico P2P exigía que los PRST acreditaran ante la CRC que sus sistemas de monitoreo tenían capacidad para detectar, como mínimo, seis patrones:(i) volumen inusual de mensajes salientes por usuario;(ii) alta dispersión de destinatarios;(iii) homogeneidad del contenido;(iv) periodicidad mecánica;(v) ausencia de tráfico entrante correlacionado; y(vi) concentración geográfica o de red.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Al respecto, la CRC considera pertinente acoger el comentario de **SUMA** en relación con la exclusión de la homogeneidad del contenido como una de las capacidades mínimas exigidas a los sistemas de monitoreo P2P. Si bien este criterio puede ser técnicamente útil para detectar determinados patrones de automatización o envío masivo, su incorporación como capacidad obligatoria podría generar una interpretación según la cual los PRSTM deben inspeccionar, evaluar o analizar el contenido de los mensajes enviados por usuarios finales en el ámbito P2P.

La finalidad de la medida no es habilitar a los PRST para revisar el contenido de comunicaciones interpersonales, sino exigirles la implementación de herramientas de monitoreo orientadas a detectar patrones objetivos de uso atípico del servicio, asociados al uso masivo de planes con SMS ilimitados, al envío de tráfico A2P simulado como P2P, al funcionamiento de granjas de SIM o a la comercialización de saldos de mensajes. Estos objetivos pueden alcanzarse mediante variables de comportamiento y metadatos de tráfico, tales como volumen de mensajes salientes, dispersión de destinatarios, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red, sin necesidad de exigir como capacidad mínima la evaluación de la homogeneidad del contenido.

En ese sentido, la CRC encuentra que retirar la referencia a la homogeneidad del contenido como patrón mínimo exigido permite preservar la finalidad preventiva de la medida, al tiempo que reduce riesgos interpretativos sobre el alcance de las obligaciones de monitoreo de los PRSTM frente al contenido de mensajes P2P. Esta modificación también resulta consistente con el enfoque de neutralidad tecnológica y proporcionalidad que informa la medida, en la medida en que mantiene capacidades de detección basadas en comportamiento observable del tráfico, sin imponer un análisis obligatorio del contenido de las comunicaciones.

Lo anterior no significa que los PRST queden impedidos para utilizar, dentro del marco legal aplicable y cuando cuenten con habilitación suficiente, técnicas adicionales de análisis que resulten legítimas y proporcionales. Sin embargo, desde la perspectiva regulatoria, la CRC considera que no debe exigirse la homogeneidad del contenido como capacidad mínima obligatoria para acreditar el cumplimiento de los sistemas de monitoreo P2P.

En este orden de ideas, la CRC acepta el comentario de **SUMA** y, en consecuencia, se ajusta el artículo 2.1.10.7.2.1.1 de la resolución para eliminar la referencia a la homogeneidad del contenido dentro de la lista de capacidades mínimas que deben acreditar los sistemas de monitoreo y control del tráfico P2P de los PRST.

Esta decisión no modifica la finalidad de la medida ni elimina la obligación de los PRST de implementar sistemas de monitoreo orientados a detectar patrones de uso atípico indicativos de fraude. La obligación se mantiene respecto de variables objetivas de tráfico que permiten identificar comportamientos anómalos sin exigir la inspección o evaluación del contenido de mensajes P2P.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

2.10.3 Flexibilidad técnica frente a requisitos mínimos de arquitectura tecnológica

ANDESCO solicitó preservar la flexibilidad técnica de los PRST para definir, conforme a su red y capacidades, los criterios más adecuados para identificar riesgos, evitando costos desproporcionados y reduciendo falsos positivos.

En sentido complementario, otros comentarios advirtieron que la libertad tecnológica no debería permitir soluciones insuficientes que cumplan formalmente con la norma sin alcanzar sus objetivos de fondo. Por ello, se propuso que la CRC, en el marco del CTLFSM, establezca capacidades funcionales mínimas, tales como análisis de series de tiempo, detección de anomalías con líneas base dinámicas, correlación multivariada entre patrones y generación automática de alertas con niveles de severidad.

Frente a este punto, la CRC comparte que la libertad tecnológica debe mantenerse como principio rector de la medida. Sin embargo, también considera pertinente que esa libertad no se traduzca en soluciones meramente formales, insuficientes o incapaces de alcanzar los objetivos regulatorios de prevención del fraude.

Por ello, sin imponer una arquitectura tecnológica cerrada, la CRC considera adecuado habilitar que, en el marco del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles —CTLFSM—, se puedan analizar parámetros técnicos de referencia, buenas prácticas, capacidades funcionales mínimas e indicadores de desempeño asociados a los sistemas de monitoreo P2P. Este espacio resulta idóneo para revisar la evolución de las metodologías, la calibración de modelos, la oportunidad de detección, la tasa de falsos positivos y la efectividad de las acciones correctivas.

Esta aproximación permite preservar la neutralidad tecnológica, pero a la vez crea un espacio técnico para que la CRC y los agentes del ecosistema evalúen si los sistemas implementados cuentan con capacidades efectivas de detección, alerta, trazabilidad y respuesta.

Teniendo en cuenta lo anterior, la CRC acepta parcialmente los comentarios relacionados con la flexibilidad técnica y los requisitos funcionales mínimos. En consecuencia, se incorpora, en el artículo 2.1.10.7.2.1.4 del proyecto de resolución, una habilitación para que el CTLFSM analice parámetros técnicos de referencia y buenas prácticas, sin imponer una tecnología, proveedor, arquitectura o metodología específica.

2.10.4 Comunicaciones críticas y riesgo de afectación a servicios financieros

ASOBANCARIA manifestó preocupación por la posible afectación de servicios financieros críticos dependientes de SMS y voz, tales como alertas transaccionales, mensajes de seguridad, códigos OTP y confirmaciones de identidad. En el contexto del monitoreo y restricción del tráfico P2P, solicitó prever procedimientos diferenciados y prioritarios para comunicaciones de entidades vigiladas por la

Superintendencia Financiera de Colombia, de modo que no queden sujetas a restricciones que generen latencia o bloqueos.

Frente a este punto, la CRC reconoce la importancia de preservar la continuidad de comunicaciones críticas, especialmente aquellas asociadas a autenticación, seguridad, alertas transaccionales y prevención del fraude. No obstante, no comparte que dichas comunicaciones deban exceptuarse del régimen de monitoreo del tráfico P2P.

La finalidad de la medida P2P es evitar que tráfico empresarial, automatizado, masivo o de naturaleza A2P sea cursado como si se tratara de tráfico interpersonal. En ese sentido, crear excepciones amplias dentro del canal P2P para comunicaciones críticas podría debilitar la medida y abrir una vía de evasión del sistema de identificación y validación previsto para el ecosistema A2P.

En ese sentido, la CRC considera que las comunicaciones críticas legítimas de carácter financiero, transaccional, de autenticación o seguridad deben cursarse mediante el régimen A2P correspondiente, esto es, a través de mecanismos trazables de identificación y validación, y no mediante tráfico P2P masivo o simulado. Esta posición es coherente con el tratamiento previsto en otros apartes del proyecto para mensajes OTP, autenticación, seguridad y comunicaciones transaccionales críticas.

Teniendo en cuenta lo anterior, la CRC no acepta crear excepciones o procedimientos diferenciados para comunicaciones críticas financieras dentro del régimen P2P. Dichas comunicaciones deberán cursarse a través del ecosistema A2P trazable, cuando correspondan a tráfico empresarial, automatizado o masivo.

2.10.5 Restricción preventiva, bloqueo de líneas y alcance de las medidas sobre terminales o usuarios

INETUM solicitó aclarar si la detección de patrones asociados a posibles usos fraudulentos —como tráfico A2P simulado como P2P, granjas de SIM o comercialización de saldos— implicará el bloqueo de terminales o líneas móviles. En caso afirmativo, pidió precisar si estas medidas darían lugar a nuevas tipologías de bloqueo, diferentes a las actualmente previstas, así como los criterios, procedimientos y condiciones bajo los cuales se aplicarían dichas restricciones.

JULIO NULDEMAR advirtió una posible contradicción técnica en la medida, al señalar que, una vez el PRST bloquea la capacidad de envío de SMS de una línea, el canal de originación queda cerrado y no sería posible generar nuevos eventos de detección asociados a dicha línea.

CLARO, por su parte, propuso un protocolo escalonado que incluye alerta interna, análisis técnico, restricción preventiva inmediata, notificación al usuario titular y mecanismos de autenticación adicional.

Frente a estos comentarios, la CRC no acoge la solicitud de incorporar en la resolución nuevas tipologías de bloqueo, procedimientos detallados de restricción o reglas específicas sobre terminales. La medida

propuesta no tiene por objeto crear un régimen autónomo de bloqueo de terminales o líneas móviles, sino establecer obligaciones de monitoreo y control orientadas a detectar patrones atípicos de uso fraudulento del tráfico P2P.

En este sentido, corresponde a cada PRST, dentro de su ámbito de control y de conformidad con la regulación vigente, adoptar medidas técnicas, contractuales y operativas proporcionales frente a usos indebidos del servicio. La CRC considera que resolución no debe detallar todos los escenarios operativos de restricción, pues ello podría generar rigideces y limitar la capacidad de reacción de los operadores frente a modalidades de fraude que evolucionan rápidamente.

Adicionalmente, el proyecto ya parte de obligaciones generales de prevención del fraude, conforme a las cuales los operadores deben hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y realizar controles periódicos sobre la efectividad de dichos mecanismos. También prevé obligaciones frente a PQR relacionadas con presunto fraude.

Frente a la observación de **JULIO NULDEMAR**, según la cual existiría una contradicción técnica en la medida en tanto, una vez restringida la capacidad de envío de SMS de una línea, el canal de originación queda cerrado y no sería posible generar nuevos eventos de detección asociados a dicha línea, la CRC considera necesario precisar el alcance de la medida propuesta.

En primer lugar, la obligación de monitoreo del tráfico P2P no debe entenderse como un mecanismo que dependa exclusivamente de la generación continua de nuevos eventos por parte de la misma línea una vez se ha adoptado una medida preventiva. La detección de patrones de uso atípico se produce con base en el análisis del comportamiento observado en un periodo determinado, a partir de variables tales como volumen inusual de mensajes salientes, dispersión de destinatarios, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red. En consecuencia, la adopción de una medida preventiva no elimina la evidencia técnica que dio lugar a la detección inicial, ni impide que el PRST conserve y analice los registros asociados al comportamiento previamente identificado.

En segundo lugar, la finalidad de la medida no es que una línea continúe generando tráfico sospechoso después de la detección para que el sistema pueda seguir «probando» la existencia del riesgo. Por el contrario, cuando se identifican patrones objetivos que indiquen un posible uso fraudulento del servicio, la finalidad regulatoria es permitir que el PRST adopte medidas proporcionales para contener el riesgo y evitar que el canal siga siendo utilizado para cursar tráfico masivo, automatizado o de naturaleza A2P simulado como P2P. Exigir que la línea continúe originando mensajes para mantener activa la detección desconocería la finalidad preventiva de la obligación y podría permitir que el comportamiento potencialmente fraudulento se prolongue en perjuicio de los usuarios.

En tercer lugar, la restricción preventiva de la capacidad de envío de SMS no implica que el PRST quede impedido para realizar verificaciones posteriores. Estas pueden adelantarse a partir de la información histórica disponible, de los registros técnicos de tráfico, de la trazabilidad de eventos previos, de la

información contractual y de uso del servicio, de eventuales reclamaciones o aclaraciones presentadas por el usuario, y de los demás elementos objetivos que permitan determinar si el comportamiento detectado corresponde efectivamente a un uso indebido del servicio o a una causa legítima. Por tanto, la revisión posterior no depende necesariamente de que la línea continúe generando nuevos eventos de tráfico.

Así mismo, la CRC considera que la observación pone de presente la importancia de diferenciar entre detección, contención y revisión. La detección se produce cuando el sistema identifica patrones atípicos; la contención busca evitar que el tráfico potencialmente fraudulento continúe cursándose; y la revisión permite valorar, con base en evidencia técnica y en la información disponible, si la medida debe mantenerse, levantarse o ajustarse. Bajo esta lógica, no existe contradicción técnica entre restringir temporalmente la capacidad de envío de SMS y conservar la posibilidad de revisar la medida adoptada, pues cada etapa cumple una función distinta dentro del esquema de prevención.

En todo caso, la CRC reitera que las medidas que adopten los PRST frente a patrones atípicos de tráfico P2P deberán observar criterios de proporcionalidad, razonabilidad y correspondencia con el riesgo identificado. La medida no debe entenderse como una obligación de bloqueo automático, indefinido o indiscriminado de líneas o terminales, sino como parte de un esquema de respuesta frente a comportamientos que puedan ser indicativos de uso fraudulento del servicio.

En esa medida, corresponderá al PRST definir, dentro de su ámbito de control y conforme a la regulación vigente, los procedimientos técnicos y operativos que permitan documentar la detección, aplicar medidas de contención cuando resulten necesarias y habilitar mecanismos de revisión o aclaración cuando proceda.

Por lo anterior, la CRC no comparte la afirmación según la cual la medida presenta una contradicción técnica que impida su aplicación. La restricción preventiva de la capacidad de envío de SMS no tiene como propósito generar nuevos eventos de detección, sino contener un riesgo previamente identificado. La evaluación posterior de la medida puede realizarse con base en la información técnica disponible, los registros históricos y los elementos objetivos asociados al comportamiento detectado. En consecuencia, no resulta necesario modificar la resolución para crear una regla específica sobre este punto, sin perjuicio de que los PRST deban implementar sus sistemas de monitoreo y respuesta de manera proporcional, documentada y técnicamente verificable.

Teniendo en cuenta lo anterior, la CRC no acepta incorporar nuevas tipologías de bloqueo o procedimientos específicos sobre terminales o líneas. La medida propuesta no crea un régimen autónomo de bloqueo de terminales, sino que establece obligaciones de monitoreo y control orientadas a detectar patrones atípicos de uso fraudulento del tráfico P2P.

En particular, frente a la observación de **JULIO NULDEMAR**, la CRC precisa que la restricción preventiva de la capacidad de envío de SMS no genera una contradicción técnica, pues su finalidad es contener un riesgo previamente identificado y no permitir la generación indefinida de nuevos eventos.

La revisión posterior de la medida puede adelantarse con base en información histórica, registros técnicos, trazabilidad de eventos, aclaraciones del usuario y demás elementos objetivos disponibles. Por tanto, se mantiene la redacción propuesta, bajo el entendimiento de que las medidas aplicadas por los PRST deberán observar criterios de proporcionalidad, razonabilidad y verificabilidad técnica.

2.10.6 Plazo de implementación, acreditación e informes de seguimiento

ANDESCO señaló que el proyecto prevé un plazo de tres meses para implementar los sistemas de monitoreo y control del tráfico P2P.

CLARO consideró que dicho término resulta insuficiente para garantizar una implementación adecuada, segura y efectiva, dado que las funcionalidades requeridas exceden la simple incorporación de herramientas de monitoreo e implican diseño, desarrollo, adquisición o adaptación de sistemas especializados, análisis, parametrización, integración con plataformas existentes, definición de reglas de negocio, pruebas técnicas y ajustes operativos.

ANDESCO también propuso ampliar el plazo de implementación de los sistemas de monitoreo P2P a seis meses contados desde la publicación en el Diario Oficial, con la presentación del primer informe de acreditación a los siete meses y del informe de resultados a los trece meses.

COLOMBIA FINTECH sugirió complementar el mecanismo de acreditación con reportes trimestrales e indicadores de desempeño como tasa de detección, tasa de falsos positivos, tiempo promedio de detección y tiempo de respuesta.

Al respecto, la CRC reconoce que la implementación de sistemas robustos de monitoreo P2P puede requerir procesos de diseño, desarrollo, adquisición o adaptación de herramientas especializadas, integración con plataformas existentes, parametrización, definición de reglas de negocio, pruebas técnicas, calibración de modelos y ajustes operativos.

En consecuencia, la CRC considera procedente revisar los plazos de implementación y las obligaciones de acreditación en el marco del régimen de transición, con el fin de garantizar que la entrada en operación de los sistemas sea técnicamente viable, estable y efectiva.

Teniendo en cuenta lo anterior, la CRC acepta parcialmente los comentarios relacionados con el plazo de implementación, acreditación e informes de seguimiento. La respuesta detallada sobre este punto se desarrollará en el numeral 6.1 del documento de respuestas, relativo al régimen de transición.

2.10.7 Protección de datos, finalidad y uso de información de contacto en notificaciones

JULIO NULDEMAR sostuvo que una disposición relacionada con obligaciones particulares en prevención del fraude en tráfico P2P podría vulnerar el principio de finalidad previsto en la Ley 1581 de

2012, al considerar que los datos de contacto obtenidos en una PQR tienen como finalidad específica la notificación de la respuesta a dicha reclamación, por lo que su uso para control de tráfico, detección de fraude o medidas preventivas requeriría autorización previa, expresa e informada del usuario.

Frente a este punto, la CRC no acoge la solicitud de incorporar una regla específica adicional sobre protección de datos, finalidad o uso de información de contacto en el marco de las medidas de monitoreo P2P. La prevención del fraude, la seguridad del servicio, la gestión de usos indebidos de la red y la atención de reclamaciones hacen parte de las obligaciones propias de los operadores frente a sus usuarios. En todo caso, cualquier tratamiento de datos personales que realicen los PRST en desarrollo de estas medidas deberá sujetarse al régimen general aplicable en materia de protección de datos personales, incluyendo los principios de finalidad, necesidad, seguridad, circulación restringida y confidencialidad.

La regulación sectorial propuesta no exonera a los operadores del cumplimiento del régimen general de habeas data y protección de datos personales. Por tanto, no resulta necesario reproducir dichas obligaciones en esta resolución ni crear una regla especial adicional para este punto. En este orden de ideas, la CRC no acepta incorporar una disposición adicional específica sobre protección de datos o finalidad en este numeral, sin perjuicio de la plena aplicación del régimen general de protección de datos personales.

2.10.8 Autenticación biométrica y notificación por correo electrónico

La CRC analizó los comentarios de la SIC relacionados con la posibilidad de incorporar medidas adicionales orientadas a fortalecer la autenticación de los usuarios y los mecanismos de notificación en el marco de las medidas de prevención del fraude. En particular, se hizo referencia a la eventual inclusión de mecanismos de autenticación biométrica para trámites ante los operadores, así como a la posibilidad de establecer una obligación de notificación por correo electrónico a los usuarios en determinados eventos asociados a la aplicación de medidas preventivas.

Al respecto, la Comisión reconoce que tanto la autenticación biométrica como la notificación por correo electrónico pueden guardar una relación general con la seguridad de los usuarios, la prevención de usos indebidos de los servicios y el fortalecimiento de los canales de interacción entre usuarios y operadores. En efecto, los mecanismos de validación de identidad pueden contribuir a verificar que quien adelanta un trámite corresponde al titular o usuario legitimado, mientras que los mecanismos de notificación pueden facilitar la trazabilidad y oportunidad de la información que se entrega al usuario.

No obstante, la CRC considera que estas medidas, si bien están relacionadas de manera general con la seguridad, no se relacionan de manera específica con las situaciones problemáticas que busca atender el presente proyecto regulatorio. El objeto de esta iniciativa se concentra en la identificación, prevención y mitigación de modalidades de fraude cibernético que se materializan mediante servicios móviles tradicionales, particularmente a través del contacto a usuarios por SMS y voz, el uso indebido de recursos de identificación, la suplantación del remitente, el tráfico A2P no trazable, el uso fraudulento

del tráfico P2P y la presentación irregular de identificadores de línea llamante. En contraste, las medidas de autenticación biométrica y de notificación por correo electrónico se refieren principalmente a condiciones de validación de identidad y comunicación con el usuario en el desarrollo de trámites o actuaciones ante los operadores, materia que tiene un alcance regulatorio distinto al abordado en este proyecto.

En esa medida, incorporar en esta resolución una obligación general de autenticación biométrica o una obligación general de notificación por correo electrónico excedería el alcance material del presente proyecto. Ambas medidas podrían implicar impactos técnicos, operativos, jurídicos y económicos específicos, asociados, entre otros aspectos, a la adecuación de procesos de atención, contratación o gestión de servicios; actualización y validación de datos de contacto; tratamiento de datos personales, incluidos eventualmente datos sensibles; definición de condiciones de interoperabilidad; seguridad de la información; experiencia del usuario; y costos de implementación y operación.

Por lo anterior, la CRC no considera procedente incorporar en el presente proyecto una obligación específica de autenticación biométrica ni una obligación general de notificación por correo electrónico a los usuarios. Lo anterior no desconoce la relevancia de estas materias, sino que reconoce que su evaluación exige un análisis regulatorio propio sobre necesidad, idoneidad, proporcionalidad, costos, beneficios, riesgos en materia de protección de datos personales y efectos operativos para los agentes obligados.

Sin perjuicio de lo anterior, la CRC precisa que en el marco del proyecto de Revisión de temáticas específicas del Régimen de Protección de Usuarios —RPU Fase 2— se analizan, entre otros aspectos, las disposiciones relacionadas con la validación de identidad para el desarrollo de trámites ante los operadores. En consecuencia, las sugerencias relacionadas con autenticación biométrica y mecanismos de notificación al usuario, incluido el uso del correo electrónico, serán consideradas en dicho escenario regulatorio, por ser el espacio más adecuado para evaluar integralmente las condiciones, garantías, mecanismos y eventuales obligaciones asociadas a la autenticación y comunicación con los usuarios en trámites ante los proveedores de servicios de comunicaciones.

En consecuencia, la CRC no acoge la incorporación de estas obligaciones en el presente proyecto, por exceder su alcance material específico. No obstante, las sugerencias serán tenidas en cuenta en el proyecto de Revisión de temáticas específicas del RPU Fase 2, en el cual se revisan las disposiciones aplicables a la validación de identidad y a las condiciones de interacción entre usuarios y operadores.

SCAMZERO señaló que el esquema escalonado de detección y actuación previsto para el tráfico P2P puede tomar varios días hábiles en completarse y que, por esa razón, no ofrece una respuesta en tiempo real frente al mensaje o la llamada individual que llega al dispositivo del usuario. Sobre esa base, propuso complementar las medidas de control en la red con herramientas de protección dirigidas al usuario final, y advirtió que las medidas no cubren canales OTT como los servicios de mensajería instantánea.

Por su parte, **SINCH** respaldó la exigencia de monitorear patrones atípicos en el tráfico P2P, pero solicitó que su aplicación se limite a metadatos —volumen y frecuencia— para no comprometer la privacidad de las comunicaciones, y advirtió que el proyecto no especifica un mecanismo de defensa o reclamación ágil frente a bloqueos erróneos, por lo que propuso establecer un canal de atención prioritario y directo con los operadores para la gestión de quejas y reclamos, que permita resolver las controversias en una primera instancia sin escalar cada incidente ante la CRC.

La tendencia de estos comentarios es complementaria y propositiva: ninguno cuestiona la obligación de monitoreo, sino que solicitan medidas adicionales de protección del usuario y de gestión de reclamaciones.

Frente a la observación sobre la ausencia de respuesta en tiempo real, la Comisión precisa que el esquema escalonado de detección y actuación no agota el conjunto de medidas adoptadas. La decisión incorpora mecanismos que operan directamente frente al usuario y de manera inmediata, tales como el etiquetado de las llamadas que derivan en la alerta de llamada sospechosa, el bloqueo de las llamadas internacionales entrantes que presenten como identificador de línea llamante un número perteneciente al Plan Nacional de Numeración colombiano, y el etiquetado de las llamadas con fines publicitarios, así como las medidas orientadas a la educación de la ciudadanía. En ese contexto, el esquema escalonado cumple una función distinta y complementaria: identificar y contener el uso indebido del canal P2P en cabeza de quien lo origina, no sustituir las medidas de protección inmediata. Por lo anterior, la CRC no acoge la solicitud de incorporar obligaciones adicionales de provisión de herramientas de protección en el terminal del usuario, sin perjuicio de que la evolución de este tipo de soluciones sea objeto de análisis en el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles —CTLFSM—.

En cuanto a la cobertura de los canales OTT, la Comisión reitera lo expuesto en el capítulo denominado «Comentarios generales», en el sentido de que el ámbito material de este proyecto se circunscribe a los servicios móviles de mensajería corta de texto y de voz, y que la extensión de obligaciones antifraude hacia servicios prestados sobre la capa de aplicación excede el alcance de la presente actuación y demanda una articulación interinstitucional que la CRC ha reconocido como pertinente. En consecuencia, no se acepta la solicitud de ampliar el ámbito de aplicación a dichos canales.

Respecto de la preocupación de **SINCH** sobre la privacidad de las comunicaciones, la Comisión se remite a lo expuesto en el aparte relativo a la protección de datos, finalidad y uso de información de contacto, y precisa que el monitoreo exigido recae sobre patrones de comportamiento del tráfico y no sobre el contenido de las comunicaciones, garantía que se refuerza con la eliminación de la homogeneidad del contenido como capacidad exigible a los sistemas de monitoreo, acogida en este mismo capítulo.

Finalmente, en relación con la solicitud de establecer un canal de atención prioritario y directo para la gestión de quejas y reclamos derivados de las medidas preventivas, la CRC no la acoge. El régimen de protección de los derechos de los usuarios de servicios de comunicaciones contenido en la Resolución CRC 5050 de 2016 ya impone a los proveedores el deber de disponer de medios de atención al usuario

y regula el trámite de las peticiones, quejas y recursos, incluida la procedencia del recurso de reposición y, en subsidio, de apelación ante la Superintendencia de Industria y Comercio. Establecer un canal paralelo y específico para esta materia generaría duplicidad frente a un régimen ya existente y de aplicación general.

Con fundamento en lo anterior, la CRC no acepta las solicitudes analizadas en el presente aparte y, en consecuencia, se mantienen las obligaciones de monitoreo y control del tráfico P2P en los términos propuestos, con los ajustes expresamente señalados en los apartes precedentes de este capítulo.

2.11 Reportes de información

CLARO

Frente al reporte sobre SMS A2P, en el que se exige incluir los umbrales y criterios aplicados por el PRST para detectar cada patrón, así como las actualizaciones realizadas durante el período reportado, **CLARO** propone eliminar este requisito.

El operador considera que esta exigencia representa un riesgo crítico para la seguridad del ecosistema de telecomunicaciones y desconoce la confidencialidad comercial. Señala que los criterios, fórmulas lógicas y umbrales de configuración desarrollados por los equipos de ingeniería de los PRST (o adquiridos mediante licencias de proveedores especializados) constituyen información clasificada como Secreto Empresarial cuya divulgación podría comprometer la efectividad de los sistemas de detección.

Añade que esta información se encuentra protegida por la Decisión 486 de la Comunidad Andina de Naciones, que ampara la información no divulgada con valor comercial y sujeta a medidas razonables de protección. Asimismo, sostiene que las herramientas de detección de fraude constituyen un factor de diferenciación competitiva, por lo que no resulta razonable obligar a un operador que ha realizado inversiones significativas en algoritmos avanzados e Inteligencia Artificial a revelar sus metodologías en documentos regulatorios que podrían terminar expuestos a la competencia.

Respecto del reporte de eventos descartados como falsos positivos en la primera etapa del esquema de respuesta, junto con los factores de contexto que motivaron dicha decisión, **CLARO** solicita eliminar esta obligación por considerarla técnicamente inviable.

Explica que las redes móviles procesan millones de eventos de SMS diariamente y que los Firewall de SMS y los sistemas de gestión de fraude operan mediante reglas automatizadas de descarte inmediato y que almacenar en registros cada evento analizado que NO coincida con un patrón de fraude generaría volúmenes de información de varios Terabytes diarios, incrementaría los costos de almacenamiento y podría degradar el rendimiento de los sistemas de procesamiento.

Finalmente señala que, en procesos automatizados, la razón para descartar un evento consiste generalmente en que el algoritmo no alcanzó el puntaje o score requerido para activar una alerta, por

lo que considera imposible exigir factores contextuales o cualitativos para millones de descartes procesados de manera automática.

Respuesta CRC:

La CRC analizó el comentario presentado por **CLARO** frente a los reportes de información asociados a las medidas de monitoreo del tráfico SMS, específicamente respecto de dos obligaciones previstas en el proyecto: i) reportar los umbrales y criterios aplicados por el PRST para la detección de patrones de tráfico, junto con sus actualizaciones; y ii) reportar información sobre eventos de detección de tráfico P2P atípico, falsos positivos y factores de contexto que motivaron su descarte.

De manera general, **CLARO** solicita eliminar estos requisitos. En relación con el primer grupo de información, sostiene que los umbrales, fórmulas lógicas, criterios de configuración y metodologías de detección pueden constituir secreto empresarial, información sensible de ciberseguridad y factores de diferenciación competitiva. En relación con el segundo grupo, afirma que exigir el registro o reporte de eventos descartados o falsos positivos resulta técnicamente inviable, dado el volumen de eventos procesados por las redes móviles y la forma automatizada en que operan los sistemas de Firewall SMS o Fraud Management System —FMS—.

A continuación, se procede a resolver el comentario:

2.11.1 Reporte de umbrales, criterios y actualizaciones de los sistemas de detección

CLARO solicita eliminar el requisito consistente en reportar los umbrales y criterios aplicados por el PRST para la detección de cada patrón, así como las actualizaciones realizadas durante el periodo reportado. A su juicio, esta información corresponde a criterios, fórmulas lógicas y configuraciones desarrolladas internamente o adquiridas a proveedores especializados, por lo que podría constituir secreto empresarial o información sensible cuya divulgación comprometería la seguridad del ecosistema y la posición competitiva de los operadores.

En el documento soporte, la CRC planteó la necesidad de contar con métricas e indicadores para evaluar la reducción del fraude y el impacto de las alternativas regulatorias. En particular, se formuló la pregunta sobre «qué métricas, indicadores o criterios» deberían establecerse en la industria para evaluar la reducción del fraude y «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»; allí se recogió, entre otros, que **ASOBANCARIA** propuso considerar el volumen de contactos y reportes asociados a smishing y vishing, y que **CLARO** propuso evaluar el número de casos escalados a PCA, el número de recursos de numeración recuperados por uso indebido y el tiempo promedio de respuesta ante incidentes por parte de la CRC.

De igual manera, el documento soporte señaló que, para la revisión y actualización periódica de parámetros de detección de comportamientos atípicos, la CRC promovería un espacio periódico o recurrente de coordinación con el fin de «facilitar el intercambio de información relevante sobre fraude», «definir lineamientos técnicos y buenas prácticas», «realizar seguimiento a la evolución del fenómeno», «apoyar la formulación y ajuste de medidas regulatorias» y «documentar los acuerdos desarrollados para su seguimiento efectivo».

Por su parte, el proyecto de resolución estableció que los PRST deben participar en el CTLFSM y que, en dicho comité, los participantes podrán proponer y acordar mejoras a los parámetros mínimos de detección cuando la evolución de las modalidades de fraude así lo requiera. Además, el proyecto previó que la acreditación de los sistemas de monitoreo se realizaría mediante un informe técnico que describa «la arquitectura del sistema implementado, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas». Finalmente, el proyecto incluyó expresamente el reporte de «los umbrales y criterios aplicados por el PRST para la detección de cada uno de los patrones, con indicación de las actualizaciones realizadas a dichos criterios durante el período reportado».

Al respecto, la CRC reconoce que los umbrales exactos, reglas internas, fórmulas lógicas, pesos de modelos, criterios de scoring, parametrizaciones propietarias, arquitectura detallada de seguridad o código fuente de los sistemas antifraude pueden constituir información sensible desde el punto de vista de seguridad de la red, secreto empresarial, propiedad intelectual y estrategia competitiva. Su divulgación detallada podría afectar la eficacia de los sistemas de detección, al permitir que actores maliciosos conozcan o infieran las condiciones bajo las cuales un comportamiento activa alertas o restricciones.

Así mismo, la CRC entiende que las capacidades de seguridad, la sofisticación de los sistemas de detección, la oportunidad de respuesta frente a incidentes y la inversión en herramientas de ciberseguridad pueden constituir elementos de diferenciación competitiva entre redes y operadores. En efecto, en mercados donde los usuarios valoran la confianza, la seguridad y la continuidad del servicio, la capacidad de un PRST para prevenir, detectar y mitigar eventos de fraude puede convertirse en un atributo relevante de calidad y reputación.

No obstante, esta consideración no elimina la necesidad de reconocer que la prevención y mitigación del fraude en servicios móviles tiene una dimensión colectiva y sistémica. Las modalidades de fraude que se materializan mediante voz y SMS no afectan únicamente a un operador, ni se agotan dentro de una sola red. Por el contrario, comprometen la confianza general de los usuarios en los servicios de telecomunicaciones, afectan la percepción de seguridad de los canales tradicionales de comunicación y pueden erosionar la competencia misma en dichos servicios, en la medida en que los usuarios migran, reducen su uso o desconfían de canales legítimos por temor a ser víctimas de fraude.

En ese sentido, la colaboración sectorial en el control del fraude no es incompatible con la protección del secreto empresarial ni con la competencia entre operadores. Por el contrario, constituye un elemento determinante para preservar la confianza en el ecosistema y asegurar que la competencia se desarrolle

sobre la base de redes y servicios confiables. El propósito de las medidas regulatorias no es homogenizar las soluciones tecnológicas de los PRST ni obligarlos a revelar la lógica propietaria de sus sistemas, sino asegurar que exista un nivel mínimo de coordinación, trazabilidad, información agregada y seguimiento que permita proteger a los usuarios, reducir el uso fraudulento de los servicios y recuperar la confianza en los canales de voz y SMS.

Por tanto, la CRC considera procedente distinguir entre información sensible no exigible en detalle e información agregada, descriptiva o funcional que sí resulta necesaria para el seguimiento regulatorio y la coordinación sectorial. Esta última puede incluir la identificación de las categorías de patrones monitoreados, los tipos generales de señales consideradas, la existencia de actualizaciones metodológicas durante el periodo reportado, la fecha o periodo en que se realizaron dichas actualizaciones y resultados agregados de operación, sin revelar umbrales exactos, código fuente, lógica propietaria, fórmulas internas o elementos que permitan replicar o evadir los sistemas de detección.

Así las cosas, la CRC acepta parcialmente el comentario de **CLARO**. En consecuencia, se ajusta la resolución, concretamente se modifica el literal (f) del numeral 2.1.10.7.2.1.5 del proyecto publicado, que corresponde al literal (e) en la versión final de la resolución como consecuencia de la supresión del literal (b), para eliminar la obligación de reportar umbrales exactos, fórmulas lógicas, criterios específicos de scoring, reglas internas de configuración, parametrizaciones propietarias, código fuente o arquitectura detallada de seguridad. No obstante, se mantendrá la obligación de remitir información agregada, descriptiva o funcional que permita verificar la existencia, actualización y efectividad general de las capacidades de detección implementadas por los PRST, así como alimentar los espacios de coordinación sectorial orientados a la protección de los usuarios y a la recuperación de la confianza en los canales de voz y SMS.

2.11.2 Reporte de eventos detectados, falsos positivos y factores de contexto

CLARO solicita eliminar los aspectos del reporte asociados al número de eventos de detección de patrones de tráfico P2P atípico, el número de casos descartados como falsos positivos y los factores de contexto que motivaron dicha determinación. Sostiene que las redes móviles procesan millones de eventos SMS diariamente y que los sistemas antifraude funcionan mediante reglas de descarte perimetral inmediato, por lo que almacenar logs de todos los eventos analizados o descartados generaría altos volúmenes de información, costos de almacenamiento y posibles afectaciones al rendimiento de la red. Además, indica que en procesos automatizados la motivación del descarte puede consistir simplemente en que el algoritmo no alcanzó el score necesario para activar la alerta.

Al respecto, el documento soporte planteó la necesidad de identificar métricas, indicadores y variables para medir la evolución del fraude, la protección al usuario y la eficacia de las medidas implementadas. En ese contexto, se recogieron propuestas de indicadores como volumen de contactos y reportes asociados a smishing y vishing, número de casos escalados a PCA, número de recursos recuperados por uso indebido y tiempo promedio de respuesta ante incidentes.

En la misma línea, el proyecto de resolución previó que, dentro de los seis meses siguientes a la presentación del primer informe de acreditación, los PRST remitan un segundo informe a la CRC. Entre los contenidos de ese informe se incluyó «el número de eventos de detección de patrones de tráfico P2P atípico registrados en el período transcurrido desde la implementación de las medidas, discriminado por tipo de patrón detectado» y «el número de casos en que el sistema descartó el evento como falso positivo en la primera etapa del esquema de respuesta, con indicación de los factores de contexto que motivaron esa determinación». También se incluyó la obligación de reportar el número de casos en que el usuario manifestó una causa legítima, el número de restricciones temporales aplicadas, los casos reportados a la CRC, las terminaciones contractuales y las PQR recibidas en relación con la aplicación de la medida.

Teniendo en cuenta lo anterior, la CRC comparte parcialmente la interpretación de **CLARO**. Exigir el almacenamiento y reporte individualizado de cada evento procesado o descartado por los sistemas antifraude podría resultar desproporcionado, especialmente si se trata de eventos que no generaron alerta o que fueron descartados automáticamente por no cumplir los criterios mínimos de activación. Una obligación de esa naturaleza podría generar cargas técnicas y costos de almacenamiento que no son necesarios para cumplir la finalidad regulatoria.

Asimismo, exigir factores de contexto cualitativos para cada descarte automatizado puede no ser compatible con la forma en que operan muchos sistemas de detección. En tales sistemas, la decisión puede depender de reglas, puntuaciones o correlaciones internas que determinan si un evento activa o no una alerta. Por tanto, la CRC no considera necesario exigir explicaciones individualizadas para cada descarte, razón por la cual se elimina el contenido del literal (b) del numeral 2.1.10.7.2.1.5 en ese sentido.

Sin embargo, sí resulta indispensable que la CRC reciba información agregada que permita evaluar la operación general de los sistemas. El seguimiento regulatorio requiere conocer los eventos que efectivamente generaron detecciones o alertas, los patrones identificados, las acciones adoptadas, los casos en que el usuario manifestó causa legítima, las restricciones aplicadas, los casos escalados y las PQR recibidas. También puede resultar útil conocer indicadores agregados de falsos positivos o descartes, cuando estos sean técnicamente disponibles, sin exigir que el PRST almacene exhaustivamente todos los eventos que no generaron alerta.

Esta información agregada no busca revelar la lógica propietaria de los sistemas ni afectar la diferenciación competitiva de los operadores. Por el contrario, busca permitir que la CRC y los espacios de coordinación sectorial cuenten con evidencia suficiente para identificar tendencias, detectar posibles fallas de calibración, evaluar la efectividad de las medidas y promover ajustes que beneficien al conjunto del ecosistema. En materia de fraude, la ausencia de información agregada y comparable puede impedir la identificación de patrones comunes, limitar la reacción coordinada del sector y mantener desprotegidos a los usuarios frente a modalidades que se desplazan entre redes, servicios y agentes.

La CRC considera que la competencia en los servicios de telecomunicaciones no se fortalece únicamente preservando la reserva de los desarrollos tecnológicos de cada operador, sino también asegurando que los usuarios confíen en que los canales de voz y SMS son seguros, verificables y cuentan con mecanismos efectivos de protección. Si los usuarios pierden confianza en estos canales por la proliferación de fraudes, la afectación no recae sobre un solo operador, sino sobre la sostenibilidad y reputación del ecosistema en su conjunto. En consecuencia, la colaboración basada en información agregada, no sensible y orientada a resultados constituye un complemento necesario de la competencia y no una restricción a ella.

En este orden de ideas, la CRC acepta parcialmente el comentario de **CLARO**. En consecuencia, se ajusta la resolución para eliminar el contenido del literal (b) del numeral 2.1.10.7.2.1.5 correspondiente a la obligación de reportar individualmente eventos descartados como falsos positivos y los factores de contexto específicos asociados a cada descarte automatizado.

No obstante, se mantendrá la obligación de reportar información agregada sobre eventos detectados, patrones identificados, acciones adoptadas, restricciones aplicadas, casos escalados, PQR y, cuando sea técnicamente disponible, indicadores agregados sobre falsos positivos o descartes. Esta información resulta necesaria para evaluar la efectividad de los sistemas sin imponer cargas desproporcionadas, sin afectar el desempeño operativo de la red y sin comprometer la confidencialidad de los algoritmos, códigos fuente o configuraciones propietarias de los PRST.

2.11.3 Optimización del régimen de reportes de información y acceso en tiempo real a la información del SENDER ID

En el marco de la revisión de los reportes de información, la CRC consideró pertinente revisar la necesidad de mantener el Formato T.5.9 — Reporte de información de SENDER ID, previsto en el proyecto de resolución como un reporte periódico a cargo del validador centralizado. De acuerdo con el proyecto, dicho formato tendría periodicidad trimestral, contenido mensual y plazo de presentación de hasta treinta días calendario después de finalizado el trimestre, y sería diligenciado por el validador centralizado encargado de la administración, validación y trazabilidad de los SENDER ID utilizados en servicios de mensajería SMS A2P.

El proyecto también indicó que el Formato T.5.9 contendría información asociada a los SENDER ID que cursen tráfico a través del esquema de validación centralizado, con el fin de reportar el uso, tráfico, implementación y cumplimiento del recurso asignado. La finalidad del Formato T.5.9 fue que la CRC contara con información periódica, estructurada y comparable sobre el funcionamiento del esquema de SENDER ID, incluyendo información sobre su uso, tráfico, implementación y cumplimiento. Esta información resulta relevante para que la Comisión pueda ejercer seguimiento regulatorio sobre el funcionamiento del esquema de validación centralizada, identificar desviaciones, evaluar tendencias y adoptar medidas de ajuste cuando resulte necesario.

No obstante, la CRC considera que la existencia del validador centralizado permite avanzar hacia un esquema más eficiente de acceso a la información. En lugar de mantener un reporte periódico adicional, que exige consolidación, corte temporal, remisión formal y posterior procesamiento por parte de la Comisión, resulta más eficiente establecer una obligación para que el validador centralizado habilite a la CRC un acceso seguro, permanente y en tiempo real a la información relevante del sistema, mediante una API u otro mecanismo tecnológico equivalente que defina la Comisión.

Este ajuste permite conservar e incluso mejorar la finalidad regulatoria originalmente perseguida por el Formato T.5.9. La eliminación del formato no implica reducir la capacidad de supervisión de la CRC ni limitar el acceso a la información sobre SENDER ID. Por el contrario, sustituye un esquema periódico y diferido por un mecanismo de acceso más oportuno, trazable y eficiente, que permite a la Comisión consultar la información directamente cuando sea necesario y con mayor actualidad que la obtenida mediante reportes trimestrales con contenido mensual.

Desde la perspectiva de simplificación normativa, este ajuste resulta consistente con la necesidad de racionalizar el régimen de reportes de información. Los operadores y agentes regulados han manifestado de manera recurrente la importancia de reducir cargas de reporte, evitar duplicidades y optimizar los requerimientos de información. En ese contexto, la CRC viene realizando esfuerzos permanentes para revisar sus esquemas de reporte, privilegiando mecanismos que permitan acceder a información útil, oportuna y verificable, sin imponer cargas formales innecesarias cuando existen alternativas tecnológicas más eficientes.

En este caso, la información que se pretendía recolectar a través del Formato T.5.9 puede ser obtenida directamente desde el sistema administrado por el validador centralizado. Por tanto, mantener simultáneamente un reporte periódico y una fuente centralizada de información podría generar una carga redundante, tanto para el validador como para la CRC, sin aportar un valor regulatorio adicional frente a un acceso directo y seguro.

La CRC considera, además, que este ajuste mejora la calidad y oportunidad de la información disponible. Un reporte periódico refleja la situación del sistema en cortes definidos y depende de procesos posteriores de consolidación y envío. En cambio, el acceso mediante API permite consultar información actualizada, reducir reprocesos, evitar inconsistencias entre bases de datos y facilitar el seguimiento regulatorio permanente del uso de los SENDER ID y del funcionamiento del esquema de validación.

En todo caso, el acceso en tiempo real deberá implementarse bajo condiciones de seguridad, disponibilidad, trazabilidad, integridad y confidencialidad de la información. La obligación del validador centralizado deberá prever que la CRC pueda acceder a la información necesaria para el ejercicio de sus funciones regulatorias, de seguimiento y supervisión, sin que ello implique publicar información sensible ni alterar las reglas de tratamiento de datos personales, reserva comercial o seguridad de la información que resulten aplicables.

Teniendo en cuenta lo anterior, la CRC elimina la creación el Formato T.5.9 — Reporte de información de SENDER ID y, en su lugar, incorpora una obligación a cargo del validador centralizado consistente en habilitar a la CRC acceso seguro, permanente y en tiempo real a la información del sistema de validación centralizada mediante una API o mecanismo tecnológico equivalente.

Esta decisión responde a un criterio de simplificación normativa y de optimización del régimen de reportes de información, en la medida en que sustituye una obligación periódica de remisión por un mecanismo más eficiente de acceso directo a la información. Con ello se reduce la carga formal asociada al reporte, se evitan duplicidades y se fortalece la capacidad de la CRC para consultar información actualizada sobre el uso, implementación, trazabilidad y cumplimiento de los SENDER ID.

2.12 Comité Técnico de Seguimiento y coordinación operativa

CLARO

Considera innecesario el CTS, ya que dice que la CRC tiene la obligación de hacer este seguimiento, sin que sea requisito la creación de este. Expone que existe ausencia de la justificación de las razones por la cuales los asignatarios de códigos cortos deben ser miembros de este comité, ya que solo deberían ser invitados. De la misma manera, expone que no debe haber un sistema de votación para tomar decisiones, toda vez que no se puede establecer una nueva instancia regulatoria.

Señala que, si la CRC quiere hacer estos seguimientos, puede citar a reuniones periódicas y tomar sus respectivas conclusiones, sin que exista un proceso de votación y de decisiones sobre los regulados. En ese sentido, señala que lo establecido en el artículo 6.13.5.1.11 sobre la naturaleza y la vinculatoriedad de las determinaciones del CTS debe ser eliminado.

En resumen, señala que el regulador no puede imponer implementaciones técnicas, sin la realización de un análisis de impacto normativo.

Respuesta CRC:

Sobre esta temática se pronunció **CLARO**, cuyo comentario se dirige contra el Comité Técnico de Seguimiento (CTS) creado en el artículo 6.13.5.1. En síntesis, el agente formula cuatro cuestionamientos: (i) que el CTS es innecesario, por cuanto la CRC ya tiene la obligación de hacer seguimiento sin que se requiera crear una instancia para ello; (ii) que los asignatarios de código corto A2P no deberían ser miembros del Comité, sino invitados; (iii) que no debe existir un sistema de votación para adoptar decisiones, pues no puede establecerse una nueva instancia regulatoria; y (iv) que debe eliminarse el numeral 6.13.5.1.11, sobre la naturaleza y vinculatoriedad de las determinaciones del CTS, porque el regulador no puede imponer implementaciones técnicas sin realizar un análisis de impacto normativo (AIN). Este planteamiento converge con la preocupación que el mismo agente expresó frente al CTLFSM sobre el riesgo de que los comités se conviertan en mecanismos de regulación paralela, y

guarda relación con la solicitud de **ASOBANCARIA** de asegurar la participación del sector financiero con voz en el CTS.

2.12.1 Sobre el diseño del CTS contenido en el proyecto de resolución y en el documento soporte

Conviene recordar el diseño de la medida. El artículo 6.13.5.1 crea el CTS como instancia permanente de carácter consultivo bajo la dirección de la CRC, cuyo objeto (6.13.5.1.1) es el seguimiento a la implementación y operación del nuevo régimen de código corto A2P, SENDER ID y plantillas de contenido, y la coordinación de la respuesta del ecosistema frente a incidentes de fraude.

Conforme al artículo 6.13.5.1.2, el CTS está conformado por los asignatarios de código corto A2P, con la CRC en la presidencia y la secretaría técnica; el validador centralizado participa como invitado permanente con voz y sin voto; y los PRST, los asignatarios de SENDER ID, los gremios y las entidades competentes concurren como invitados a sesiones específicas.

El artículo 6.13.5.1.9 prevé que las propuestas se adopten por mayoría simple de los miembros con derecho a voto; y el artículo 6.13.5.1.11 dispone que, además de su naturaleza consultiva y técnica frente a la CRC, las determinaciones sobre parámetros técnicos de operación son de cumplimiento obligatorio para los asignatarios de código corto A2P, los PRST y el validador centralizado en los términos y plazos de la respectiva acta.

El proyecto publicado contemplaba, en paralelo, el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles (CTLFSM), creado en el artículo 2.1.10.7.3 como instancia de intercambio de alertas, identificación de patrones de fraude y revisión técnica de medidas frente al fraude cibernético en los servicios de voz móvil y SMS, tanto en el ecosistema P2P como en el A2P.

2.12.2 Supresión del CTS y consolidación de funciones en el CTLFSM

Revisadas las intervenciones de **CLARO** y de **ASOBANCARIA** en este capítulo, junto con las de **BLIPBLIP**, **ETB**, **INETUM**, **NEXVIA** y **SCAMZERO** en el capítulo denominado «Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM», la Comisión advierte que ambas instancias comparten un mismo objeto material (la revisión técnica de las medidas de mitigación del fraude en servicios móviles y la coordinación de la respuesta del ecosistema frente a incidentes), un mismo liderazgo (la CRC, que preside y ejerce la secretaría técnica de las dos), un núcleo común de participantes y un mismo tipo de producto que son determinaciones técnicas destinadas a servir de insumo a la actualización de la regulación.

La coexistencia de dos comités con ese grado de solapamiento genera duplicidad de instancias, multiplica la carga administrativa de los agentes que deben concurrir a ambas, fragmenta la visión del fenómeno del fraude entre los ecosistemas P2P y A2P (cuando la evidencia recogida en el documento soporte muestra que las modalidades de fraude migran entre uno y otro) y dificulta la trazabilidad de

los insumos técnicos que alimentan la adaptación regulatoria. Adicionalmente, tal duplicidad resulta contraria al mandato de simplificación regulatoria del artículo 19 de la Ley 1341 de 2009, modificado por el artículo 15 de la Ley 1978 de 2019, invocado por varios agentes a lo largo del proceso.

Por lo anterior, la Comisión adopta una solución de mayor alcance que la propuesta por el agente. Así, en lugar de ajustar el CTS, lo suprime como instancia autónoma e incorpora la integridad de sus funciones en el CTLFSM, que subsiste como única instancia permanente de coordinación técnica del proyecto. En consecuencia:

- Se suprimen los artículos 6.13.5.1 a 6.13.5.1.13 de la Sección 5 del Capítulo 13 del TÍTULO VI de la Resolución CRC 5050 de 2016.

- La Sección 5 del Capítulo 13 del TÍTULO VI se renombra «Seguimiento y reporte de incidentes» y conserva únicamente las reglas de seguimiento y reporte de incidentes, que se renumeran como artículo 6.13.5.1 y sus numerales.

- Se modifican el artículo 2.1.10.7.3 y sus numerales para incorporar al CTLFSM la totalidad de las funciones que el proyecto publicado atribuía al CTS, incluidas el seguimiento a la implementación y operación del régimen de código corto A2P, SENDER ID y plantillas de contenido A2P, y la coordinación de la respuesta del ecosistema frente a incidentes de fraude.

Ninguna de las funciones del CTS se pierde con la fusión. Por el contrario, todas se reubican en el CTLFSM. El nuevo numeral 2.1.10.7.3.1 recoge expresamente el seguimiento a la implementación del régimen, la revisión y recomendación de actualización de los parámetros técnicos de monitoreo del tráfico A2P —incluidos los umbrales de detección de patrones anómalos y los criterios de gestión de las listas dinámicas de URL y de dominios fraudulentos—, el análisis de los incidentes de fraude, la recomendación de acciones correctivas y preventivas, la facilitación del intercambio de información entre los actores del ecosistema con observancia de las disposiciones sobre protección de datos personales y confidencialidad, la recomendación de ajustes regulatorios y la documentación en actas.

2.12.3 Sobre la conformación del CTS y la incorporación de los PRSTM como miembros

La Comisión no acepta la solicitud de degradar a los Integradores Tecnológicos —que, conforme a la definición del proyecto, son los asignatarios del recurso de identificación denominado código corto A2P— a la condición de invitados. Estos agentes son claves en el nuevo régimen: son titulares del código corto A2P y están obligados a integrarse con el validador centralizado y a cursar el tráfico A2P, de modo que su participación con voz y voto en las sesiones que tengan por objeto ese ecosistema es coherente con el objeto del Comité, que es precisamente la coordinación y el seguimiento de la operación que ellos ejecutan.

La Comisión sí acepta la incorporación de los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM) con voz y voto en las sesiones relativas al ecosistema A2P. Los PRSTM son los operadores de la red sobre la que se cursa el tráfico A2P y destinatarios de las determinaciones técnicas de operación (integración con el validador, enrutamiento, umbrales de monitoreo), de modo que su participación con voto atiende, por la vía de la participación, la asimetría advertida por **CLARO**, según la cual el CTS podía adoptar determinaciones que involucraban a los PRST sin que estos concurrieran a su adopción.

La fusión permite ir más allá y atender esa asimetría de raíz mediante una regla de participación según la temática, incorporada en el numeral 2.1.10.7.3.2. Conforme a esa regla, la CRC cita a cada sesión únicamente a los agentes obligados al cumplimiento de las medidas que constituyan su objeto: cuando la sesión verse sobre las medidas aplicables al servicio de voz móvil o al tráfico P2P, serán citados con voz y voto los PRST obligados a tales medidas; cuando verse sobre la revisión técnica, la implementación o la operación del ecosistema A2P, serán citados con voz y voto los Integradores Tecnológicos y los PRSTM; y cuando verse sobre materias distintas —intercambio de información, estadísticas agregadas o alertas de fraude—, la CRC citará a los agentes, entidades o autoridades cuya concurrencia resulte pertinente. De este modo, ningún agente es convocado a votar sobre medidas de las que no es destinatario, ni queda excluido de la deliberación sobre las medidas que sí lo obligan.

El validador centralizado conserva su condición de invitado permanente, con voz y sin voto, y su citación es obligatoria en toda sesión que tenga por objeto el ecosistema A2P, en atención a las observaciones de **INETUM** y de **CLARO** sobre la conveniencia de su concurrencia por custodiar la base de datos de marcas, contratos KYC y plantillas. Los asignatarios de SENDER ID, las asociaciones gremiales del sector, los organismos internacionales de referencia y las entidades del orden nacional con competencias en prevención del fraude cibernético conservan su calidad de invitados, con voz y sin voto.

2.12.4 Sobre la solicitud de ASOBANCARIA de participación del sector financiero

La Comisión acoge la solicitud de **ASOBANCARIA** de asegurar la participación del sector financiero. El numeral 2.1.10.7.3.2 habilita expresamente a la CRC para citar como invitado, con voz y sin voto, a un representante del sector financiero a través de su gremio, así como a organizaciones representativas de los usuarios y de la protección al consumidor digital, cuando los temas de la agenda así lo ameriten. La preocupación del agente sobre la subordinación de las entidades financieras a la operación de un agente privado pierde su objeto con la fusión: la instancia subsistente es presidida por la CRC, su secretaría técnica es ejercida por la Comisión y sus decisiones no vinculan de manera directa o autónoma a ningún agente, según se expone a continuación.

2.12.5 Sobre el sistema de votación y la naturaleza de las determinaciones del Comité (6.13.5.1.11)

En este punto, la Comisión acoge el comentario de **CLARO** y adopta una solución más completa que la solicitada. La Comisión coincide en que ni el CTS ni el CTLFSM constituyen ni pueden constituir una nueva instancia regulatoria, y en que la potestad regulatoria es indelegable y permanece exclusivamente en cabeza de la CRC. En consecuencia, el numeral 2.1.10.7.3.4 de la resolución dispone que las decisiones del CTLFSM tienen, en todos los casos, el carácter de recomendaciones técnicas dirigidas a la CRC y no constituyen imposiciones regulatorias autónomas adoptadas por vía de acta. Bajo esa redacción: (i) no son vinculantes para la CRC ni afectan sus competencias en materia de regulación; y (ii) no crean, modifican, adicionan, degradan ni derogan obligaciones regulatorias, y en ningún caso pueden desmejorar los parámetros técnicos mínimos del artículo 2.1.10.7 ni las obligaciones del Capítulo 13 del TÍTULO VI.

Con ello se atiende de raíz la objeción según la cual el regulador impondría implementaciones técnicas por vía de acta: ninguna obligación nace del acta del Comité. Cuando la CRC, en ejercicio de su autonomía regulatoria, acoja total o parcialmente una recomendación técnica, la incorporará al marco regulatorio mediante resolución.

El sistema de votación se conserva, pero cambia de naturaleza: no es el mecanismo mediante el cual se imponen determinaciones a los regulados, sino el mecanismo mediante el cual el Comité formaliza y documenta sus recomendaciones técnicas. Cada participante obligatorio citado tiene un voto, con independencia de su tamaño o participación de mercado; las recomendaciones se entienden adoptadas por mayoría simple de los asistentes; las abstenciones se registran sin sumarse a ninguna opción; y las posturas empatadas quedan incluidas en el acta con los argumentos de cada posición, sin que la CRC cuente con voto dirimente, pues un voto de esa naturaleza carecería de sentido sobre un producto que no la vincula. La Comisión no acepta, en cambio, la solicitud de suprimir todo mecanismo de adopción de recomendaciones, pues ello privaría al Comité de su utilidad como instancia de coordinación técnica y devolvería al ecosistema la dispersión que la medida busca evitar.

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

3.1 Bloqueo de llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano

ASOBANCARIA

Sostiene que el Proyecto incorpora obligaciones de etiquetado, validación y bloqueo que pueden incidir en servicios financieros críticos dependientes de los canales de SMS y voz (alertas transaccionales, mensajes de seguridad, códigos OTP y confirmaciones de identidad, entre otros). A diferencia de la

mensajería comercial, estas comunicaciones forman parte de la arquitectura de prevención del fraude, por lo que su interrupción, demora o clasificación errónea podría comprometer la seguridad de las transacciones, abrir ventanas de exposición o retrasar la reacción frente a operaciones sospechosas.

En ese contexto, **ASOBANCARIA** indica, frente al bloqueo de llamadas internacionales, que el bloqueo de llamadas entrantes con numeración nacional (CLI), salvo el roaming debidamente identificado, podría afectar comunicaciones legítimas de entidades que se apoyan en centros de contacto o enrutamiento internacional. Por ello, solicita prever un tratamiento específico para su tráfico internacional legítimo.

Por lo anterior, **ASOBANCARIA** estima necesario prever procedimientos diferenciados y prioritarios para las comunicaciones de las entidades vigiladas por la SFC (especialmente mensajes transaccionales, alertas de seguridad y autenticación reforzada), de modo que no queden sujetas a restricciones que generen latencia o bloqueos.

ANDESCO

Indica que el artículo 2.1.10.7.2.2.1 prohíbe absolutamente las llamadas internacionales entrantes que presenten CLI colombiano, salvo roaming identificado. Afirma que el artículo 2.1.10.7.2.2.3 obliga a bloquear todas las llamadas que presenten numeración incluida en la Lista DNO. Ambas prohibiciones carecen de excepciones para casos de uso legítimos.

Dice que una prohibición absoluta sin excepciones puede afectar actividades lícitas garantizadas por la libertad de empresa (Art. 333 CP). Las restricciones deben ser proporcionales y prever mecanismos de excepción para casos justificados. La ausencia de un marco de attestation previo a la prohibición (equivalente a STIR/SHAKEN) significa que se prohíbe una conducta sin primero crear las herramientas técnicas para distinguir entre CLI legítimo y CLI suplantado en el tráfico internacional.

Recomienda establecer un procedimiento de inscripción voluntaria para clientes corporativos que usen numeración colombiana desde el exterior con fines legítimos (análogo al etiquetado de llamadas publicitarias), un proceso expedito de revisión para titulares de numeración bloqueados erróneamente por la Lista DNO, con resolución en máximo 48 horas y un plazo de 18 meses para desarrollar un marco de attestation de llamadas (STIR/SHAKEN adaptado al contexto colombiano) que permita a futuro distinguir técnicamente entre CLI legítimo y suplantado, antes de implementar la prohibición absoluta.

En complemento de lo anterior, indica que en materia de llamadas internacionales con CLI colombiano, la carga regulatoria debe asignarse principalmente a los originadores del tráfico y a los carriers internacionales que transportan o entregan llamadas con información irregular de origen, sin recargar al PRST terminante con obligaciones que no puede controlar integralmente.

Propone que, en lugar de prohibir el CLI spoofing de forma absoluta sin herramientas técnicas de distinción, la CRC debe liderar el desarrollo de un marco de attestation de llamadas (equivalente al STIR/SHAKEN norteamericano adaptado al contexto colombiano) en un plazo de 18-24 meses, con los

PRST y la industria de carriers internacionales. Este marco permitiría a futuro distinguir técnicamente entre llamadas con CLI legítimo y llamadas con CLI suplantado, haciendo la prohibición más efectiva y menos propensa a falsos positivos.

BYTECOL

Advierte que algunas medidas propuestas, como el bloqueo de llamadas internacionales entrantes con CLI colombiano, podrían generar impactos desproporcionados sobre comunicaciones legítimas, especialmente en entornos de telefonía IP, centros de contacto y servicios en la nube. En ese sentido, enfatiza que la regulación debe enfocarse en diferenciar de forma técnica y proporcional las comunicaciones fraudulentas de las legítimas, para evitar que medidas antifraude afecten canales formales de atención, autenticación, cobranza y servicio al cliente.

Plantea que, aunque el proyecto busca proteger a los usuarios frente a llamadas no deseadas, comerciales abusivas y fraudulentas, es necesario diferenciar dentro de las comunicaciones empresariales tres categorías: llamadas fraudulentas, llamadas comerciales o publicitarias y gestiones de cobranza, atención contractual y comunicaciones transaccionales o de servicio, destacando que estas últimas son actividades lícitas y reguladas por normas como la Ley 2300 de 2023, por lo que no deben ser tratadas como publicidad o fraude ni sujetas a bloqueo o etiquetado por esa condición.

Asimismo, frente a la propuesta de bloquear llamadas internacionales entrantes con CLI colombiano, advierte que esta medida no considera adecuadamente el funcionamiento del ecosistema actual de comunicaciones, donde el uso de telefonía IP, SIP trunks y plataformas en la nube puede implicar el uso legítimo de numeración colombiana desde infraestructura internacional. En ese sentido, señala que el problema central no es la ruta técnica, sino la falta de trazabilidad y verificación del origen, por lo que un bloqueo general podría afectar tanto a actores fraudulentos como a comunicaciones legítimas, reduciendo la confianza del usuario y desplazando el tráfico hacia canales menos regulados, con impacto en servicios esenciales como los financieros y de cobranza.

Expone que el proyecto no diferencia adecuadamente entre llamadas fraudulentas, llamadas comerciales y comunicaciones legítimas asociadas a relaciones contractuales preexistentes, como la cobranza, la autenticación, la prevención del fraude o la atención al cliente. **BYTECOL** sostiene que estas últimas cumplen funciones esenciales y ya están sujetas a regulación específica, por lo que no deberían recibir el mismo tratamiento que las llamadas publicitarias o fraudulentas. En consecuencia, solicita que la resolución establezca expresamente que las gestiones de cobranza y demás comunicaciones transaccionales o de servicio queden excluidas de las medidas de bloqueo y etiquetado previstas para llamadas publicitarias.

Otro desacuerdo importante se refiere a la presunción de que toda llamada internacional que utilice un número colombiano es sospechosa de fraude. **BYTECOL** argumenta que, en el contexto actual de las comunicaciones empresariales, numerosas organizaciones utilizan infraestructura internacional o plataformas de telefonía IP para originar llamadas legítimas con numeración colombiana autorizada.

Desde su perspectiva, el verdadero problema no es la ruta técnica de la llamada, sino la ausencia de mecanismos que permitan verificar de manera confiable la identidad del originador. Por ello, considera que un bloqueo indiscriminado afectaría tanto a actores fraudulentos como a empresas que operan legítimamente y cuyos usuarios necesitan reconocer el número desde el cual son contactados.

En desarrollo de este argumento, **BYTECOL** cuestiona la proporcionalidad de la medida propuesta. Señala que el bloqueo general no constituye la alternativa más adecuada porque no distingue entre comunicaciones legítimas y fraudulentas, no permite procesos de verificación y puede impedir llamadas relacionadas con pagos, autenticaciones, prevención del fraude, atención al cliente y otras comunicaciones necesarias. Además, advierte que los defraudadores podrían migrar fácilmente a otros canales, mientras que los usuarios perderían acceso a comunicaciones legítimas.

Como alternativa, la empresa propone sustituir el bloqueo general por un esquema de verificación de origen que permita acreditar previamente la legitimidad de las llamadas. Entre sus propuestas destacan la creación de un registro para proveedores y originadores legítimos; la obligación de conservar documentación sobre la identidad del cliente, la finalidad de la comunicación y la trazabilidad técnica; la utilización de un etiquetado informativo en lugar del bloqueo cuando el origen pueda verificarse; y la incorporación de un «puerto seguro» que limite la responsabilidad de los proveedores que hayan cumplido diligentemente con los mecanismos de verificación establecidos por la CRC.

Asimismo, **BYTECOL** propone que cualquier régimen de bloqueo incorpore un procedimiento de revisión ágil que pueda ser solicitado no solo por el titular de la línea, sino también por proveedores de telefonía IP, operadores, clientes corporativos, entidades financieras, empresas de cobranza y usuarios afectados.

Igualmente, solicita que el Análisis de Impacto Normativo evalúe específicamente las consecuencias de la regulación sobre la telefonía IP, los centros de contacto, el sector financiero y las comunicaciones empresariales legítimas, incluyendo los posibles costos derivados de bloqueos erróneos y la eventual migración del tráfico hacia plataformas OTT menos reguladas. También plantea que las obligaciones regulatorias se distribuyan de acuerdo con las capacidades reales de cada actor de la cadena y advierte que una regulación excesivamente restrictiva podría generar distorsiones en la competencia al favorecer canales no sujetos al mismo nivel de supervisión.

Finalmente, **BYTECOL** presenta una propuesta concreta de ajustes normativos. Entre ellos solicita incorporar una excepción al bloqueo para las llamadas con origen verificado; excluir expresamente las gestiones de cobranza, comunicaciones transaccionales, autenticación y prevención del fraude del concepto de llamadas publicitarias; establecer un sistema de etiquetado diferenciado para llamadas verificadas; crear un procedimiento de revisión de bloqueos y etiquetados; reconocer un régimen de responsabilidad limitado para los proveedores diligentes; y prever un período de implementación gradual una vez se definan los estándares técnicos. En sus peticiones finales reitera que comparte el objetivo de combatir el fraude, pero insiste en que las medidas regulatorias deben preservar las comunicaciones legítimas, proteger a los usuarios sin afectar de forma desproporcionada a los proveedores de telefonía IP y garantizar el funcionamiento de sectores como el financiero y el de cobranzas.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CLARO

Señala que la identificación de tráfico de líneas que están en roaming internacional real, sólo lo puede determinar la red home o el PRST dueño de la línea, no lo puede saber el carrier de origen ni otro PRST nacional.

Aunado a lo anterior, menciona que si un tráfico LDI entrante viene con identificador (CLI) con numeración colombiana que pertenezca a un PRST distinto al que se va a entregar, no va a ser posible bloquear por el PRST destino porque no puede determinar si es tráfico de un usuario en Roaming o si tráfico con enmascaramiento de origen con numeración nacional.

Adicionalmente, se solicita a la CRC que incluya en el artículo 2.1.10.7.2.2.1 lo siguiente:

«El incumplimiento reiterado de esta disposición por parte de un carrier internacional facultará al PRST colombiano para realizar la suspensión inmediata del acuerdo de interconexión por motivos de riesgo de ciberseguridad nacional, notificando el hecho a la CRC y a la Superintendencia de Industria y Comercio (SIC).

Queda expresamente prohibido el uso de los nodos y acuerdos de interconexión internacional (LDI) para el ingreso, tránsito o terminación de tráfico de voz con fines publicitarios, comerciales o de cobranza dirigidos a usuarios en el territorio nacional, cuando dichos contenidos sean promovidos u originados por o a nombre de personas naturales o jurídicas nacionales. En caso de que un PRST detecte la configuración de este escenario a través de sus sistemas de monitoreo, estará plenamente facultado para realizar la suspensión inmediata y preventiva de la ruta o del acuerdo de interconexión con el carrier internacional que entregue dicho tráfico, sin que esto configure una violación a los niveles de servicio ni a las obligaciones de interconexión regulatoria, debiendo reportar la evidencia técnica ante la CRC y la SIC en un plazo no mayor a cinco (5) días hábiles».

ETB

Considera que el proyecto concentra de manera excesiva las obligaciones de detección y mitigación sobre los operadores receptores nacionales, sin reconocer que una parte sustancial de la capacidad técnica para identificar irregularidades se encuentra precisamente en los carriers internacionales y en los puntos donde se origina o transporta el tráfico hacia Colombia.

ETB estima necesario que la CRC avance hacia la incorporación de obligaciones explícitas de trazabilidad, auditoría, conservación de registros, validación de identificadores y cooperación operativa para los carriers internacionales que participan en el transporte de tráfico hacia el país.

SAEM

Afirma que el proyecto prohíbe el enmascaramiento del CLI y se ordena bloquear llamadas internacionales entrantes con CLI nacional (2.1.10.7.2.2.1); se exige monitoreo en tiempo real con etiquetado «Alerta de llamada sospechosa» (2.1.10.7.2.2.2); se crea el registro de «Llamada con fines

publicitarios», con bloqueo cuando el destinatario esté en el RNE (2.1.10.7.2.2.2.1); y se impone la lista DNO (2.1.10.7.2.2.3).

Al respecto, indica que las campañas legítimas de voz (notificación, encuestas, cobranza autorizada) suelen usar un número único de retorno, que un monitoreo mal calibrado puede confundir con robocall y etiquetar o bloquear, afectando la contactabilidad legítima. Dice que la prohibición de enmascaramiento es razonable frente al fraude, pero requiere precisar que el uso legítimo de un CLI de retorno corporativo no constituye enmascaramiento.

Sostiene que el marco STIR/SHAKEN de autenticación de identificador de llamada en Estados Unidos y Canadá —que el propio proyecto evaluó como alternativa— redujo parte del spoofing, pero las llamadas fraudulentas persistieron, especialmente desde gateways internacionales y redes no IP, confirmando que el origen ilícito y los puntos de entrada no autenticados son el verdadero foco. Ello respalda, según **SAEM**, concentrar el esfuerzo en el bloqueo del tráfico internacional con CLI nacional falsificado, más que en cargar al originador formal.

Propone lo siguiente: (i) Precisar que el uso de un CLI de retorno corporativo legítimo, asignado y verificable, no constituye enmascaramiento; (ii) calibrar los umbrales de detección de robocall (ACD/ASR) en el marco del CTLFSM, con participación de los originadores corporativos, para evitar falsos positivos; (iii) priorizar y dotar de recursos el bloqueo del tráfico internacional entrante con CLI nacional falsificado, foco principal del fraude.

Concretamente, solicita precisar que el uso de un CLI de retorno corporativo legítimo no constituye enmascaramiento, y concentrar el esfuerzo en el bloqueo del tráfico internacional entrante con CLI nacional falsificado.

SSC

Dice que comparte plenamente el objetivo del proyecto: combatir el fraude y proteger al usuario. Afirma que su intervención no controvierte ese fin, sino el medio elegido para alcanzarlo. Solicita a la CRC que se abstenga de adoptar el bloqueo de las llamadas con identificador de línea llamante (CLI) nacional como regla general, por las razones de fondo y de procedimiento que se exponen, y adopte en su lugar un mecanismo de verificación y autenticación de origen, que sirve mejor al mismo objetivo. Adicionalmente, dice que es importante que la CRC haga un análisis jurídico sobre la medida que se quiere adoptar y su impacto sobre la violación al principio de neutralidad de red, principio de origen legal y que su limitación debe estar regido por otra Ley o por orden de autoridad judicial. Asimismo, el bloqueo planteado, afecta a algunos usuarios, que de acuerdo al estudio, no se plantea un mecanismo para evitar vulnerar el derecho de esas personas, ni la forma de restablecerlo; por lo que se solicita una referencia así sea sumaria sobre esos dos puntos.

Sostiene que el fraude telefónico es un fenómeno grave que exige acción decidida del Estado, y los operadores son los primeros perjudicados por él. Dice que la discusión no está en el fin, sino en cómo

alcanzarlo sin causar un daño mayor que el que se quiere evitar. Afirma que la raíz del problema es una sola: en la señalización tradicional no es posible distinguir, de forma confiable, el origen real de una llamada que entra del exterior presentando un CLI nacional. Esa imposibilidad afecta por igual a los tres actores del ecosistema:

• El usuario no puede saber, al recibir la llamada, si quien lo contacta es realmente su banco o un defraudador que presenta el mismo número; por ello cae en el engaño.

• El operador de LDI no puede acreditar ante la red de destino que un tráfico legítimo lo es, ni separarlo del fraudulento, pues la información del originador se diluye en la cadena internacional de intermediarios, y dificulta al operador nacional, así sea de LDI conocer la procedencia completa del tráfico, con el agravante que ese tipo de exigencias a los prestadores internacionales - conectantes – pueden no ser de recibo o simplemente hacen que se tomen medidas de enmascarar mucho antes de que sea entregadas a nosotros.

• La autoridad y los operadores móviles no pueden distinguir la llamada legítima de la suplantada, y ante esa ceguera se ven tentados a tratar todo el tráfico por igual.

Esa carencia común tiene un nombre técnico: falta de trazabilidad y autenticación del origen. Es la causa estructural. El fraude, el riesgo para el tráfico legítimo y la dificultad regulatoria son manifestaciones de la misma ausencia. Cualquier medida que no ataque esa causa —sino solo uno de sus síntomas— resultará, por definición, ineficaz.

Menciona que conviene precisar, ante todo, por qué una llamada que presenta un número colombiano puede ingresar al país por una ruta internacional, pues de ello depende comprender que no se trata de una anomalía sospechosa, sino de la forma en que operan hoy las comunicaciones empresariales. Dice que según se advirtió en la etapa anterior de este proceso, sin que la observación fuera atendida, las empresas que se comunican con sus clientes —entidades financieras, aseguradoras, aerolíneas, prestadores de salud, comercios— ya no lo hacen, en su mayoría, desde infraestructura física ubicada en Colombia, sino a través de plataformas tecnológicas en la nube (CPaaS/OTT) y de centros de contacto cuya infraestructura se encuentra en el exterior.

Afirma que, cuando esas plataformas cursan una llamada en nombre de la empresa, presentan el número colombiano que legítimamente le pertenece al cliente, aunque la llamada se origine técnicamente en infraestructura internacional. La numeración es real y está asignada al cliente; lo que es internacional es el medio que la transporta. En la práctica, esta operación supone que el titular de la numeración autoriza a la plataforma a presentar su número como identificador de línea llamante cuando cursa comunicaciones en su nombre. Esa autorización ocurre hoy de hecho, pero sin un soporte documental estandarizado ni un mecanismo regulatorio que permita acreditarla; en ningún caso implica cesión ni transferencia del recurso, que permanece asignado al cliente y bajo su responsabilidad. Formalizar y hacer verificable esa cadena de autorización es, precisamente, uno de los objetos del esquema de verificación de origen que más adelante se propone. Este tráfico no busca ocultar su origen

ni eludir obligación alguna: paga el cargo de acceso regulado por su terminación y corresponde a comunicaciones empresariales lícitas —verificaciones, cobranzas autorizadas, atención al cliente y notificaciones transaccionales—, que ascienden a millones de comunicaciones al año.

Añade que, de hecho, constituye hoy la mayor parte del tráfico de larga distancia internacional —estimado en alrededor del 80%, proporción que la propia Comisión debe verificar—, como consecuencia de la migración global de las comunicaciones empresariales hacia plataformas en la nube. Debe distinguirse, por tanto, de la suplantación fraudulenta: ambos pueden presentar un CLI nacional desde el exterior, pero el primero corresponde a un cliente real e identificable que ha autorizado el uso de su número, mientras el segundo oculta deliberadamente su origen. Esa distinción —imposible de establecer con el solo dato de la nacionalidad del CLI— es precisamente lo que un mecanismo de verificación de origen permitiría acreditar, y lo que el bloqueo indiscriminado ignora.

Dice que el bloqueo del CLI nacional no supera el test de proporcionalidad. Sostiene que toda medida regulatoria que restringe derechos —en este caso, el derecho del usuario a recibir información veraz e imparcial, reconocido como principio orientador en el artículo 2, numeral 7, de la Ley 1341 de 2009 (en desarrollo de los artículos 20 y 15 de la Constitución Política), así como su derecho a la adecuada y eficiente provisión del servicio de comunicaciones, que la CRC está obligada a proteger conforme a los artículos 2.4, 4.1, 7 y 19 de la misma Ley— debe superar el test de proporcionalidad exigido por la jurisprudencia constitucional, además de ajustarse a los principios de mínima intervención y regulación eficiente que enmarcan la actuación de la CRC. El bloqueo del prefijo +57 en la ruta de tráfico internacional suprime de forma indiscriminada llamadas lícitas que el usuario quiere y necesita recibir, interfiriendo el canal de comunicación sin un análisis individualizado de cada llamada. La medida no supera ninguna de las tres gradas del test —idoneidad, necesidad y proporcionalidad en sentido estricto—.

Respecto de la proporcionalidad dice lo siguiente:

1- No es idóneo (no sirve para el fin)

Qué exige este requisito: una medida solo es válida si efectivamente conduce a lograr el objetivo que persigue.

El bloqueo se condiciona a que el número tenga apariencia colombiana, pero el defraudador evade la medida con solo usar un número de otro país, o trasladándose a aplicaciones de mensajería (OTT), y sigue estafando igual. Una medida que el propio defraudador esquiva con un cambio tan simple no sirve para combatir el fraude: actúa sobre una apariencia —la nacionalidad del número— y no sobre la causa real, que es la imposibilidad de verificar el verdadero origen de la llamada.

Adicionalmente, nosotros los prestadores en Colombia (conexión con el exterior) no podemos adoptar medidas como bloqueos, desconexión provisional, o cuarentenas que ejerzan alguna presión sobre las conectantes internacionales y evitar que se sigan presentando estos eventos, ya que ellos van a seguir

entregando tráfico que pueden enmascarar con numeración de otros países similar a la asignada en Colombia. Por ello, el control y la gestión de su tráfico anómalo resultan inocuos, y la medida recae sobre el eslabón equivocado de la cadena: el prestador nacional, que no tiene cómo incidir sobre el verdadero origen del fraude.

2. No es necesario (existe un medio menos lesivo, que la propia resolución ya emplea)

Qué exige este requisito: si hay otra forma de lograr el mismo objetivo causando menos daño, la autoridad está obligada a escoger esa, no la más drástica.

Ese medio menos drástico existe, y la propia resolución lo usa: en el artículo 2.1.10.7.2.2.2 ordena etiquetar las llamadas sospechosas con una alerta visible («Alerta de llamada sospechosa»), en lugar de bloquearlas.

Es decir, frente a un riesgo de fraude en voz, la Comisión ya eligió advertir al usuario en vez de cortar la llamada. Si para unos casos basta con etiquetar, no se entiende por qué para el tráfico internacional se acude al bloqueo total, que es la medida más severa. El etiquetado, acompañado de la verificación del origen, permite que la autoridad y el usuario distingan lo legítimo de lo fraudulento sin suprimir comunicaciones lícitas: ataca la causa del problema, no su apariencia. La existencia de este medio menos lesivo e igualmente idóneo, ya adoptado por la propia Comisión para supuestos análogos, basta por sí sola para que la medida no supere el test de proporcionalidad, pues su análisis es secuencial y el fracaso de una sola grada determina su invalidez.

3. No es proporcional en sentido estricto (el daño que causa es mayor que el beneficio que produce)

Qué exige este requisito: el beneficio que se obtiene debe ser mayor que el daño que se causa; si el daño pesa más, la medida no se justifica.

El bloqueo elimina comunicaciones legítimas que el usuario quiere y necesita recibir —la verificación de su banco, la confirmación de una cita médica, el aviso de su aerolínea, la cobranza autorizada—, así como la actividad lícita de las empresas que las realizan. A cambio, obtiene un beneficio parcial y fácilmente evadible: el defraudador lo sortea con un simple cambio de numeración. El usuario no queda más protegido: queda desconectado de servicios que necesita, mientras el estafador lo alcanza por otra vía. El daño es cierto; el beneficio, parcial y evadible. La medida causa más perjuicio que provecho.

Conclusión: el bloqueo restringe derechos sin ser necesario para su fin —existiendo un medio menos lesivo e igualmente eficaz que la propia Comisión ya adopta— y sin superar la proporcionalidad en sentido estricto, con una idoneidad además deficiente por no atacar la causa real del fraude. Vulnera, por ello, el derecho del usuario a recibir información (artículo 2, numeral 7, de la Ley 1341 de 2009 y artículo 20 de la Constitución Política) y los principios de mínima intervención y regulación eficiente que rigen la actuación de la CRC (artículos 2.4, 4.1, 7 y 19 de la Ley 1341 de 2009)».

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Además de todo lo anterior, **SSC** dice que el bloqueo distorsiona la competencia sin justificación económica. En concreto, sostiene que el bloqueo carece de justificación económica y, además, distorsiona la competencia en perjuicio del sector regulado. No protege ningún ingreso de los operadores —el cargo de acceso por terminación ya está garantizado por la regulación, con independencia del bloqueo— y, en cambio, desplaza tráfico legítimo hacia plataformas que no pagan ese cargo ni están sujetas a la regulación sectorial. A su juicio, lo anterior se demuestra en dos pasos.

Paso 1. El bloqueo no protege ningún ingreso del operador móvil

Cuando un operador de Larga Distancia Internacional (LDI) entrega una llamada al operador móvil para que la termine, le paga el cargo de acceso, que es un peaje regulado por la propia Comisión. El artículo 4.3.2.8 de la Resolución CRC 5050 de 2016, modificado por la Resolución CRC 7753 de 2025, establece que los proveedores de Larga Distancia Internacional pagan cargos de acceso por originación y por terminación en las redes móviles.

El operador móvil recibe así su remuneración regulada por terminar la llamada, con independencia de la ruta por la que esta llegue. En consecuencia, no existe ningún ingreso del operador que termina la llamada que el bloqueo venga a proteger: ese ingreso proviene del cargo de acceso ya tasado por la Comisión y no depende de bloquear unas llamadas y permitir otras. La medida carece, por este lado, de toda justificación económica.

Paso2. El bloqueo desplaza tráfico legítimo del sector regulado hacia las plataformas OTT no reguladas

Descartada la protección de ingresos, el bloqueo no resulta neutro sobre la estructura del mercado. Una parte sustancial del tráfico internacional con CLI nacional corresponde a comunicaciones legítimas de empresas hacia sus usuarios —avisos comerciales, gestiones de cobranza, notificaciones de servicio—. Bloqueada la ruta de voz, ese tráfico no desaparece: migra hacia las plataformas OTT —señaladamente WhatsApp, que ya ofrece en Colombia productos pagos de mensajería de negocios y de llamadas comerciales, con tarifas fijadas por Meta según el país de destino del usuario—, las cuales terminan la comunicación sobre la red de datos sin pagar cargos de acceso, sin asumir contraprestaciones y sin estar sujetas al régimen de calidad ni a la regulación sectorial de la CRC.

El efecto recae sobre el propio sector regulado, y de manera más aguda sobre los operadores de LDI. Por un lado, los operadores de LDI pierden el transporte de ese tráfico y el margen asociado; el perjuicio es especialmente grave para los operadores de LDI independientes, que carecen de red móvil propia y, a diferencia de los operadores integrados verticalmente, no tienen forma de compensar la pérdida, al punto de que el bloqueo puede comprometer la viabilidad misma de su línea de negocio. Por otro lado, los operadores móviles dejan de percibir el cargo de acceso de voz, pues la comunicación se termina como dato a través de la plataforma. El único beneficiario es un actor —Meta, a través de WhatsApp— que no soporta las cargas regulatorias, tributarias ni de calidad que la Comisión impone a sus regulados.

Así, una medida expedida por la CRC para proteger a los usuarios de sus servicios termina trasladando tráfico legítimo —y los ingresos que lo acompañan— desde los operadores que ella regula hacia plataformas que escapan a esa regulación. Esa redistribución no obedece a que los operadores regulados compitan peor, ofrezcan peor precio o menor calidad, sino a una prohibición regulatoria que cierra la ruta de voz y acelera la migración hacia las OTT. Se trata, por tanto, de una distorsión de la competencia por vía administrativa, no por las dinámicas propias del mercado.

En síntesis, el bloqueo no protege ingreso alguno —pues el cargo de acceso ya lo garantiza— y, en cambio, desplaza tráfico legítimo desde los operadores regulados, especialmente los de LDI, hacia las plataformas OTT no reguladas, en perjuicio de la competencia en el sector. Ese efecto sobre la estructura del mercado es precisamente el que debe evaluar la Superintendencia de Industria y Comercio en sede de abogacía de la competencia, conforme se desarrolla en la sección V de este escrito, antes de la adopción de la medida».

De otra parte, en relación con la abogacía de competencia relacionada con esta medida, **SSC** dice que, si bien el numeral 5 del proyecto anuncia el trámite de abogacía de la competencia ante la Superintendencia de Industria y Comercio, conforme al artículo 7 de la Ley 1340 de 2009 y al Capítulo 30 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, dicho trámite debe abordar de manera específica los efectos que el bloqueo de CLI nacional produce sobre la estructura del mercado de larga distancia internacional descritos en la sección III de su escrito. El concepto de la SIC no es vinculante, pero el artículo 7 obliga a la CRC a motivar expresamente, en las consideraciones del acto, las razones por las cuales se aparte de él, y el artículo 2.2.2.30.7 del mismo Decreto 1074 de 2015 le impone dejar constancia del análisis de competencia en la parte considerativa del acto administrativo. La Sala de Consulta y Servicio Civil del Consejo de Estado, en concepto del 4 de julio de 2013, advirtió que la omisión de este trámite, o el apartamiento inmotivado del concepto, puede acarrear la nulidad del acto administrativo por expedición irregular. Por ello, la CRC no debe expedir la resolución sin que el análisis de competencia se haya pronunciado sobre el desplazamiento de tráfico legítimo desde los operadores regulados hacia las plataformas OTT no reguladas que la medida genera, y sin dejar constancia de ese análisis en la parte considerativa.

Por otro lado, **SSC** propone una medida idónea, necesaria y proporcional es la que ataca la causa raíz —la falta de trazabilidad y autenticación del origen— y no su síntoma. Un esquema de verificación de origen sirve, simultáneamente, a los tres actores: el usuario puede confiar en lo que ve, distinguiendo una llamada verificada de una no verificada; el operador de LDI puede acreditar la legitimidad de su tráfico y separarlo del fraudulento; y la autoridad reduce el fraude real sin suprimir comunicaciones lícitas. **SSC** indica los elementos de esta medida:

• Excepción de origen verificado: junto al roaming, eximir del bloqueo el tráfico con CLI nacional cuyo origen sea certificado por un operador inscrito en un registro ante la CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

• Verificación documental del cliente como condición de la excepción: acreditación de la identidad del cliente, de la asignación legítima de la numeración presentada y de la autorización del titular para su uso.

• Etiquetado en lugar de bloqueo para el tráfico verificable, en coherencia con el artículo 2.1.10.7.2.2.2.

• Puerto seguro de responsabilidad para el operador que certifique el origen conforme al estándar, frente a alteraciones producidas en eslabones anteriores de la cadena que no le eran detectables.

• Mecanismo de impugnación para el operador y el usuario destinatario afectados por el bloqueo o etiquetado de tráfico legítimo.

• Implementación gradual, condicionando los componentes de verificación a la entrada en operación del registro de origen verificado».

Con base en todo lo expuesto, **SSC** eleva las siguientes peticiones:

«1. Abstenerse de adoptar, en el artículo 2.1.10.7.2.2.1, el bloqueo de las llamadas con CLI nacional como regla general, por no superar el test de proporcionalidad.

2. Adoptar en su lugar un esquema de verificación y autenticación de origen, con etiquetado del tráfico no verificado, conforme a la sección VI de este escrito.

3. Completar el Análisis de Impacto Normativo de la medida de bloqueo, cuantificando con datos del tráfico colombiano el volumen y la proporción del tráfico internacional entrante con CLI nacional que corresponde a comunicaciones empresariales legítimas frente al fraudulento, e incorporando el costo del tráfico legítimo que resultaría bloqueado, antes de adoptar la medida.

4. Someter la medida al concepto de abogacía de la competencia de la Superintendencia de Industria y Comercio, por su efecto sobre el mercado de larga distancia internacional (LDI) y el desplazamiento de tráfico legítimo hacia plataformas no reguladas, conforme a las secciones III y V de este escrito.

5. Que, en caso de mantenerse el bloqueo del tráfico con CLI nacional proveniente de la ruta de larga distancia internacional, la obligación de ejecutarlo recaiga sobre el operador propietario de la numeración (operador destino) y no sobre el operador de LDI. El operador destino es el único que conoce en tiempo real el estado de roaming de sus propios abonados y, por tanto, el único en capacidad de distinguir el tráfico de roaming legítimo del que presenta un CLI suplantado. Imponer el bloqueo al operador de LDI —que carece de esa información— produce el bloqueo indiscriminado de comunicaciones legítimas, mientras que asignarlo al operador destino permite bloquear únicamente el tráfico efectivamente fraudulento, preservando el roaming legítimo.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

6. De mantenerse alguna forma de bloqueo, incorporar un puerto seguro de responsabilidad: el operador que verifique y certifique el origen conforme al estándar que defina la CRC no responderá por alteraciones del CLI producidas por terceros en eslabones anteriores de la cadena internacional, que no le eran detectables.

7. Extender el procedimiento de revisión previsto en el artículo 2.1.10.7.2.2.2.2 —hoy limitado al etiquetado y al titular de la línea— para que cubra también los casos de bloqueo de tráfico legítimo y para que pueda ser invocado por el operador de larga distancia internacional y por el usuario destinatario afectados, quienes carecen actualmente de cualquier mecanismo para impugnar el bloqueo de una comunicación lícita.

8. Precisar la fuente, actualización y propagación de la lista DNO (artículo 2.1.10.7.2.2.3) y excluir la responsabilidad por numeración cuya inclusión no era conocible al momento de cursar la llamada.

9. Establecer un plazo de implementación gradual y suficiente para las medidas de prevención de fraude en voz (artículos 2.1.10.7.2.2.4 y 20). En caso de adoptarse el esquema de verificación de origen propuesto en la sección VI, su exigibilidad debe condicionarse a la entrada en operación previa del registro de origen verificado y a la definición del estándar técnico correspondiente, del mismo modo en que el proyecto condicionó la entrada en vigencia del régimen de mensajería A2P a la previa selección del validador centralizado. En caso de mantenerse el bloqueo, su entrada en vigencia debe diferirse y escalonarse para permitir las adecuaciones técnicas necesarias y las pruebas que eviten la supresión de tráfico legítimo, en lugar de su exigibilidad inmediata conforme al artículo 20».

TIGO

Señala que el enmascaramiento se origina y puede modificarse en el origen, fuera del control del PRST terminante. Cita que el propio documento soporte constata que en Colombia no existen hoy implementaciones activas de STIR/SHAKEN, que no es un estándar de uso global —en el benchmark internacional aparece principalmente en países como Brasil, Canadá y Estados Unidos, mientras la mayoría privilegia el bloqueo de llamadas internacionales con numeración local y las listas DNO— y que no es compatible con las redes tradicionales (SS7/ISUP) sin adaptadores, por lo que su efectividad depende de los originadores y de los carriers internacionales. En consecuencia, las obligaciones en voz deben asignarse principalmente a los carriers internacionales y a los originadores del tráfico, sin recargar al último eslabón de la cadena.

Manifiesta que la Comisión reconoce explícitamente en la Sección 11 del documento soporte (Limitaciones y sensibilidad del modelo), la «Migración a redes full IP reduce costos de STIR/SHAKEN». Este reconocimiento técnico constituye el eje central de su postura: el gran reto del regulador debe ser asegurar que la carga económica exigida vaya al estricto ritmo de la modernización e inversión en infraestructura de cada operador, evitando forzar inversiones artificiales en tecnologías que están destinadas a desaparecer.

PTC

Expone que el artículo 2.1.10.7.2.2.1., establece que los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número que haga parte del Plan Nacional de Numeración (PNN) colombiano, **PTC** manifestó que es importante que la CRC incorpore expresamente en la resolución, el formato y la numeración que debe bloquearse «+5760X», «5760X», «60X», «+573X», «573X», «3X» por las rutas LDI, razón por la cual, se sugiere la siguiente redacción:

«2.1.10.7.2.2.1. norma que establece que Los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano, y con numeración «+5760X», «5760X», «60X», «+573X», «573X», «3X» por las rutas destinada a Larga Distancia Internacional (LDI).»

Respuesta CRC:

ASOBANCARIA, **ANDESCO**, **BYTECOL** y **SSC** manifestaron, con diferentes alcances, que el bloqueo de las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración (PNN) colombiano podría afectar comunicaciones legítimas gestionadas mediante centros de contacto, plataformas de telefonía IP, SIP Trunks, soluciones CPaaS o infraestructura tecnológica ubicada en el exterior. En particular, **ASOBANCARIA** y **BYTECOL** hicieron referencia a comunicaciones relacionadas con autenticación, prevención del fraude, alertas financieras, cobranza, atención al cliente y notificaciones transaccionales; mientras **ANDESCO** y **SSC** cuestionaron la ausencia de un mecanismo previo de autenticación o attestation que permita distinguir el CLI legítimo del suplantado.

En esa misma línea, **ANDESCO**, **BYTECOL** y **SSC** solicitaron establecer mecanismos que permitan acreditar previamente la legitimidad de determinados originadores. **ANDESCO** propuso un procedimiento de inscripción voluntaria para clientes corporativos y el desarrollo futuro de un marco de attestation equivalente a STIR/SHAKEN; **BYTECOL** planteó la creación de un registro de proveedores y originadores legítimos, la conservación de documentación sobre la identidad del cliente y la utilización de etiquetado para el tráfico verificable; y **SSC** propuso una excepción de «origen verificado», sustentada en la acreditación de la identidad del cliente, la asignación de la numeración y la autorización del titular para su uso.

Por su parte, **CLARO** y **SSC** formularon observaciones específicas respecto de la excepción prevista para el roaming internacional. Ambos señalaron que el operador propietario de la numeración es quien dispone de la información necesaria para conocer el estado de movilidad de sus propios abonados y que un operador de larga distancia internacional o un PRSTM distinto no puede determinar, de manera general, si un número perteneciente a otra red se encuentra efectivamente en roaming. **ETB** y **TIGO**, a su vez, cuestionaron la distribución de las obligaciones en la cadena de transporte de la llamada y

sostuvieron que una parte relevante de la capacidad para identificar anomalías se encuentra en los originadores y carriers internacionales.

En contraste, **SAEM** consideró razonable concentrar los esfuerzos en el bloqueo del tráfico internacional entrante con CLI nacional falsificado, aunque solicitó diferenciar dicho escenario del uso legítimo de un CLI corporativo de retorno y propuso que la calibración de los mecanismos de monitoreo se adelante en el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles (CTLFSM). Finalmente, **PTC** solicitó precisar operativamente los formatos de numeración pertenecientes al PNN colombiano que deben ser objeto de bloqueo en las rutas de larga distancia internacional.

Frente a estos comentarios, la Comisión considera necesario precisar, en primer lugar, que la medida propuesta no se fundamenta en la premisa de que toda llamada internacional sea fraudulenta ni tiene como propósito restringir la utilización de plataformas tecnológicas, infraestructura en la nube o centros de contacto ubicados fuera del territorio nacional. El supuesto objeto de la disposición es específico y se circunscribe a las llamadas que ingresan al país a través de una ruta internacional y presentan como identificador de línea llamante un número perteneciente al Plan Nacional de Numeración colombiano (PNN), salvo el tráfico de roaming internacional debidamente identificado.

Sumado a lo anterior, la Comisión considera necesario señalar que el fundamento técnico de la medida objeto de análisis no radica en cuestionar la legitimidad de los modelos tecnológicos utilizados para originar o cursar comunicaciones desde infraestructura internacional, sino en la inexistencia, en el estado actual del ecosistema internacional de telecomunicaciones, de mecanismos técnicos interoperables que permitan a la red receptora verificar objetivamente que un identificador de línea llamante (CLI) perteneciente al Plan Nacional de Numeración Colombiano, presentado mediante una ruta internacional, corresponde efectivamente a un actor autorizado y que dicho identificador preservó su integridad durante toda la cadena de señalización. En consecuencia, el objeto de la medida no consiste en autenticar la identidad del originador de las llamadas internacionales, sino en establecer una regla objetiva de tratamiento para un escenario en el cual dicha autenticidad no puede ser verificada de manera general, automática e interoperable por las redes receptoras.

A partir de la anterior precisión, la Comisión considera necesario diferenciar dos aspectos técnicamente distintos que de manera permanente se traerán a consideración, (i) la legitimidad de la infraestructura utilizada para originar o cursar una llamada y (ii) la posibilidad de verificar objetivamente la autenticidad del identificador de línea llamante presentado al usuario, ya que mientras el primero corresponde a una decisión tecnológica del originador, el segundo constituye el aspecto sobre el cual recae la medida regulatoria propuesta.

En este sentido, la Comisión comparte con **ASOBANCARIA**, **BYTECOL** y **SSC** que la utilización de infraestructura tecnológica internacional puede corresponder a modelos empresariales legítimos y que la ubicación física de una plataforma no permite, por sí sola, calificar una llamada como fraudulenta. No obstante, esta consideración no desvirtúa la medida, pues resulta necesario distinguir entre la

infraestructura utilizada para soportar o cursar una comunicación y la identidad numérica que se presenta al usuario receptor.

La discusión regulatoria no recae sobre la ubicación de los servidores, plataformas CPaaS o centros de contacto utilizados por una empresa. El aspecto técnicamente relevante es la presentación, mediante una ruta internacional, de un identificador perteneciente al PNN colombiano y la posibilidad de determinar que el actor que utiliza dicho número como CLI se encuentra efectivamente autorizado para presentarlo en una llamada específica.

Al respecto, es importante recordar que, de conformidad con el Decreto 25 de 2002, compilado en el Decreto 1078 de 2015, la CRC es el Administrador del Plan Nacional de Numeración. Asimismo, el artículo 2.2.12.1.2.5 del Decreto 1078 de 2015 establece que los números, bloques de numeración, códigos y prefijos son recursos públicos pertenecientes al Estado, los cuales pueden ser asignados a los proveedores de redes y servicios de telecomunicaciones bajo las condiciones definidas en el ordenamiento aplicable. En consecuencia, la asignación de numeración no confiere un derecho de propiedad sobre el recurso ni lo convierte en un activo de libre disposición de los particulares.

Para la prestación de servicios de voz, la numeración E.164 constituye el recurso público estructurado conforme al estándar internacional definido por la UIT, cuya finalidad primordial es proveer el recurso numérico necesario para identificar y permitir el acceso unívoco a los usuarios y servicios correspondientes. En Colombia, la numeración E.164 se clasifica en geográfica y no geográfica; dentro de esta última se encuentran la numeración de redes y la numeración de servicios.

La numeración geográfica tiene como propósito soportar la prestación de servicios asociada con regiones geográficas específicas. En consecuencia, una numeración geográfica colombiana no pierde su naturaleza ni la finalidad asociada a su asignación dentro del PNN por el hecho de que una empresa decida utilizar una infraestructura tecnológica ubicada en el exterior para gestionar sus comunicaciones.

Por esta razón, frente a los planteamientos de **BYTECOL** y **SSC** sobre la migración de las comunicaciones empresariales hacia plataformas globales, la Comisión precisa que el traslado de la infraestructura tecnológica utilizada para cursar una llamada no modifica, por sí mismo, las características ni las condiciones regulatorias del recurso de numeración presentado al usuario.

De igual forma, la numeración móvil corresponde a numeración E.164 no geográfica de redes. Su carácter no geográfico implica que la numeración no se encuentra asociada a una región territorial específica dentro de Colombia, pero no significa que pierda su naturaleza de numeración nacional ni que exista una autorización general para presentarla como identidad llamante desde cualquier red, plataforma o carrier internacional.

En otros términos, la Comisión no comparte una interpretación según la cual el carácter no geográfico de la numeración móvil equivalga a una portabilidad global del identificador de originación. La ausencia de vinculación de un número móvil con Bogotá, Medellín, Cali o cualquier otra región específica no

implica que dicho número pueda ser inyectado como CLI desde cualquier punto de la cadena internacional y que las redes nacionales deban presumir que el actor que lo presenta se encuentra autorizado para utilizarlo.

La finalidad de la numeración móvil continúa siendo proveer el recurso numérico nacional significativo necesario para identificar y permitir el acceso unívoco al usuario dentro de la estructura de numeración y de las redes correspondientes. En consecuencia, debe diferenciarse entre el carácter no geográfico de la numeración móvil y la autenticidad del uso de dicha numeración como identificador de la parte llamante.

Tampoco resulta equiparable este escenario con la portabilidad numérica móvil, como sugiere **SSC** al referirse a la separación entre numeración y red. Dentro del entorno nacional existe una base de datos centralizada de números portados que soporta los procedimientos de enrutamiento y permite conocer la red asociada a una numeración para los efectos correspondientes. La portabilidad modifica la red en la que el usuario recibe el servicio, pero no supone que la utilización del número quede desvinculada de los mecanismos nacionales establecidos para su tratamiento y enrutamiento.

Por el contrario, cuando una llamada ingresa mediante una cadena internacional presentando un número colombiano, el PRST receptor puede recibir el valor correspondiente al CLI sin disponer de un elemento técnico que permita establecer que el actor que presenta el número es aquel autorizado para utilizarlo o que dicho identificador preservó su integridad durante los diferentes segmentos de la cadena internacional.

Adicionalmente, el régimen de administración de los recursos de identificación establece que estos no pueden ser vendidos o comercializados, ni cedidos o transferidos sin autorización previa y expresa de la CRC, y que deben utilizarse en la forma y aplicación específica para la cual fueron asignados.

Ahora bien, frente al argumento de **SSC** según el cual la autorización otorgada por el titular de una numeración a una plataforma internacional no constituye una cesión o transferencia del recurso, la Comisión considera que, aun aceptando para efectos del análisis o en gracia de discusión que en un caso particular no se configure jurídicamente una cesión o transferencia, ello no resuelve el problema técnico objeto de la medida.

Una autorización contractual otorgada por una empresa a una plataforma CPaaS, un proveedor de telefonía IP o un centro de contacto constituye una relación jurídica entre particulares. Dicha autorización, sin embargo, no se incorpora automáticamente a la señalización de la llamada ni se transforma en una credencial técnica interoperable que pueda ser verificada por todos los PRST que intervienen en la terminación de la comunicación.

Debe distinguirse, por tanto, entre estar autorizado contractualmente para realizar comunicaciones en nombre de una empresa y poder acreditar técnicamente, durante el establecimiento de una llamada

específica, que el CLI presentado corresponde efectivamente al número autorizado y que no fue alterado en un eslabón previo de la cadena internacional.

La primera circunstancia puede ser acreditada mediante contratos, mandatos o documentos comerciales. La segunda requiere mecanismos técnicos que permitan vincular la autorización con la comunicación concreta, verificarla por la red receptora y preservar la integridad de dicha información a lo largo de la cadena de señalización.

Por ello, la Comisión no comparte las propuestas de **ANDESCO**, **BYTECOL** y **SSC** orientadas a considerar un registro documental de originadores como una excepción suficiente al bloqueo.

La verificación de la identidad de un cliente, la asignación de determinada numeración y la existencia de una autorización para su uso pueden constituir mecanismos de conocimiento del originador. Sin embargo, no garantizan, por sí mismos, la autenticidad de cada llamada ni la integridad del CLI durante su transporte.

Así, ante dos llamadas internacionales que presentan exactamente el mismo número colombiano, una efectuada por la plataforma contratada por una empresa legítima y otra originada por un actor que suplanta dicho número, el PRST receptor continuará recibiendo el mismo valor de CLI. Si la condición de «origen verificado» propuesta por **ANDESCO**, **BYTECOL** y **SSC** no acompaña técnicamente a cada comunicación mediante un atributo autenticado, interoperable y verificable, el registro no permite determinar durante el establecimiento de la llamada cuál de las dos comunicaciones corresponde al originador previamente inscrito.

En consecuencia, la Comisión considera que la verificación ex ante de un originador y la autenticación técnica de una llamada son problemas diferentes. La primera permite conocer a un cliente. La segunda exige acreditar la identidad presentada en cada comunicación y preservar esa información a través de la cadena de transporte, y, es efectivamente sobre esta diferencia que se fundamenta la medida regulatoria propuesta, mientras la verificación documental permite identificar a un cliente o proveedor, la aplicación del numeral 2.1.10.7.2.2.1 responde a la imposibilidad de verificar, de manera objetiva e interoperable, la autenticidad del CLI presentado en una llamada específica que ingresa al país mediante una ruta internacional.

Precisamente, **ANDESCO** sostiene que actualmente no existen herramientas técnicas suficientes para distinguir entre un CLI legítimo y uno suplantado en el tráfico internacional; por su parte **SSC** reconoce que la señalización tradicional no permite distinguir de forma general y confiable entre una llamada legítima y una llamada suplantada cuando ambas ingresan del exterior presentando el mismo CLI nacional. **TIGO** también señala las limitaciones de las redes SS7/ISUP y la ausencia de una implementación general de STIR/SHAKEN que abarque las diferentes arquitecturas y rutas internacionales.

Para la Comisión, estas consideraciones no desvirtúan la medida propuesta. Por el contrario, confirman la existencia del riesgo técnico que se pretende mitigar.

El Calling Party Number constituye información transportada mediante los mecanismos de señalización empleados en el establecimiento de la comunicación. Sin embargo, el transporte de dicho parámetro no equivale a un mecanismo de autenticación de extremo a extremo que permita establecer que el actor que presenta la numeración se encuentra autorizado por el asignatario o usuario legítimo para utilizarla.

En este punto, la Comisión no comparte la conclusión de **SSC** según la cual la falta de trazabilidad y autenticación obliga a sustituir el bloqueo por un esquema documental de verificación. Precisamente, la imposibilidad de distinguir de manera general, automática y confiable entre una llamada legítima y una llamada suplantada cuando ambas ingresan mediante una ruta internacional presentando el mismo CLI colombiano impide construir una excepción objetiva basada únicamente en el identificador recibido.

La falta de autenticación no proporciona una base técnica suficiente para presumir la legitimidad del identificador cuya autenticidad precisamente no puede ser comprobada.

Por el contrario, mientras no exista un mecanismo interoperable que permita a la red receptora verificar que la numeración presentada fue utilizada por un actor autorizado y preservó su integridad durante la cadena internacional, no existe actualmente una base técnica objetiva para diferenciar, únicamente a partir del CLI recibido, el tráfico autorizado del tráfico suplantado.

Lo anterior no implica desconocer la propuesta de **ANDESCO** y **SSC** sobre el desarrollo de arquitecturas de attestation ni las consideraciones formuladas por **TIGO** respecto de STIR/SHAKEN. La Comisión reconoce la evolución de los mecanismos internacionales de autenticación del identificador de línea llamante y la posibilidad de evaluar su incorporación al marco regulatorio colombiano en el largo plazo.

No obstante, la implementación de estas arquitecturas exige definir condiciones de interoperabilidad, gobernanza, entidades de confianza, administración de certificados y tratamiento de redes o rutas internacionales que no preserven la información de autenticación. Por esta razón, la inexistencia actual de una arquitectura con despliegue generalizado e interoperabilidad internacional no obliga al regulador a mantener sin intervención un vector de fraude mientras se desarrolla una solución tecnológica futura.

En relación con el roaming internacional, **CLARO** sostiene que la identificación del tráfico correspondiente a líneas que se encuentran efectivamente en roaming solo puede ser realizada por la red home o por el PRST que administra al abonado, y señala que un carrier de origen u otro PRST nacional no puede determinar de manera general dicha circunstancia. **SSC** plantea un argumento similar y, a partir de ello, solicita que, de mantenerse la medida, la obligación de bloqueo recaiga sobre el operador propietario de la numeración.

La Comisión comparte parcialmente la precisión técnica realizada por **CLARO** y **SSC** en cuanto a la disponibilidad de la información de movilidad. Un PRSTM puede conocer el estado de registro y roaming

de sus propios abonados, en la medida en que administra el HLR, HSS o los elementos equivalentes de gestión de suscriptores y movilidad, o dispone de acceso legítimo a la información necesaria para la prestación del servicio.

En contraste, un PRSTM no puede determinar de manera general, automática y confiable si un número perteneciente a otro operador se encuentra en roaming, pues no dispone de acceso universal a la información de registro administrada por la red de origen del abonado. El conocimiento de dicha condición por un tercero dependería de los mecanismos de señalización, coordinación o intercambio de información habilitados para procedimientos específicos.

Por ello, la condición de roaming de un abonado perteneciente a una red distinta no constituye una información universalmente disponible para todos los PRSTM que intervienen en el encaminamiento de una llamada, ni puede inferirse de manera confiable a partir del CLI presentado. La información sobre el registro y localización del abonado es administrada principalmente por su operador de origen, a través de las funciones de movilidad y de las bases de datos de suscriptores de la red, y no se encuentra necesariamente disponible para un operador tercero encargado de recibir o terminar el tráfico internacional.

Sin embargo, la Comisión no comparte la conclusión planteada por **CLARO** y **SSC** según la cual esta limitación técnica desvirtúa la medida de bloqueo o implica que el tráfico deba cursarse siempre que el PRSTM encargado de aplicarla no pueda verificar directamente si el abonado se encuentra en roaming.

Aceptar esta interpretación supondría que toda llamada internacional entrante que presente como CLI un número móvil colombiano tendría que ser cursada ante la sola imposibilidad del PRSTM receptor de consultar o validar el estado de movilidad del abonado, es decir sin bloqueo. En la práctica, ello trasladaría a la medida de bloqueo una exigencia de verificación que no siempre puede ser satisfecha por el actor que recibe el tráfico y convertiría la excepción de la medida, a saber, el no bloqueo de llamadas en roaming, en la regla general; es decir, ante la duda de si se trata de un número en roaming, el PRST debe permitir la comunicación a pesar de que pueda ser un número con enmascaramiento que simula roaming.

Bajo ese entendimiento, bastaría con que no pudiera descartarse de manera absoluta la posibilidad de que el número presentado correspondiera a un usuario registrado en una red visitada para permitir el curso de la llamada. Esto reduciría de manera sustancial la efectividad de la medida, pues el tráfico que se busca mitigar podría continuar ingresando con CLI móvil colombiano amparado en una hipótesis meramente eventual de roaming, aun cuando no exista información técnica que permita acreditar dicha condición.

En consecuencia, la imposibilidad de un PRSTM de verificar directamente el estado de roaming de abonados pertenecientes a otras redes no puede traducirse en una autorización automática del tráfico. La excepción debe sustentarse en mecanismos técnicos y operativos que permitan identificar o validar de manera suficiente la condición legítima de roaming, sin que la sola presentación de un CLI móvil

colombiano ni la imposibilidad de descartar una ubicación en una red visitada sean elementos suficientes para inaplicar la medida de bloqueo.

La excepción prevista en el proyecto se refiere al tráfico de roaming internacional debidamente identificado como tal. Ahora bien, la observación formulada por **CLARO** y reiterada por **SSC** evidencia que la forma técnica y operativa de identificar, transmitir y validar dicha condición a través de los distintos actores de la cadena requiere un análisis específico, particularmente cuando el PRST que debe ejecutar la medida no es aquel que administra la información de movilidad del abonado.

Por esta razón, la Comisión considera que la identificación, validación y tratamiento operativo del tráfico correspondiente a usuarios en roaming internacional será objeto prioritario de análisis en el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles —CTLFSM—.

En dicho Comité deberá estudiarse la alternativa técnica y operativa más adecuada para hacer efectiva la excepción de roaming prevista en la regulación, considerando las diferentes arquitecturas de red, la información disponible para los PRSTM que administran a los abonados, las capacidades de los operadores de larga distancia internacional y demás actores que intervienen en el transporte de las llamadas, así como los mecanismos mediante los cuales la condición de roaming pueda ser identificada y validada por el actor encargado de aplicar la medida.

En este sentido, las observaciones de **CLARO** y **SSC** serán consideradas como un insumo técnico para el análisis que se adelante en el CTLFSM, cuyo propósito deberá ser determinar e implementar el mecanismo que permita preservar la efectividad del bloqueo frente a la utilización fraudulenta de numeración colombiana y, simultáneamente, generar los menores impactos posibles sobre los usuarios que legítimamente utilizan el servicio de roaming internacional.

El análisis que se adelante en el CTLFSM no supone el intercambio generalizado de bases individualizadas o listas de usuarios en roaming entre los participantes. El proyecto dispone que en dicho Comité no se compartirá información que contenga datos personales de los usuarios. Por tanto, el objeto de estudio deberá centrarse en la definición de procedimientos, responsabilidades, mecanismos de identificación, información técnica susceptible de ser utilizada y alternativas interoperables que permitan reconocer el tráfico sujeto a la excepción.

Los participantes del CTLFSM podrán proponer y recomendar a la CRC mejoras en la implementación de las medidas mínimas, la Comisión podrá requerir información relacionada con los asuntos objeto de análisis y podrán conformarse mesas de trabajo para el estudio de aspectos específicos. Conforme al numeral 2.1.10.7.3.4, tales recomendaciones no vinculan a la CRC ni a los agentes, y solo adquieren exigibilidad cuando la Comisión las acoge mediante la resolución correspondiente.

De esta manera, la respuesta a la dificultad técnica señalada por **CLARO** y **SSC** no consiste en eliminar el bloqueo debido a que todos los PRSTM no pueden consultar la información de movilidad de los abonados de terceros. Consiste en estudiar e implementar, en el marco del CTLFSM, el mecanismo

técnico y operativo más adecuado para materializar la excepción ya prevista en la regulación, buscando generar los menores impactos posibles sobre los usuarios legítimos.

Por otra parte, **ASOBANCARIA** solicita establecer un tratamiento específico para las comunicaciones de las entidades vigiladas por la Superintendencia Financiera de Colombia, particularmente para alertas transaccionales, mensajes de seguridad y procedimientos de autenticación. **BYTECOL**, en un sentido similar, solicita excluir las actividades de cobranza, autenticación, prevención del fraude, atención contractual y comunicaciones transaccionales o de servicio de las medidas de bloqueo. **SAEM** también advierte que las campañas legítimas de notificación o cobranza pueden utilizar identificadores corporativos de retorno.

Al respecto, la Comisión reconoce la importancia de las comunicaciones relacionadas con la prevención del fraude, la seguridad de las transacciones, la atención al cliente y las gestiones de cobranza legítimas. No obstante, la naturaleza económica del originador o la finalidad declarada de una llamada no modifican las características técnicas del CLI presentado ni proporcionan a la red receptora un elemento que permita verificar su autenticidad.

Desde la perspectiva de la señalización, una llamada no incorpora un atributo técnicamente autenticado que permita establecer que corresponde a una «alerta financiera legítima», una «cobranza autorizada» o una «comunicación transaccional». La finalidad económica o funcional de la llamada no constituye, por sí misma, una propiedad verificable del identificador de línea llamante.

Más aún, las mismas finalidades señaladas por **ASOBANCARIA** y **BYTECOL** pueden ser simuladas por los actores fraudulentos. Una llamada de vishing puede presentarse precisamente como una alerta de fraude, un procedimiento de autenticación bancaria, una comunicación relacionada con una transacción sospechosa o una gestión de cobranza y utilizar como elemento para generar confianza el número legítimo de la entidad suplantada.

En consecuencia, la Comisión no considera procedente establecer excepciones generales basadas exclusivamente en el sector económico del supuesto originador o en la finalidad declarada de la comunicación. Una excepción de esta naturaleza crearía un mecanismo de evasión de la medida sin solucionar la imposibilidad técnica de verificar la autenticidad del CLI.

En particular, frente a **ASOBANCARIA**, la Comisión considera que la criticidad de las comunicaciones financieras no constituye una razón para aceptar un identificador cuya legitimidad no puede ser comprobada. Por el contrario, precisamente la relevancia de las comunicaciones asociadas con autenticación y prevención del fraude refuerza la necesidad de impedir que un actor fraudulento pueda presentarse ante el usuario utilizando el mismo número de la entidad financiera que pretende suplantar.

En cuanto a **SAEM**, la Comisión precisa que la medida objeto de estos comentarios corresponde específicamente al tratamiento del tráfico internacional que presenta numeración perteneciente al PNN colombiano. Por tanto, el análisis sobre la utilización legítima de un CLI corporativo de retorno deberá

considerar la ruta mediante la cual se cursa la comunicación y las condiciones aplicables al recurso de numeración utilizado. La utilización de un número corporativo legítimamente asignado no constituye, por esa sola circunstancia, una conducta fraudulenta; sin embargo, su presentación a través de una ruta internacional continúa sujeta al problema de verificabilidad analizado anteriormente.

Respecto de las propuestas de **ANDESCO**, **BYTECOL** y **SSC** de sustituir el bloqueo por mecanismos de etiquetado, la Comisión considera que ambas herramientas atienden escenarios técnicamente diferentes.

El etiquetado resulta adecuado cuando los sistemas de monitoreo identifican patrones o comportamientos indicativos de una posible actividad fraudulenta. En estos escenarios existe una sospecha derivada del volumen de llamadas, su duración, frecuencia u otros parámetros y patrones analizados. Precisamente por ello el proyecto contempla la presentación de una alerta al usuario.

El supuesto de una llamada internacional que presenta numeración colombiana es diferente. En este caso, el riesgo se encuentra directamente relacionado con la presentación de una identidad numérica nacional cuya legitimidad no puede ser verificada mediante la ruta internacional.

Por esta razón, la Comisión no comparte el argumento de **SSC** según el cual el etiquetado constituye necesariamente un medio igualmente eficaz por el hecho de ser menos restrictivo. Permitir la terminación de la llamada y limitar la intervención a una advertencia mantendría disponible el contacto potencialmente fraudulento y trasladaría al usuario la decisión de determinar si debe confiar en un número que puede coincidir exactamente con el de su entidad financiera, aseguradora o proveedor de servicios.

La existencia de una alternativa menos restrictiva no determina por sí sola la improcedencia de la medida seleccionada. Para ello sería necesario acreditar que dicha alternativa ofrece un nivel equivalente de efectividad frente al riesgo específicamente identificado, condición que no se deriva de los comentarios formulados.

En relación con el cuestionamiento de proporcionalidad presentado principalmente por **SSC** y, en términos generales, por **ANDESCO** y **BYTECOL**, la Comisión tampoco comparte que la medida carezca de idoneidad porque un defraudador pueda utilizar numeración extranjera o migrar hacia canales OTT.

La finalidad de la medida no consiste en eliminar mediante una única obligación todas las modalidades presentes y futuras de fraude telefónico. El vector específicamente identificado consiste en la presentación, mediante rutas internacionales, de numeración perteneciente al PNN colombiano con la capacidad de generar frente al usuario una apariencia de identidad nacional cuya autenticidad no puede ser comprobada por la red receptora.

El bloqueo impide precisamente la utilización de este mecanismo.

Que un actor fraudulento pueda modificar posteriormente su conducta, utilizar un número extranjero o recurrir a otro canal no implica que mantenga la misma capacidad de presentarse ante el usuario mediante el número colombiano de la entidad o persona que pretende suplantar. La eventual adaptación del defraudador corresponde a un vector diferente que debe ser analizado y atendido mediante medidas complementarias.

En este punto, la Comisión coincide parcialmente con **SAEM** en que los puntos de ingreso del tráfico internacional que presenta CLI nacional constituyen un escenario relevante de intervención. La medida propuesta actúa precisamente en dicho punto, al impedir que una numeración colombiana no verificable continúe siendo presentada como identidad llamante al usuario.

Asimismo, la medida no opera aisladamente. El proyecto incorpora mecanismos de monitoreo, etiquetado de llamadas sospechosas, listas de no originación e intercambio de alertas, y crea el CTLFSM como instancia permanente de coordinación técnica frente a la evolución de los patrones de fraude.

En cuanto a las observaciones de **ETB**, **ANDESCO** y **TIGO** sobre la distribución de las obligaciones a lo largo de la cadena internacional, la Comisión reconoce que el origen de una alteración del CLI puede encontrarse en segmentos previos y que el PRST nacional que recibe o termina una llamada no necesariamente dispone de control sobre todos los originadores, carriers o intermediarios que participaron en su transporte.

Sin embargo, esta consideración exige diferenciar dos asuntos. El primero corresponde a la identificación del actor que alteró el CLI y a la eventual atribución de responsabilidad por dicha conducta. El segundo consiste en determinar si una llamada que presenta al usuario una identidad numérica nacional no verificable debe ser terminada.

La dificultad para identificar ex post al carrier u originador que modificó el CLI no implica que la red deba permitir la presentación del identificador al usuario. La imposibilidad de controlar integralmente todos los eslabones anteriores de la cadena no elimina la capacidad de adoptar una medida preventiva respecto del tráfico que ingresa al país bajo la condición objetiva definida en la regulación.

En este contexto, los planteamientos de **ETB** y **TIGO** respecto de las capacidades de los carriers internacionales y originadores constituyen elementos relevantes para continuar analizando los mecanismos de trazabilidad, cooperación e intercambio de información en el CTLFSM. Sin embargo, no desvirtúan la necesidad de impedir que un CLI nacional cuya autenticidad no puede comprobarse sea presentado al usuario mediante una ruta internacional.

La Comisión tampoco comparte los argumentos de **SSC** relacionados con una supuesta vulneración del principio de neutralidad de red. La medida no regula el acceso de los usuarios a contenidos, aplicaciones o servicios a través de Internet ni establece mecanismos de gestión de tráfico de datos basados en la fuente, propiedad o naturaleza del contenido. La disposición regula el tratamiento del identificador de

línea llamante en comunicaciones de voz y la presentación de recursos pertenecientes al Plan Nacional de Numeración.

Asimismo, el análisis costo-beneficio y de sensibilidad contenido en el Documento Soporte comparó la prohibición del enmascaramiento del CLI con la alternativa de etiquetado. Los resultados muestran que la medida de bloqueo presenta una mayor relación beneficio-costo en todos los escenarios evaluados y conserva un desempeño superior incluso bajo supuestos conservadores de efectividad. Por tanto, no existe sustento para concluir que el etiquetado constituya una alternativa igualmente eficaz frente al riesgo específicamente analizado.

Del mismo modo, el derecho del usuario a recibir información no implica que las redes deban presentar como identidad nacional confiable un identificador cuya legitimidad no puede ser verificada. Por el contrario, la protección de los usuarios y la preservación de la confianza en los servicios de comunicaciones justifican la adopción de medidas dirigidas a impedir que los recursos de numeración nacional sean utilizados para generar una apariencia de identidad susceptible de facilitar escenarios de suplantación.

Ahora bien, sobre el argumento de **SSC** según el cual la remuneración por terminación ya se encuentra garantizada mediante cargos de acceso no desvirtúa la medida, dado que la intervención regulatoria responde a una finalidad distinta: mitigar una modalidad específica de fraude asociada a la utilización de numeración colombiana como elemento de confianza frente al usuario.

La eventual decisión de determinados originadores de modificar sus canales de contacto constituye una posible reacción de los agentes frente a las condiciones aplicables al uso de la numeración y a la presentación del CLI, pero no demuestra que la medida introduzca un tratamiento discriminatorio entre operadores o modelos empresariales.

La obligación se activa a partir de una condición objetiva del tráfico: el ingreso de una llamada mediante una ruta internacional presentando numeración perteneciente al PNN colombiano, salvo los escenarios exceptuados. La regla no depende de la identidad del proveedor de larga distancia internacional, de su condición de operador integrado o independiente ni del sector económico del presunto originador.

Finalmente, en relación con la solicitud de **PTC** de incorporar expresamente en la disposición los diferentes formatos en que puede presentarse la numeración colombiana en las rutas LDI, la Comisión considera relevante distinguir entre el alcance sustancial de la obligación y los aspectos técnicos requeridos para su implementación. La referencia al Plan Nacional de Numeración permite delimitar el conjunto de recursos objeto de la medida con independencia de las distintas representaciones o formatos que puedan observarse en la señalización. Sin perjuicio de ello, los aspectos operativos asociados con la normalización y reconocimiento de los formatos de numeración podrán ser analizados en los espacios técnicos de seguimiento de la implementación (CTLFSM), con el fin de asegurar una aplicación homogénea de la medida.

Por las razones expuestas, la Comisión no acoge las solicitudes de **ASOBANCARIA** y **BYTECOL** dirigidas a establecer excepciones generales para comunicaciones financieras, de autenticación, cobranza, prevención del fraude, atención al cliente o carácter transaccional, toda vez que la finalidad de la comunicación no constituye un atributo técnico que permita autenticar el CLI presentado y puede ser igualmente simulada en escenarios de suplantación.

La Comisión tampoco acoge las propuestas de **ANDESCO**, **BYTECOL** y **SSC** orientadas a sustituir el bloqueo por un registro exclusivamente documental de originadores, una excepción general de «origen verificado» o un mecanismo de etiquetado, dado que la verificación ex ante de un cliente no garantiza la autenticidad de cada comunicación ni permite determinar que el CLI recibido preservó su integridad a lo largo de la cadena internacional.

Frente a los comentarios de **CLARO** y **SSC** respecto del roaming internacional, la Comisión reconoce que un PRSTM dispone de información sobre el estado de movilidad de sus propios abonados y que dicha información no se encuentra disponible de manera general y automática para los demás operadores respecto de usuarios pertenecientes a terceros. No obstante, esta circunstancia no permite presumir que toda llamada internacional con numeración móvil colombiana corresponde a un abonado en roaming ni desvirtúa la medida de bloqueo.

La identificación, validación y tratamiento operativo del tráfico correspondiente a usuarios en roaming internacional será objeto prioritario de estudio en el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles —CTLFSM—, con el propósito de analizar e implementar el mecanismo técnico y operativo más adecuado para hacer efectiva la excepción prevista en la regulación y generar los menores impactos posibles sobre los usuarios que legítimamente utilizan el servicio de roaming internacional.

A partir de lo anterior, y en coherencia con la naturaleza no vinculante de las decisiones del Comité precisada en el numeral 2.1.10.7.3.4, la Comisión ajustará el numeral 2.1.10.7.2.2.4 para disponer que la implementación de la medida de bloqueo prevista en el numeral 2.1.10.7.2.2.1 será exigible a partir del vencimiento de los tres (3) meses siguientes a la entrada en vigencia de la resolución mediante la cual la CRC acoja la recomendación técnica del CTLFSM sobre los aspectos técnicos y operativos necesarios para la identificación, validación y tratamiento del tráfico correspondiente a usuarios en roaming internacional.

La Comisión precisa que el hito de exigibilidad no puede anclarse en la sola celebración de la sesión del Comité ni en el acta que de ella resulte. Como se expone en el capítulo denominado «Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM», las decisiones del Comité tienen en todos los casos el carácter de recomendaciones técnicas dirigidas a sus miembros y a la CRC y no son fuente de obligaciones para los agentes. En consecuencia, la certeza sobre el momento a partir del cual la medida resulta exigible, y sobre el contenido técnico y operativo con arreglo al cual debe implementarse, solo puede derivar del acto administrativo mediante el cual la Comisión resuelva acoger vía regulación una determinada recomendación. Este diseño atiende, además, la observación de **ETB**

según la cual el Comité no puede constituir un mecanismo para introducir obligaciones regulatorias por fuera del procedimiento correspondiente, y otorga a los agentes obligados un plazo cierto de tres (3) meses contados desde un acto administrativo publicado y no desde un acta.

La revisión de los aspectos técnicos y operativos necesarios para la identificación, validación y tratamiento del tráfico correspondiente a usuarios en roaming internacional tendrá carácter prioritario en la agenda del Comité. Para tal efecto, y conforme al numeral 2.1.10.7.3.3, la CRC convocará la sesión correspondiente en ejercicio de la facultad de determinar la temática de cada sesión, citando con voz y voto a los PRST obligados al cumplimiento de la medida.

En dicho espacio se analizarán las capacidades de los diferentes actores de la cadena, la información disponible para los PRSTM que administran la movilidad de los abonados, los mecanismos para identificar y validar técnicamente la condición de roaming y la forma en que dicha condición pueda ser reconocida por el actor encargado de aplicar la medida. Este análisis deberá observar las disposiciones aplicables en materia de protección de datos personales y no supondrá el intercambio general de bases individualizadas de usuarios en roaming.

Las observaciones de **ETB** y **TIGO** respecto de la participación de los carriers internacionales y la distribución de las actividades entre los distintos actores de la cadena serán igualmente consideradas en el CTLFSM para efectos de analizar mejoras en los mecanismos de trazabilidad, intercambio de alertas y cooperación operativa. Asimismo, las consideraciones de **SAEM** sobre la calibración de los mecanismos de detección y los aspectos técnicos de implementación señalados por **PTC** podrán ser abordadas en los espacios técnicos previstos en el proyecto (CTLFSM).

Los resultados del análisis desarrollado en el CTLFSM permitirán identificar y recomendar mejoras técnicas y operativas en la implementación de las medidas y constituirán insumo técnico, no vinculante, para la evaluación correspondiente por parte de la CRC, la cual, cuando evidencie la necesidad de una adaptación regulatoria, la incorporará mediante el acto administrativo que corresponda.

En consecuencia, la Comisión mantiene la medida de bloqueo de las llamadas internacionales entrantes que presenten como identificador de línea llamante un número perteneciente al Plan Nacional de Numeración colombiano, al considerar que, en el estado actual del ecosistema internacional de telecomunicaciones, las redes receptoras no disponen de mecanismos técnicos generales, interoperables y objetivamente verificables que permitan autenticar la legitimidad del CLI perteneciente al Plan Nacional de Numeración colombiano cuando este es presentado mediante una ruta internacional, bajo estas condiciones, la medida establece una regla objetiva de tratamiento frente a un escenario en el que la autenticidad del identificador no puede ser comprobada de manera general.

La utilización de infraestructura internacional, plataformas CPaaS, SIP Trunks, soluciones de telefonía IP o centros de contacto ubicados en el exterior no constituye, por sí misma, una actividad fraudulenta. Sin embargo, dicha circunstancia tampoco autentica el CLI colombiano presentado en una llamada específica ni proporciona a la red receptora un mecanismo interoperable para establecer que el

identificador fue utilizado por un actor autorizado y preservó su integridad durante la cadena internacional de transporte.

La Comisión continuará realizando seguimiento a la implementación de la medida en el marco del CTLFSM, con especial atención a la correcta aplicación de la excepción de roaming internacional, a la identificación de posibles impactos sobre comunicaciones legítimas y a la evolución de los mecanismos de autenticación de identidad de línea llamante. Lo anterior, con el propósito de preservar la protección de los usuarios frente al fraude y, simultáneamente, implementar las soluciones técnicas que permitan generar los menores impactos posibles sobre quienes utilizan legítimamente los servicios de comunicaciones.

3.2 Monitoreo de llamadas que derivan en la etiqueta de «Alerta de llamada sospechosa»

ANDESCO

Indica que el artículo 3 de la norma obliga a los PRST a etiquetar llamadas sospechosas con la indicación 'Alerta de llamada sospechosa' visible en el dispositivo del usuario receptor.

Advierte que esta función no es implementable en todos los segmentos de la red colombiana. El etiquetado de llamadas visible en el terminal del usuario requiere: (i) soporte de la red en el nivel de señalización (4G/VoLTE o 5G); (ii) soporte del sistema operativo del terminal (Android/iOS con versión reciente); (iii) APIs del fabricante del terminal que permitan mostrar metadatos de la llamada en la pantalla de identificación.

Dice que las redes 2G y 3G no soportan esta funcionalidad de señalización. En Colombia, una proporción significativa de usuarios aún opera en redes 2G/3G (especialmente en zonas rurales y población de menores ingresos). Para esos usuarios, el etiquetado es técnicamente imposible independientemente de lo que haga el operador. La responsabilidad de mostrar la etiqueta recae sobre el sistema operativo del terminal y el fabricante, no sobre el PRST, quien solo puede enviar la señalización. Si el teléfono no la interpreta, la etiqueta no se muestra.

Afirma que imponer una obligación cuyo cumplimiento depende de terceros no regulados genera inseguridad jurídica para los PRST, quienes quedarían expuestos a sanciones por incumplimiento de una obligación que no está bajo su control completo. A esto se suma que el costo de implementar sistemas de señalización de etiquetado de llamadas en infraestructura 4G/VoLTE es significativo y no fue cuantificado en el AIN. Para las redes 2G/3G, el costo es prácticamente ilimitado (requeriría migración completa a 4G, que es un proceso de varios años).

COLOMBIA FINTECH

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Expresa que el artículo 2.1.10.7.2.2.2. exige que los PRST implementen sistemas de monitoreo en tiempo real del tráfico de voz con capacidad de detectar cuatro tipos de patrones (volumen inusual, robocall, correlación con listas de numeración fraudulenta y enmascaramiento de numeración). Sin embargo, no establece ningún parámetro de calidad mínima del sistema de monitoreo, ni exige que este sea distinto o independiente del sistema de monitoreo P2P. Se sugiere que la CRC precise que:

1. El sistema de monitoreo de voz y el de P2P deben poder intercambiar señales de alerta, dado que los fraudes modernos son frecuentemente multicanal (combinan SMS y voz en una misma campaña fraudulenta). La correlación cruzada entre eventos detectados en ambos canales es una capacidad crítica para la identificación de campañas de fraude sofisticadas.

2. El sistema de monitoreo de voz debe tener capacidad de actualización dinámica de los patrones de detección, de modo que pueda incorporar nuevas firmas de fraude identificadas a través del CTLFSM sin necesidad de reemplazar la solución tecnológica completa. Esto favorece la adopción de soluciones SaaS de prevención de fraude, que por su naturaleza de actualización continua son más eficientes que las soluciones on-premise con ciclos de actualización largos.

Con respecto a los criterios técnicos de detección de patrones de robocall (duración promedio de llamada (ACD) baja y patrones de llamadas cortas y secuenciales) señala que son inherentes a operaciones legítimas de cobranza asistida por agentes virtuales (AI) y a campañas de gestión de cartera vencida de entidades financieras. Las llamadas a deudores en mora tienen ACD estructuralmente más bajo (el cliente cuelga, no contesta o la conversación es breve) y se realizan en secuencias. El numeral 2.1.10.7.2.2.2.2.4 establece adicionalmente que el etiquetado se mantiene activo durante el procedimiento de revisión, lo que impide reversar el daño operativo aun cuando la solicitud sea procedente. El efecto neto es que llamadas legítimas de entidades financieras quedan marcadas como sospechosas en el dispositivo del receptor, deteriorando la tasa de contacto y el cumplimiento del deber de gestión de cobro.

Para este punto, solicita a la CRC modificar el artículo 2.1.10.7.2.2 para excluir explícitamente del criterio de patrón sospechoso las llamadas originadas desde numeración inscrita en el portal del artículo 6.14.3.1 (sector financiero), o subsidiariamente, que el parágrafo del numeral 2.1.10.7.2.2.2.2.4 se modifique para suspender el etiquetado durante la tramitación de la revisión cuando el solicitante sea una entidad vigilada por la SFC y acredite la legitimidad del uso.

INETUM

Solicita que se aclare si la detección de patrones anómalos en tráfico de voz no implicará acciones de bloqueo sobre las líneas afectadas o bloqueo de terminales afectados.

JULIO NULDEMAR

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Expone que el proyecto impone obligaciones simétricas y uniformes de monitoreo, detección de señalización anómala y ejecución de bloqueos instantáneos en la infraestructura core de red a todos los operadores por igual.

Señala que, de acuerdo con la Ley 1341 de 2009 y la jurisprudencia constitucional, la regulación sectorial debe respetar el principio de proporcionalidad y razonabilidad. Los OMV se caracterizan por una condición técnica de subordinación operativa específica: carecen de elementos de red centrales (Core Network) y dependen contractualmente de la infraestructura del Operador Móvil de Red (PRM) anfitrión.

De otra parte, señala que un OMV no posee el control físico ni lógico sobre las capas de señalización profunda necesarias para interceptar, filtrar o detener de forma autónoma el tráfico. Imponerle obligaciones directas de bloqueo sobre infraestructura ajena configura un acto administrativo con objeto imposible, violando el principio general del derecho según el cual a nadie se le puede obligar a lo imposible, lo que vicia la legalidad de la resolución.

Concluye que debe incluirse un artículo en la norma exclusivamente para los agentes que ostentan el control físico y lógico del Core de Red, y propone el siguiente texto «**ARTÍCULO NUEVO. ENFOQUE DIFERENCIADO POR ROL DE RED.** Las obligaciones técnicas referidas al monitoreo de sistemas de señalización, control de originación de comunicaciones en capas profundas y ejecución material de bloqueos de tráfico forzoso establecidos en esta resolución, serán exigibles única y exclusivamente a los PRST que ostenten el control físico, lógico y la titularidad de la infraestructura central de red (Core Network y elementos de acceso). Los Operadores Móviles Virtuales (OMV) quedarán eximidos de responsabilidad administrativa frente a fallas técnicas de filtrado que dependan de la infraestructura del operador anfitrión».

SEGUROS BOLÍVAR

Considera que un etiquetado exclusivamente automatizado puede generar riesgos cuando el algoritmo clasifique de manera errónea una línea corporativa legítima como sospechosa. Si bien el proyecto de resolución prevé la posibilidad de solicitar una revisión, cuyo trámite podría tardar hasta diez (10) días hábiles, durante ese tiempo podría producirse un perjuicio derivado del etiquetado incorrecto. Por ello, propone que la etiqueta de «llamada sospechosa» sea suspendida mientras se adelanta el proceso de revisión.

SUMA

Considera que, aunque comparte el objetivo de fortalecer la detección temprana de fraude mediante sistemas de monitoreo en tiempo real, la obligación propuesta presenta inquietudes de precisión técnica, proporcionalidad y viabilidad operativa. Señala que la identificación de patrones de fraude en tráfico de voz no puede realizarse en tiempo real, ya que requiere el análisis posterior del tráfico finalizado, a partir de registros como los CDR y bases de datos construidas para tal fin.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Asimismo, **SUMA** advierte que el esquema de etiquetado y revisión de llamadas puede afectar a usuarios legítimos, al generar impactos reputacionales sin una instancia previa de defensa y trasladar al usuario la carga de demostrar la legitimidad de su comportamiento. Por ello, considera necesario fortalecer las garantías de debido proceso, asegurando que las medidas sean proporcionales, motivadas y cuenten con mecanismos efectivos de revisión.

En este sentido, **SUMA** propone que las medidas de monitoreo sean establecidas como lineamientos o recomendaciones de buena práctica sectorial y no como obligaciones estrictas, debido a que podrían generar cargas técnicas y regulatorias desproporcionadas, afectar a PRSTM con menores capacidades, aumentar la supervisión y generar controversias jurídicas.

Finalmente, **SUMA** señala que la lucha contra prácticas fraudulentas debe orientarse mediante buenas prácticas de monitoreo, mecanismos adecuados de supervisión, identificación de los actores que utilizan recursos de identificación, coordinación sectorial y uso de las facultades administrativas existentes, evitando regulaciones excesivamente intrusivas que afecten la innovación, la evolución tecnológica y la calidad de los servicios.

TIGO

Señala que existen limitaciones técnicas relevantes para que el etiquetado de llamadas pueda visualizarse como una advertencia efectiva en el dispositivo del usuario final. La presentación de una etiqueta, alerta o categoría durante la llamada no depende exclusivamente del PRST, sino de factores externos a su control.

Por otra parte, el análisis de patrones durante el establecimiento de la llamada supone una carga técnica y operativa significativa. La detección en tiempo real de comportamientos como llamadas cortas, volúmenes atípicos, marcación secuencial, suplantación o tráfico anómalo exige capacidades avanzadas de procesamiento, correlación y parametrización, cuyo despliegue puede ser complejo, costoso y no necesariamente uniforme entre redes.

Por lo anterior, considera que la propuesta no debería exigir la concurrencia de un número mínimo de patrones ni imponer una metodología cerrada de análisis. La regulación vigente reconoce el uso de herramientas tecnológicas para la gestión y prevención de prácticas irregulares, pero no establece una tipología obligatoria ni predeterminada de patrones que deban ser aplicados en todos los casos. En esa medida, la nueva disposición debería preservar la flexibilidad técnica del PRST para definir, según la arquitectura de su red, la información disponible y sus capacidades operativas, los criterios más adecuados para identificar riesgos.

Sugiere que, en lugar de condicionar la actuación del operador a la verificación de múltiples patrones simultáneos, la norma permita el uso de al menos uno de los criterios mínimos de análisis. Concluye que este enfoque permite avanzar en la mitigación del fraude sin imponer cargas desproporcionadas y sin restringir la innovación en herramientas de detección.

Puntualmente, solicita que el alcance de las medidas aplicables a SMS P2P y voz se limite a la implementación de herramientas tecnológicas basadas en al menos un criterio razonable de análisis de patrones, y no en la exigencia acumulativa de todos los patrones previstos en la propuesta regulatoria.

Respuesta CRC:

ANDESCO y **TIGO** formularon observaciones relacionadas con la viabilidad técnica y el alcance efectivo del etiquetado de llamadas, al considerar que la visualización de la indicación «Alerta de llamada sospechosa» puede depender de la arquitectura y tecnología de red, las capacidades del terminal y las funcionalidades implementadas por terceros. En particular, **ANDESCO** sostuvo que las redes 2G y 3G no soportan esta funcionalidad y que, por tanto, los PRST podrían quedar sujetos al cumplimiento de una obligación cuyo resultado final no se encuentra íntegramente bajo su control.
Por otra parte, **SUMA** y **TIGO** cuestionaron el alcance del monitoreo en tiempo real. **SUMA** señaló que la identificación de patrones requiere el análisis de tráfico ya finalizado, particularmente a partir de CDR, mientras **TIGO** sostuvo que la detección de comportamientos anómalos supone capacidades avanzadas de procesamiento y que la regulación debería permitir a cada PRST utilizar únicamente alguno de los criterios de análisis previstos. **COLOMBIA FINTECH**, por su parte, propuso fortalecer la correlación entre los sistemas antifraude de voz y SMS P2P y garantizar la capacidad de actualización dinámica de los patrones de detección.

A su vez, **COLOMBIA FINTECH**, **SEGUROS BOLÍVAR** y **SUMA** advirtieron sobre el riesgo de falsos positivos y sus posibles efectos respecto de actividades legítimas. **COLOMBIA FINTECH** hizo referencia particular a campañas de cobranza y al uso de agentes virtuales, cuyas características de tráfico pueden presentar baja duración promedio de llamada —ACD— o secuencias reiteradas de intentos. Por ello, solicitó excluir del monitoreo determinada numeración del sector financiero o suspender el etiquetado durante el procedimiento de revisión. **SEGUROS BOLÍVAR** formuló esta última solicitud en términos similares, mientras **SUMA** propuso que las medidas fueran transformadas en lineamientos o buenas prácticas de carácter no obligatorio.

Finalmente, **INETUM** solicitó aclarar si la detección de un patrón anómalo implica el bloqueo de líneas o terminales y **JULIO NULDEMAR** propuso excluir de las obligaciones a los Operadores Móviles Virtuales —OMV— que no tengan control físico y lógico sobre la infraestructura central de la red del operador anfitrión.

Frente a estos comentarios, la Comisión considera necesario partir de una distinción técnica fundamental. El monitoreo del tráfico, la detección de un patrón de comportamiento, la generación de una etiqueta y la representación visual de dicha información en el terminal corresponden a funciones diferentes dentro de la cadena técnica de tratamiento de una llamada. Por consiguiente, las eventuales limitaciones existentes en una de dichas capas no pueden trasladarse automáticamente a las demás ni permiten concluir, de manera general, que la medida sea técnicamente imposible.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Esta distinción resulta particularmente relevante frente a los planteamientos de **ANDESCO** y **TIGO**. La eventual imposibilidad de que un terminal específico represente determinada información en su interfaz no significa que el PRST carezca de capacidad para monitorear el tráfico, identificar el comportamiento de una numeración, clasificar temporalmente el riesgo o generar información asociada a la llamada dentro de las funciones y plataformas que administra.

De igual manera, tampoco resulta técnicamente preciso afirmar, en términos absolutos, que las tecnologías 2G y 3G son inherentemente incapaces de soportar la presentación de información asociada con la identidad del llamante.

Las especificaciones 3GPP contemplan para los sistemas GSM y UMTS el servicio suplementario *Calling Name Presentation* —CNAP—. La especificación 3GPP TS 22.096 identifica CNAP como un servicio de presentación del nombre del llamante y prevé que la red lo invoque durante la fase de establecimiento de la llamada cuando la información correspondiente se encuentre disponible; igualmente, contempla el suministro de información o indicadores de presentación a la parte llamada.[13]

Lo anterior no significa que CNAP sea equivalente, por sí mismo, a la implementación de la etiqueta regulatoria propuesta ni que todos los terminales 2G o 3G existentes en Colombia estén actualmente en capacidad de mostrar de manera homogénea la expresión «Alerta de llamada sospechosa». La propia especificación reconoce que pueden presentarse limitaciones derivadas del interfuncionamiento de señalización y que la precedencia entre información suministrada por la red e información almacenada localmente puede depender de la implementación del terminal.[14]

Sin embargo, estas consideraciones permiten descartar la premisa categórica según la cual existe una imposibilidad inherente y absoluta en las redes GSM y UMTS para suministrar información adicional relacionada con la identificación del llamante. La limitación técnicamente relevante se encuentra en el nivel de implementación, interoperabilidad, aprovisionamiento y representación final en determinados entornos de red y terminales; no en una imposibilidad universal de las tecnologías 2G y 3G para transportar o presentar información asociada con la identificación de la llamada.

Precisamente, el Documento Soporte no desconoció las dificultades asociadas con el despliegue de la medida en entornos tecnológicos heterogéneos. Dentro del análisis multicriterio se incluyeron expresamente la compatibilidad tecnológica, el riesgo de estigmatización, la fatiga por alertas, la rapidez de despliegue, el riesgo de implementación y los costos de adecuación tecnológica, operación y supervisión. En relación con la compatibilidad tecnológica, la CRC reconoció que la alternativa de monitoreo y etiquetado requiere desplegar capacidades de monitoreo, etiquetado y visualización en

13 3GPP TS 22.096 V11.0.0, Universal Mobile Telecommunications System (UMTS); LTE; Calling Name Presentation (CNAP) - Stage 1. ETSI. Disponible en: https://www.etsi.org/deliver/etsi_ts/122000_122099/122096/11.00.00_60/ts_122096v110000p.pdf

14 3GPP TS 22.096 V11.0.0, ibíd. La especificación contempla aspectos de presentación e implementación del servicio CNAP, sin que ello implique una visualización uniforme en todos los terminales.

múltiples entornos tecnológicos y, por ello, recibió una valoración relativa inferior en ese criterio particular.[15]

No obstante, la evaluación regulatoria no se agota en identificar la existencia de una dificultad técnica. El Análisis de Impacto Normativo exige ponderarla frente a los demás efectos de las alternativas. Una vez evaluados integralmente los criterios definidos, la alternativa de lineamientos regulatorios para monitoreo y etiquetado obtuvo el mejor resultado global, con un puntaje agregado de 42,5 %, frente al 29,4 % de la alternativa de rangos exclusivos para comunicaciones comerciales y publicitarias y el 28,1 % del statu quo.[16]

Por ello, la existencia de costos de adaptación, diferencias entre tecnologías o limitaciones de visualización no constituye un elemento sobreviniente omitido en la evaluación. Se trata de factores expresamente considerados y ponderados por la Comisión al seleccionar la alternativa.

Adicionalmente, el estado actual de las redes móviles colombianas tampoco permite evaluar la medida bajo el supuesto de que la prestación de los servicios se soporta predominantemente y de manera exclusiva sobre tecnologías legadas.

De acuerdo con el análisis de infraestructura y cobertura móvil publicado por la CRC con información al cuarto trimestre de 2024, en Colombia existían 29.820 sitios móviles. Del total de sitios, el 94,5 % contaba con tecnología 4G, el 76 % con 3G, el 25 % con 2G y el 5,2 % con 5G. La tecnología 4G era la de mayor cobertura y alcanzaba el 97 % de las cabeceras municipales y centros poblados. La CRC también identificó una reducción de la presencia de tecnologías 2G y 3G asociada con el proceso de modernización de la infraestructura.[17]

Estas cifras deben interpretarse adecuadamente. La presencia de 3G en el 76 % de los sitios no significa que el 76 % de los usuarios o del tráfico de voz dependa exclusivamente de dicha tecnología, pues un mismo sitio puede soportar simultáneamente varias generaciones de red. De hecho, la presencia de 4G en el 94,5 % de los sitios evidencia un grado amplio de superposición y modernización tecnológica. Esta

15 Comisión de Regulación de Comunicaciones (CRC), Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles - Documento Soporte, Proyecto 2000-41-7-1. Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-soporte-mitigacion-fraude-servicios-moviles.pdf

16 CRC, Documento Soporte del proyecto de mitigación del fraude en servicios móviles, análisis multicriterio de alternativas, ibíd.

17 CRC, «CRC presenta nuevo análisis de infraestructura y cobertura móvil en Colombia», información con corte al cuarto trimestre de 2024. Disponible en: https://www.crcom.gov.co/es/noticias/comunicado-prensa/crc-presenta-nuevo-analisis-infraestructura-y-cobertura-movil-en

conclusión corresponde a una inferencia técnica derivada de la distribución de tecnologías reportada por la CRC.[18]

En la misma dirección, las cifras sectoriales de MinTIC muestran que al cierre del cuarto trimestre de 2024 Colombia superaba los 49 millones de accesos a Internet móvil, de los cuales el 84 % utilizaba 4G y el 7,7 % 5G. La Comisión reconoce que la tecnología de acceso a Internet móvil no equivale necesariamente a la tecnología mediante la cual se cursa cada llamada de voz y, por tanto, dichas cifras no deben utilizarse como una medición directa de tráfico VoLTE o VoNR. Sin embargo, sí constituyen un indicador objetivo de la evolución conjunta del ecosistema de acceso, infraestructura y terminales hacia tecnologías móviles de generaciones posteriores.[19]

En consecuencia, la persistencia de redes y terminales 2G o 3G no desvirtúa la idoneidad de la medida. La regulación no puede quedar condicionada a que una funcionalidad alcance previamente una capacidad de visualización absolutamente uniforme en el cien por ciento de las tecnologías y terminales existentes, pues ello supondría utilizar como parámetro regulatorio permanente las capacidades del segmento tecnológicamente más limitado de la red y postergar la incorporación de mecanismos de protección que ya pueden beneficiar a una proporción material y creciente de usuarios.

La efectividad de la medida no responde, por tanto, a una lógica de todo o nada. La ausencia de cobertura universal de la funcionalidad desde el primer día de implementación no significa ausencia de beneficio regulatorio. Cada escenario en el que la red se encuentre en capacidad de advertir al usuario sobre un comportamiento potencialmente sospechoso constituye una oportunidad adicional de prevención antes de que el contacto fraudulento produzca sus efectos.

En este sentido, la amplia presencia de infraestructura 4G y la evolución del ecosistema hacia tecnologías más recientes permiten razonablemente prever que la medida pueda generar beneficios desde el corto plazo y que su alcance efectivo se amplíe conjuntamente con la modernización de las redes y del parque de terminales.[20]

Además, debe recordarse que la medida seleccionada no ordena bloquear una llamada por la sola detección de estos patrones. Su finalidad consiste en incorporar una capa adicional de información preventiva para el usuario, preservando la terminación de la comunicación. El proyecto dispone que, una vez detectado alguno de los patrones definidos, se aplique temporalmente la indicación «Alerta de llamada sospechosa». La propia estructura normativa diferencia este supuesto de las hipótesis específicas de bloqueo previstas en otras disposiciones.[21]

---

18 CRC, análisis de infraestructura y cobertura móvil, ibíd. La conclusión sobre superposición tecnológica corresponde a una inferencia técnica a partir de la coexistencia de varias generaciones de red en los sitios reportados.

19 Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), cifras sectoriales de accesos a Internet móvil al cuarto trimestre de 2024. Disponible en: https://www.mintic.gov.co/portal/715/w3-article-400791.html

20 CRC, análisis de infraestructura y cobertura móvil en Colombia, cit.

21

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Esta característica resulta especialmente relevante en el análisis de proporcionalidad. El etiquetado busca reducir la asimetría de información que enfrenta el usuario al recibir una llamada y advertirle sobre la presencia de características de tráfico asociadas con situaciones potencialmente riesgosas, sin impedirle atender la comunicación. El Documento Soporte evaluó precisamente alternativas de etiquetado en las que el objetivo consiste en alertar sobre un riesgo sin bloquear tráfico que eventualmente pueda ser legítimo.[22]

Ahora bien, frente al argumento de **SUMA** según el cual los patrones solo pueden identificarse después de finalizado el tráfico mediante el análisis de CDR, la Comisión considera que dicha afirmación confunde el momento en el que se genera determinado dato con la arquitectura utilizada para procesarlo.

Es cierto que algunos indicadores requieren información derivada de llamadas finalizadas. La duración promedio de llamada —ACD—, por ejemplo, incorpora la duración de comunicaciones concluidas, mientras indicadores de respuesta requieren conocer el resultado de los intentos de establecimiento. Sin embargo, de ello no se deriva que estos datos únicamente puedan procesarse mediante análisis retrospectivos, periódicos o *batch* realizados mucho tiempo después del evento.

Una plataforma de monitoreo puede incorporar continuamente nuevos eventos a una ventana móvil de análisis y recalcular los indicadores asociados con una numeración, rango, origen o relación de tráfico. Cuando una llamada finaliza, su duración puede incorporarse al conjunto de observaciones disponible; cuando se produce un nuevo intento, su resultado puede actualizar la tasa correspondiente; y cuando el comportamiento acumulado supera el umbral o configura el patrón definido en la metodología, el sistema puede modificar el estado de riesgo asociado con las siguientes comunicaciones.

Por tanto, el monitoreo en tiempo real no debe confundirse con la exigencia técnicamente imposible de conocer la duración final de una llamada antes de que esta termine o de detectar un patrón estadístico antes de que existan eventos suficientes para formarlo. La obligación prevista en el proyecto debe entenderse como una capacidad de monitoreo continuo y operativo del tráfico que permita incorporar los eventos disponibles, actualizar los indicadores y adoptar la medida correspondiente una vez el sistema identifique la configuración de alguno de los patrones. Esta interpretación es consistente con el texto del proyecto, que primero exige sistemas de monitoreo en tiempo real con capacidad de detectar determinadas categorías y, posteriormente, vincula el etiquetado al momento en que el sistema detecte «alguno de estos patrones».[23]

CRC, Proyecto de Resolución «Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles», Proyecto 2000-41-7-1. Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/proyecto-resolucion-mitigacion-fraude-servicios-moviles.pdf

22 CRC, Documento Soporte del proyecto de mitigación del fraude en servicios móviles, análisis de alternativas de monitoreo y etiquetado, cit.

23 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, artículo propuesto 2.1.10.7.2.2.2, cit.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En ese contexto, los CDR pueden constituir una fuente de información relevante, pero no existe fundamento técnico para afirmar que su utilización obliga necesariamente a implementar procesos exclusivamente diferidos. La forma en que los registros, eventos de establecimiento, resultados de las llamadas y demás metadatos sean ingeridos, correlacionados y procesados dependerá de la arquitectura tecnológica utilizada por cada PRST.

Esta precisión permite también responder al planteamiento de **TIGO**. El proyecto no exige la concurrencia simultánea de todos los patrones previstos para aplicar la etiqueta. Existe una diferencia entre la capacidad mínima que debe tener el sistema y la condición que activa la medida.

El artículo propuesto exige que los sistemas tengan capacidad para detectar, como mínimo, las categorías de comportamiento allí relacionadas. Sin embargo, la obligación de etiquetar se activa cuando el sistema detecte alguno de esos patrones. Por tanto, no se requiere que una misma numeración presente simultáneamente volumen inusual, características de robocall, correlación con numeración asociada a fraude y eventos de enmascaramiento.[24]

La solicitud de **TIGO** de permitir que cada PRST implemente únicamente uno de los criterios conduce a una consecuencia diferente. Bajo esa propuesta, un proveedor podría decidir monitorear solamente volumen y carecer de capacidades para correlacionar numeración asociada con fraude, mientras otro podría analizar exclusivamente llamadas cortas y no disponer de mecanismos para detectar eventos de enmascaramiento.

Una regulación de esa naturaleza no establecería un estándar mínimo de detección, sino que mantendría capacidades fragmentadas y puntos ciegos distintos entre las redes. Ello resulta contrario al problema regulatorio identificado por la Comisión y reproduciría precisamente la heterogeneidad de mecanismos de prevención que la alternativa seleccionada pretende superar.[25]

La definición de categorías mínimas de riesgo tampoco equivale a imponer una metodología tecnológica cerrada. El proyecto no determina un fabricante, una plataforma, un algoritmo, un modelo de inteligencia artificial, un esquema SaaS o una solución *on-premise*. Tampoco establece un valor universal e inmodificable para todos los umbrales. Por el contrario, el proyecto permite que determinados parámetros sean definidos en las metodologías internas de los PRST y prevé expresamente que las categorías y parámetros de detección puedan ser actualizados o mejorados en el marco del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles —CTLFSM—. Además, exige acreditar la implementación mediante un informe técnico que describa la arquitectura, los parámetros adoptados y las pruebas de funcionamiento.[26]

---

24 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, ibíd.; la activación del etiquetado se vincula a la detección de «alguno» de los patrones previstos.

25 CRC, Documento Soporte del proyecto de mitigación del fraude en servicios móviles, identificación del problema y evaluación de la heterogeneidad de medidas de gestión y control, cit.

26 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, disposiciones sobre parámetros de detección, informe técnico y Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles (CTLFSM), cit.

Existe, por tanto, una diferencia entre establecer capacidades funcionales mínimas y prescribir la tecnología mediante la cual deben alcanzarse. La regulación adopta el primer enfoque. Esta distinción es concordante con el principio de neutralidad tecnológica contenido en la Ley 1341 de 2009, que garantiza la libre adopción de tecnologías teniendo en consideración las recomendaciones y normas de organismos técnicamente competentes. La neutralidad tecnológica protege la libertad de seleccionar la solución utilizada para prestar el servicio; no implica que cada PRST pueda definir unilateralmente qué riesgos regulatorios decide atender o si implementa las capacidades mínimas exigidas.

Por esta misma razón, la Comisión reconoce la pertinencia técnica del comentario de **COLOMBIA FINTECH** respecto de la evolución dinámica de los patrones de fraude, pero no considera necesario privilegiar regulatoriamente las soluciones SaaS frente a arquitecturas *on-premise*. Ambos modelos pueden, dependiendo de su diseño, incorporar actualizaciones de reglas, firmas o modelos de detección. La obligación regulatoria debe centrarse en el resultado funcional y en la capacidad de adaptación, no en el modelo comercial bajo el cual se suministra la solución.

De igual manera, la correlación entre alertas de voz y SMS P2P planteada por **COLOMBIA FINTECH** puede incrementar la capacidad de identificar campañas multicanal. Sin embargo, de esta consideración no se deriva la necesidad de ordenar una arquitectura específica de integración entre plataformas.

El proyecto crea el CTLFSM como instancia de intercambio de alertas, identificación de patrones de fraude y revisión técnica de las medidas aplicables a voz y SMS. En dicho espacio los participantes pueden proponer y acordar mejoras en la implementación de las medidas mínimas, y la CRC puede requerir estadísticas consolidadas destinadas a construir una visión nacional agregada de las anomalías identificadas.[27]

Por tanto, la correlación multicanal constituye un elemento técnico susceptible de ser profundizado en el CTLFSM conforme evolucionen las modalidades de fraude, sin que resulte necesario imponer desde la regulación una topología particular de los sistemas internos de cada PRST.

En relación con los falsos positivos señalados por **COLOMBIA FINTECH**, **SEGUROS BOLÍVAR** y **SUMA**, la Comisión considera necesario precisar que la detección de un patrón no constituye una declaración jurídica de que el titular de la numeración cometió fraude.

Los parámetros descritos en la regulación corresponden a indicadores de actividad potencialmente sospechosa. La baja duración promedio de las llamadas, la secuencialidad o un volumen atípico pueden presentarse en determinados modelos legítimos de comunicación, pero también constituyen variables útiles para identificar comportamientos automatizados o anómalos.

27 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, disposiciones relativas al CTLFSM, cit.

El hecho de que una variable tenga presencia tanto en tráfico legítimo como en escenarios de riesgo no determina que sea técnicamente inútil. Si ese fuera el criterio, prácticamente ningún modelo de detección comportamental sería viable. La función de un sistema de monitoreo consiste precisamente en analizar el comportamiento dentro de una metodología, una ventana temporal y unos parámetros de decisión que permitan diferenciar progresivamente los escenarios observados.

Por consiguiente, ACD no debe interpretarse como una presunción autónoma de fraude. Tampoco lo son, de manera aislada, la marcación secuencial o el volumen de llamadas. Son elementos de detección cuya aplicación exige parametrización y calibración.

La Comisión ya reconoció este riesgo en el Documento Soporte. La estigmatización derivada de la clasificación incorrecta de comunicaciones legítimas fue incorporada como criterio específico del análisis multicriterio, y la alternativa de monitoreo y etiquetado recibió una valoración relativa inferior en dicho componente precisamente por la posibilidad de falsos positivos. La compatibilidad tecnológica y la precisión del sistema fueron igualmente evaluadas.[28]

En consecuencia, los comentarios recibidos no evidencian un riesgo desconocido por el regulador, sino una de las variables que deberá ser gestionada durante la implementación.

Ahora bien, la solución técnica frente a un falso positivo potencial no consiste en suprimir el monitoreo, convertirlo en una recomendación voluntaria o excluir anticipadamente categorías completas de originadores. Consiste en calibrar los umbrales, analizar las ventanas de observación, incorporar nueva información y revisar los resultados de los modelos.

Para este efecto, la CRC considera necesario precisar en la resolución que, a partir de la publicación en el Diario Oficial de la resolución que adopta esta medida, los PRST deberán construir y mantener una línea base del comportamiento del tráfico de voz originado en sus redes, a partir de una ventana móvil correspondiente a los últimos treinta (30) días calendario y de la información disponible en sus sistemas de gestión y monitoreo.. La metodología deberá considerar, como mínimo, las variaciones del tráfico por franjas horarias, días hábiles y no hábiles, el volumen de llamadas, la duración promedio —ACD—, la tasa de respuesta —ASR—, el tipo de numeración y el origen y destino del tráfico, así como las demás variables que permitan caracterizar el comportamiento normal de la red y diferenciarlo de patrones potencialmente sospechosos. Con fundamento en esta línea base, los PRST deberán definir, actualizar y recalibrar periódicamente los umbrales de detección, para lo cual podrán utilizar técnicas estadísticas, analíticas, de aprendizaje de máquina o modelos híbridos, e incorporar mecanismos para el control de falsos positivos. La metodología deberá mantenerse documentada, servir de soporte al informe técnico previsto en el numeral 2.1.10.7.2.2.4 y permanecer actualizada y disponible para la CRC cuando esta la requiera. Todos estos cambios se verán reflejados en el artículo 2.1.10.7.2.2.2.

28 CRC, Documento Soporte del proyecto de mitigación del fraude en servicios móviles, criterios de estigmatización, compatibilidad tecnológica y precisión del sistema dentro del análisis multicriterio, cit.

La Comisión tampoco acoge la solicitud de **COLOMBIA FINTECH** y **SEGUROS BOLÍVAR** de suspender automáticamente el etiquetado por la sola presentación de una solicitud de revisión. Una solicitud de revisión constituye el inicio del mecanismo previsto para establecer si existe una causa legítima que explique el comportamiento detectado. Su presentación no acredita por sí misma dicha causa. Si la interposición de la solicitud produjera automáticamente la suspensión de la etiqueta, el sistema podría ser neutralizado durante el período de análisis precisamente cuando todavía subsiste incertidumbre respecto del patrón.

Además, una regla de suspensión automática generaría una vía elemental de evasión: ante la aplicación de la medida bastaría con presentar una solicitud para abrir una ventana temporal sin advertencia al usuario, aun cuando el patrón detectado continuara activo. Debe tenerse en cuenta que la etiqueta tiene naturaleza preventiva, informativa y temporal. No bloquea la llamada, no suspende la línea y no constituye una sanción administrativa ni una declaración definitiva de fraude. El proyecto prevé la posibilidad de solicitar revisión, establece un plazo máximo de diez días para resolver la solicitud completa y dispone que el etiquetado se mantenga hasta la conclusión del procedimiento o hasta que cese el patrón, lo que ocurra primero.[29]

La proporcionalidad de la medida debe analizarse a partir de su diseño integral y no únicamente desde la hipótesis de un falso positivo. En primer lugar, es idónea porque entrega al usuario información adicional frente a un comportamiento de tráfico que el sistema ha clasificado como potencialmente sospechoso. En segundo lugar, preserva la comunicación y no impone como consecuencia inicial un bloqueo. En tercer lugar, la medida es temporal y revisable. Finalmente, los parámetros pueden evolucionar a partir de la experiencia técnica y del CTLFSM.

La Comisión considera, además, que la implementación deberá generar información que permita evaluar el desempeño de los modelos. Las estadísticas sobre eventos detectados, etiquetas aplicadas y revisiones solicitadas pueden ser requeridas por la CRC, y el CTLFSM se encuentra facultado para analizar los patrones y acordar mejoras en las medidas mínimas.[30]

En este contexto, indicadores como la proporción de etiquetas objeto de revisión, las tasas de reversión, la recurrencia de causas legítimas similares y el comportamiento de determinados patrones podrán constituir insumos técnicos para perfeccionar progresivamente la precisión de las herramientas. Esta conclusión corresponde a una inferencia operativa consistente con las facultades de seguimiento y actualización previstas para la CRC y el CTLFSM.[31]

---

29 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, procedimiento de revisión de la etiqueta «Alerta de llamada sospechosa», cit.

30 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, facultades de seguimiento e información y funciones del CTLFSM, cit.

31 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, ibíd. La utilización de tasas de revisión, reversión y recurrencia como métricas de calibración es una inferencia operativa basada en dichas facultades de seguimiento.

La existencia de este mecanismo de aprendizaje regulatorio también desvirtúa el planteamiento de **SUMA** según el cual la medida debe limitarse a una buena práctica voluntaria. El problema identificado por la Comisión corresponde precisamente a la baja efectividad de las herramientas disponibles para prevenir y mitigar el contacto con los usuarios con fines fraudulentos. El Documento Soporte señala que la alternativa de mantener el statu quo obtuvo un desempeño global de 28,1 %, frente al 42,5 % obtenido por la alternativa seleccionada.[32]

Transformar la medida en una recomendación significaría mantener un escenario en el que cada proveedor podría decidir si implementa sistemas de monitoreo, qué categorías de riesgo analiza y cuál es el alcance de sus capacidades. Ello no asegura un estándar mínimo homogéneo de protección y permite que modalidades de fraude aprovechen precisamente las diferencias de madurez tecnológica entre redes.

Respecto de la solicitud de **INETUM**, la Comisión aclara que la detección de alguno de los patrones establecidos en el numeral 2.1.10.7.2.2.2 no implica, por ese solo hecho, el bloqueo de la línea, de las llamadas o del equipo terminal. La consecuencia prevista específicamente en dicho numeral consiste en aplicar temporalmente la etiqueta «Alerta de llamada sospechosa» a las llamadas originadas desde el número o rango involucrado. Las hipótesis de bloqueo se encuentran previstas de manera separada para otros escenarios, como las llamadas internacionales entrantes que presenten determinadas condiciones de CLI y la numeración incluida en la Lista de No Originación —DNO—.[33]

Por último, frente a la propuesta de **JULIO NULDEMAR** de excluir a los OMV de las obligaciones técnicas cuando no sean propietarios de la infraestructura central de red, la Comisión no comparte que la condición de OMV permita concluir, de manera general, la existencia de una imposibilidad material de cumplimiento.

Los modelos de operación móvil virtual pueden presentar diferentes grados de autonomía e integración tecnológica. La ausencia de propiedad física sobre un elemento del Core no equivale necesariamente a la inexistencia de capacidades funcionales, información de tráfico, plataformas de gestión o mecanismos de integración con la red anfitriona. Más aún, el criterio propuesto de «control físico, lógico y titularidad» no resulta tecnológicamente neutro frente a arquitecturas actuales basadas en virtualización, servicios administrados y funciones de red ejecutadas sobre infraestructura de terceros. En estos entornos, la propiedad del hardware no constituye el único criterio para determinar quién administra una función o dispone de capacidad para implementar un procedimiento.

La Comisión considera que debe distinguirse entre la obligación regulatoria del PRST y la ubicación técnica en la cual se ejecuta materialmente una función determinada. Que un filtro, una correlación de

32 CRC, Documento Soporte del proyecto de mitigación del fraude en servicios móviles, resultados del análisis multicriterio: 42,5 % para la alternativa seleccionada y 28,1 % para el statu quo, cit.
33 CRC, Proyecto de Resolución de mitigación del fraude en servicios móviles, diferenciación normativa entre monitoreo/etiquetado y supuestos específicos de bloqueo, cit.

señalización o una funcionalidad específica deba ejecutarse en una plataforma administrada por el operador anfitrión puede exigir coordinación técnica y contractual entre las partes; no demuestra que el OMV se encuentre, por definición, excluido de toda obligación de prevención del fraude.

Aceptar una exención general generaría, además, un nivel de protección diferente para el usuario dependiendo del modelo de red utilizado por su proveedor. Igualmente, podría crear incentivos para que funciones relevantes fueran trasladadas contractualmente a terceros con el efecto de diluir las obligaciones regulatorias. Lo anterior no significa desconocer las limitaciones técnicas efectivamente existentes en determinados modelos de OMV. La evaluación de la implementación y, en su caso, de una conducta concreta deberá considerar la arquitectura del proveedor, las funciones que administra, los elementos que se encuentran dentro de su capacidad de actuación y los mecanismos de coordinación disponibles con su operador anfitrión.

Por las razones expuestas, la Comisión no acoge las solicitudes orientadas a eliminar la obligación de monitoreo y etiquetado, transformarla en una buena práctica voluntaria, limitar la capacidad mínima de los sistemas a uno solo de los patrones definidos, excluir de manera general numeración perteneciente al sector financiero, suspender automáticamente la etiqueta durante el procedimiento de revisión o eximir de manera general a los OMV.

La Comisión reconoce que la implementación del etiquetado puede presentar diferencias de alcance y visualización en determinadas tecnologías y terminales. No obstante, estas diferencias no configuran una imposibilidad técnica absoluta, fueron consideradas dentro del análisis multicriterio y deben valorarse en el contexto de un ecosistema móvil en proceso de modernización, en el cual 4G se encuentra presente en el 94,5 % de los sitios móviles y alcanza el 97 % de las cabeceras municipales y centros poblados.[34]

La medida puede, por tanto, producir beneficios efectivos desde el corto plazo y ampliar progresivamente su alcance conforme evolucionen las redes y los terminales. La ausencia de visualización universal desde el inicio no desvirtúa su idoneidad ni justifica posponer un mecanismo de advertencia disponible para una base creciente de usuarios.

Asimismo, la Comisión precisa que la obligación de monitoreo en tiempo real exige una capacidad continua de procesamiento y actualización de los patrones a partir de la información disponible, pero no supone que el PRST deba identificar un comportamiento estadístico antes de que existan los eventos necesarios para su configuración. La utilización de datos provenientes de llamadas finalizadas no impide su incorporación continua a ventanas móviles de análisis ni la actualización del estado de riesgo aplicable a comunicaciones subsiguientes.

Finalmente, el proyecto preserva un equilibrio entre un estándar mínimo común y la flexibilidad tecnológica. Los PRST deben tener capacidad para detectar las categorías mínimas previstas, pero

34 CRC, «CRC presenta nuevo análisis de infraestructura y cobertura móvil en Colombia», cit.

conservan autonomía para definir la arquitectura, las soluciones y, en los términos de la regulación, los parámetros utilizados. El etiquetado que se activa ante la detección de alguno de los patrones tiene carácter temporal, no bloquea la llamada y está sujeto a un procedimiento de revisión. Los patrones y condiciones técnicas podrán evolucionar en el marco del CTLFSM.

En consecuencia, la Comisión mantiene la medida propuesta al considerar que constituye una intervención técnicamente viable, progresiva y proporcional para fortalecer la información disponible para los usuarios frente a llamadas que presentan comportamientos potencialmente sospechosos, sin imponer una tecnología específica ni impedir la terminación inicial de las comunicaciones.

3.3 Etiquetado de llamadas con fines publicitarios

ANDESCO

Sostiene que las medidas asociadas al tráfico de voz deben replantearse bajo criterios estrictos de proporcionalidad y costo-eficiencia. El servicio de voz móvil se encuentra en una fase de declive estructural por la sustitución hacia servicios de datos y aplicaciones OTT, por lo que imponer inversiones significativas en plataformas, señalización, monitoreo y etiquetado sobre un canal decreciente puede generar ineficiencias económicas y destrucción de valor sectorial. Cualquier obligación en materia de voz debería limitarse a variables de señalización técnica y transporte que estén bajo control razonable del operador.

Advierte que la presentación visual de etiquetas como «Alerta de llamada sospechosa» o «Llamada con fines publicitarios» en el terminal del usuario depende de la capa de aplicación, del sistema operativo, del fabricante del dispositivo y de aplicaciones de terceros, no del core de red del PRST. Por tanto, señala que la regulación no debería imponer al PRST una obligación de resultado sobre elementos que no controla, ni hacerlo responsable de la visualización efectiva de la etiqueta.

Dice que la obligación de consultar el Registro de Números Excluidos (RNE) y abstenerse de contactar a usuarios inscritos debe recaer sobre el originador de la comunicación publicitaria o comercial, en tanto es quien conoce la finalidad de la campaña, la base de datos utilizada, las autorizaciones otorgadas por el usuario y la eventual aplicación de excepciones legales. Trasladar al PRST la obligación de verificar y bloquear llamada a llamada frente al RNE implica imponerle una función de calificación jurídica y vigilancia material que excede su rol de proveedor de infraestructura y transporte, pues no cuenta con información suficiente para determinar si una llamada es publicitaria, transaccional, de servicio, solicitada por el usuario o amparada por una excepción legal. En consecuencia, la regulación debería promover reglas claras aplicables a los originadores, bajo la vigilancia de las autoridades competentes, en lugar de una obligación de validación y bloqueo en tiempo real a cargo del PRST.

BLIP BLIP

Señala que la creación de una etiqueta previa de identificación para este tipo de llamadas podría marcar el fin de estos servicios, dado que los usuarios tienden a no contestar llamadas identificadas mediante etiquetas. Advierte que, cuando la etiqueta sea «oficial», el riesgo es mayor y podría significar la desaparición de este tipo de llamadas, en detrimento de toda la industria.

Igualmente, sugiere crear un identificador similar al propuesto para SMS A2P, mediante un etiquetado propositivo con etiqueta de verificación o SenderID verificado a través de protocolos como STIR/SHAKEN, analizando los costos de implementación bajo el concepto de costos eficientes.

Concluye en la importancia de que los portadores y PRST que ofrecen servicios de voz para marketing eviten modificar el CLI mediante prefijos y sufijos que generen confusión en los identificadores de llamadas y falsas expectativas en los consumidores.

CLARO

Señala que esta medida resulta técnicamente inviable por las siguientes razones:

- Es técnicamente inviable en redes heredadas 2G/3G), se utiliza el estándar RCD (Rich Call Data) conectado al validador centralizado de la CRC.

- El Registro Central Único: La empresa que desea hacer telemercadeo no va operador por operador inscribiéndose. Va al validador centralizado, supera el filtro de KYC, registra sus números y declara explícitamente: "Estas líneas se usarán para campañas comerciales".

- La red solo transporta la llamada de voz normal, mientras que la «inteligencia» y el texto en pantalla corren por la capa de datos de los teléfonos inteligentes.

- El operador móvil no puede ser juez y parte al cruzar las llamadas en tiempo real con el RNE y «bloquearlas» si detecta una infracción.

Frente a la obligación del PRST que surge cuando el sistema de monitoreo detecta algún patrón de actividad sospechosa de etiquetar las llamadas originadas desde el número o rango de numeración involucrado con la indicación «Alerta de llamada sospechosa», visible en el dispositivo del usuario receptor, Claro menciona que la intención de la CRC de alertar al usuario es buena, pero la solución planteada es técnicamente inaplicable para el mercado colombiano bajo la tecnología de red actual:

- **Limitación de la señalización telefónica tradicional (SS7/SIP):** Las redes de voz tradicionales de los PRST en Colombia solo transmiten dos datos en la señalización hacia el teléfono del usuario: el número telefónico (CLI) y, en redes muy avanzadas (VoLTE/IMS), un campo de texto corto de nombre (CNAM). Modificar la señalización en tiempo real para «inyectar» un texto dinámico como «Alerta de llamada sospechosa» requiere que toda la red del país esté migrada a redes IMS 4G/5G puras y que los teléfonos de los usuarios soporten protocolos avanzados de visualización de identidad.

En tecnologías 2G y 3G (que aún cubren gran parte del territorio nacional), esto es físicamente imposible.

- **Dependencia del Sistema Operativo del Teléfono (Apple / Android):** El operador móvil (PRST) no controla la pantalla del teléfono del usuario. La visualización de textos o alertas de SPAM depende exclusivamente de los sistemas operativos (iOS de Apple y Android de Google) o de aplicaciones de terceros como Truecaller. Un operador no puede garantizar por red que el texto aparezca en la pantalla de un iPhone o un Android si el sistema operativo del teléfono no está diseñado para leer esa etiqueta del operador.

- **Asfixia Comercial a Call Centers Legítimos**: Los algoritmos de Machine Learning pueden equivocar el diagnóstico. Si un call center legítimo de un banco o una EPS realiza llamadas masivas (con un ACD corto y un ASR bajo porque la gente no contesta), el sistema lo etiquetará automáticamente como «Alerta de llamada sospechosa».

- **La Ventana del Mes de Castigo:** Mantener el etiquetado hasta por un mes después de que cese el patrón, implica destruir comercialmente a cualquier empresa legítima. Tener la etiqueta de «Sospechosa» durante 30 días hará que nadie conteste sus llamadas, lo que generará millonarias demandas por daños y perjuicios de las empresas hacia los operadores móviles.

Para que una obligación de esta naturaleza sea técnicamente viable, como mínimo deberían cumplirse simultáneamente las siguientes condiciones:

- Cobertura y operación sobre redes 4G/IMS en el 100% de las llamadas cursadas.
- Disponibilidad de equipos terminales compatibles con tecnologías 4G/IMS en el 100% de los usuarios.
- Uso de tarjetas SIM compatibles con dichas funcionalidades en el 100% de la base instalada.

Actualmente ninguna de estas condiciones se cumple de manera integral en el mercado colombiano. Persisten usuarios conectados mediante tecnologías 2G y 3G, dispositivos sin capacidades avanzadas de presentación de identidad y tarjetas SIM que no soportan este tipo de funcionalidades.

Frente a la obligación de los PRSTM de consolidar una base de datos de todos los clientes originadores inscritos en las listas propias para etiquetar llamadas con fines publicitarios, menciona **CLARO** que crea riesgos de inconstitucionalidad, seguridad de la información y viola principios de proporcionalidad en el tratamiento de datos personales, siendo más eficiente un modelo de fiscalización basado en reportes bajo demanda tras una denuncia. Se propone ajustar la normativa para reportar solo el inventario de empresas registradas, optimizando el control sin saturar los sistemas con tráfico masivo.

COLOMBIA FINTECH

Señala que el artículo 2.1.18.1. amplía el alcance del RNE pero no excluye expresamente las comunicaciones de cobranza sobre obligaciones en mora, lo que genera ambigüedad sobre si un deudor inscrito en el RNE puede bloquear el contacto de gestión de cartera de su acreedor.

Solicita que la CRC aclare expresamente que la gestión de cobro sobre una obligación crediticia vigente no está sujeta a las restricciones del RNE, con independencia de la inscripción del deudor en dicho registro, en articulación con lo ya establecido en la Ley 2300 de 2023 para las entidades vigiladas por la SFC.

ETB

Señala que aunque es muy es positiva la posibilidad de realizar acciones ante las posibles actividades que impliquen riesgos para los usuarios, se debe tener presente la posibilidad de bloquear, retrasar o etiquetar como sospechosas comunicaciones legítimas representa un riesgo operativo significativo para los operadores y para los usuarios finales. Este riesgo resulta particularmente sensible cuando se trata de comunicaciones transaccionales, servicios financieros, autenticaciones, alertas de seguridad o comunicaciones asociadas a servicios esenciales.

Indica que los operadores podrían enfrentar simultáneamente dos riesgos regulatorios contrapuestos:

- por un lado, ser cuestionados por no bloquear oportunamente una comunicación fraudulenta; y
- por otro, ser objeto de reclamaciones, investigaciones o sanciones por bloquear una comunicación legítima como resultado de un falso positivo razonable.

Este escenario genera incertidumbre jurídica y puede incentivar conductas excesivamente conservadoras o, por el contrario, limitar la efectividad de los mecanismos de mitigación ante el temor de asumir responsabilidades por decisiones automatizadas.

Por estas razones, considera indispensable la Comisión incorpore una disposición expresa en el sentido que los PRST no serán objeto de responsabilidad o sanción cuando ejecuten o adopten medidas de bloqueo, etiquetado o mitigación sustentadas en criterios objetivos de riesgo, indicadores de fraude reconocidos por la industria, información proveniente de autoridades competentes o parámetros definidos por la propia regulación, siempre que hayan actuado de manera diligente y dentro del ámbito de control que razonablemente les corresponde.

Así mismo, considera necesario reconocer que ningún sistema de detección de fraude es infalible. Siempre existirán errores inevitables, porque los mecanismos de monitoreo funcionan con probabilidades, patrones de comportamiento y análisis automatizados. Señala que esta solicitud cobra especial relevancia si se tiene en cuenta que las obligaciones previstas en el proyecto trascienden en muchos casos el ámbito de control directo de los operadores. Como ha expuesto, una parte significativa

de las conductas fraudulentas se origina en plataformas OTT, aplicaciones de mensajería, redes sociales, proveedores de contenidos, integradores tecnológicos, carriers internacionales y otros actores sobre los cuales los PRST no tienen control material ni capacidad de intervención directa. De igual manera, en el caso de los OMV, numerosas funcionalidades asociadas al monitoreo, autenticación, validación, detección y bloqueo dependen de infraestructura y plataformas administradas por terceros, como los operadores de red.

En este contexto, señala que resulta contrario a los principios de razonabilidad y proporcionalidad exigir a los PRST resultados absolutos frente a riesgos cuya generación, administración o mitigación depende parcial o totalmente de terceros. Manifiesta que el ordenamiento jurídico reconoce el principio general según el cual nadie está obligado a lo imposible (*ad impossibilia nemo tenetur*), razón por la cual las obligaciones regulatorias deben evaluarse a la luz de las capacidades reales de actuación y control de los sujetos obligados.

Concluye que, cuando la regulación exige a los operadores desplegar mecanismos de prevención sobre eventos que ocurren fuera de su red, sobre contenidos que no generan, administran ni controlan, o sobre plataformas cuya operación depende de terceros, resulta necesario establecer salvaguardas regulatorias que reconozcan dichas limitaciones objetivas.

NEXVIA

Señala que el proyecto deposita en el PRST la totalidad del ciclo, detección, etiquetado, mantenimiento de la marca y resolución de las reclamaciones del titular afectado, sin prever organismo, auditoría ni reporte alguno que verifique la correcta aplicación de las medidas. La asimetría con el régimen de SMS es notoria, para los mensajes de los agentes independientes se crea un validador, plantillas, registros y causales de recuperación; para las llamadas, gestionadas por los propios operadores, se confía en la autorregulación sin control. Ello pese a que la modalidad de mayor efectividad defraudatoria es precisamente la llamada de suplantación de entidades, frente a la cual el SMS (por su carácter asincrónico y verificable) ofrece al usuario mayor capacidad de reacción. Frente a los artículos 2.1.10.7.2.2.x, propone la siguiente redacción:

> «Adiciónese: «El PRST reportará mensualmente a la CRC y al CTLFSM los números y rangos etiquetados, los patrones que motivaron el etiquetado, su duración y las solicitudes de retiro recibidas y su resultado. La CRC podrá auditar en cualquier momento los sistemas de monitoreo y ordenar el retiro de etiquetas impuestas sin justificación. Contra la decisión del PRST que niegue el retiro del etiquetado, el titular podrá acudir ante la CRC, que resolverá de plano en un término máximo de diez (10) días hábiles.»

TIGO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Este operador señala que existe un error de concepto fundamental en la arquitectura técnica de la propuesta: la pretensión de regular el core de telecomunicaciones para obligar a los operadores a ejecutar el etiquetado informativo de llamadas (Llamada de origen publicitario, Sospecha de fraude).
El procesamiento, la interfaz visual (UI) y la renderización de las etiquetas en la pantalla de un dispositivo móvil ocurren estrictamente a nivel de la capa de aplicación. Esta capa es gestionada de manera exclusiva por los desarrolladores de sistemas operativos (Google Android, Apple iOS) y por aplicaciones especializadas de gestión de contactos de terceros. El desarrollo, mantenimiento y actualización de aplicaciones de usuario final no es, bajo ninguna circunstancia, del resorte, competencia ni capacidad técnica de los PRST ni de los elementos de su red CORE (IMS, SBC, etc.).

Indica que para que el CORE de un operador pudiese inyectar y garantizar la visualización de una etiqueta enriquecida en el terminal, se requeriría obligar a la industria a desarrollar e instalar aplicaciones propietarias en el 100% de los terminales del país para desplazar las interfaces de llamada nativas, lo cual alteraría las condiciones de competencia y la homologación internacional de equipos; o en su defecto, pretender de forma inviable que los protocolos de señalización de red (SIP/ISUP) fuercen la modificación del código fuente de sistemas operativos globales.

Manifiesta que la CRC no puede imponer una obligación de resultado a los PRST cuando las herramientas para lograrlo dependen enteramente de terceros actores globales de software que están fuera de la jurisdicción del regulador y del control técnico de los operadores. Señala que intentar que las redes de telecomunicaciones asuman funciones de desarrollo de software aplicativo desnaturaliza el rol de los PRST como proveedores de infraestructura y transporte, configurando una obligación materialmente imposible de cumplir.

Frente a la propuesta contenida en el artículo 2.1.10.7.2.2.2.1, este operador reitera que la obligación de etiquetar llamadas con fines publicitarios debe ser revisada desde su viabilidad técnica. En los servicios tradicionales de voz, el PRST no controla integralmente la forma en que una etiqueta será presentada en el dispositivo del usuario final, la cual se hace en la capa de aplicación del modelo OSI. La visualización de una advertencia o de una categoría de llamada depende de elementos que no están bajo control exclusivo del operador, como las capacidades del terminal, el sistema operativo, la interoperabilidad con otras redes y las funcionalidades habilitadas por fabricantes o terceros.

Adicionalmente, considera que la obligación de bloquear llamadas publicitarias por una supuesta validación frente al RNE excede el alcance de la Ley 2300 de 2023 y desnaturaliza el rol del PRST. Dicha ley regula la contactabilidad comercial y publicitaria entre productores o proveedores de bienes y servicios y los consumidores, por lo que la carga de consultar el RNE, depurar las bases de datos, verificar autorizaciones y definir si una campaña puede ejecutarse recae en quien origina la comunicación y conoce su finalidad, destinatarios, base legal y autorizaciones aplicables.

Concluye que trasladar al PRST la obligación de verificar, llamada a llamada, si el destinatario está inscrito en el RNE y, con base en ello, bloquear la comunicación, implica imponerle una función material de vigilancia, calificación jurídica y restricción de comunicaciones que corresponde al originador de la

campaña y, en caso de incumplimiento, a las autoridades competentes. Señala que el PRST no cuenta con información suficiente para determinar si una llamada es publicitaria, transaccional, de servicio, solicitada por el usuario, autorizada con posterioridad a la inscripción en el RNE o amparada en alguna excepción legal. En consecuencia, indica que la medida puede generar bloqueos indebidos de comunicaciones legítimas y afectar derechos de usuarios y empresas, sin una relación directa y proporcional con la prevención del fraude cibernético.

PTC

Expone que respecto de las obligaciones contenidas en el Artículo 2.1.10.7.2.2.2.1. «Etiquetado de llamadas con fines publicitarios», y el artículo 2.1.10.7.2.2.2.2. «Procedimiento de revisión del etiquetado de llamada sospechosa representan erogaciones económicas considerables para los PRST, quienes han visto como el modelo de negocio de LDI ha venido perdiendo participación en el mercado. En todo caso, señala que la CRC debe establecer un plazo de al menos seis (6) meses para la implementación de dichas medidas, por cuanto su implementación no solo representa un esfuerzo económico, sino una coordinación interna administrativa de aprobación presupuestal y de desarrollo que puede involucrar a proveedores y terceros ajenos a PTC.

Respuesta CRC:

ANDESCO, **BLIPBLIP**, **CLARO**, **COLOMBIA FINTECH**, **ETB**, **NEXVIA**, **TIGO** y **PTC** cuestionan la viabilidad de exigir a los PRST la visualización de las indicaciones «Alerta de llamada sospechosa» y «Llamada con fines publicitarios» en todos los equipos terminales, dadas las diferencias entre arquitecturas y generaciones de red, las condiciones de interoperabilidad y la dependencia de las funcionalidades de los dispositivos, sistemas operativos y terceros. Asimismo, advierten riesgos de falsos positivos, plantean la utilización de mecanismos como STIR/SHAKEN y RCD, cuestionan el bloqueo llamada a llamada frente al RNE y formulan observaciones relacionadas con la responsabilidad, supervisión y plazo de implementación de las medidas.

Frente a estos comentarios, la CRC considera necesario precisar que el etiquetado de una llamada no equivale a que el core del operador modifique directamente la pantalla del equipo terminal ni a garantizar que una expresión sea visualizada de manera idéntica por todos los usuarios. Técnicamente, el etiquetado comprende la identificación de la condición que activa la medida, la aplicación de una política de tratamiento sobre la comunicación, la asociación de una indicación diferenciada del CLI y el suministro de esa información durante el establecimiento de la llamada para que pueda ser preservada y entregada hacia la parte terminante mediante los mecanismos técnicamente soportados.

En este sentido, la CRC acoge parcialmente las observaciones de **ANDESCO**, **CLARO** y **TIGO** respecto de que los PRST no controlan unilateralmente la interfaz gráfica de los dispositivos, los sistemas operativos ni la representación final de información en todos los terminales. Sin embargo, no comparte que de esta limitación se derive que el etiquetado sea una función exclusivamente ubicada en la capa

de aplicación y completamente ajena a las redes de telecomunicaciones. Tal planteamiento confunde la marcación técnica de la comunicación con su renderización final: la primera consiste en identificar y asociar información a la llamada durante su tratamiento en red; la segunda corresponde a la forma en que el extremo receptor interpreta y presenta esa información.

Por ello, la CRC considera procedente precisar que el etiquetado deberá aplicarse en el origen de la comunicación por el PRST que controla su originación. Es en este punto donde el proveedor puede relacionar el tráfico con la numeración o identidad de llamada involucrada y aplicar la condición correspondiente antes de entregar la comunicación a otra red. La red terminante, por el contrario, recibe una llamada previamente cursada y no dispone necesariamente, a partir del CLI considerado aisladamente, de información suficiente para determinar su finalidad o conocer integralmente los patrones de tráfico asociados al originador.

Para materializar técnicamente la medida, el PRST de origen deberá contar con un criterio objetivo que active el tratamiento. En las llamadas con fines publicitarios, dicha condición deriva de la finalidad declarada por quien desarrolla la campaña; en las llamadas sospechosas, de los patrones y parámetros de monitoreo definidos en la regulación. Identificada la condición, las funciones de control de llamada o sesión, procesamiento de señalización o control de borde que correspondan según la arquitectura del proveedor deberán aplicar la política de etiquetado antes de la interconexión y asociar a la comunicación la indicación correspondiente sin modificar los dígitos del CLI.

La CRC comparte, por tanto, la observación de **BLIPBLIP** en cuanto a que la identificación de la finalidad o condición de una llamada no debe realizarse mediante la incorporación de prefijos o sufijos al número presentado. El CLI y la etiqueta cumplen funciones técnicamente diferenciables: uno identifica la numeración llamante y la otra suministra información contextual sobre la finalidad declarada o sobre una condición de riesgo asociada a la comunicación.

La información de etiquetado deberá suministrarse durante el establecimiento de la llamada mediante mecanismos técnicamente soportados por las redes involucradas. En arquitecturas SIP existen mecanismos estandarizados que permiten asociar información contextual a una sesión, incluida información relacionada con la razón de la llamada. Sin embargo, la CRC no considera adecuado imponer en la regulación un encabezado SIP, parámetro ISUP o solución tecnológica única, pues las capacidades de las arquitecturas y de los mecanismos de interfuncionamiento son diferentes. La obligación debe formularse como un resultado funcional: identificar, marcar y suministrar desde origen la condición asociada a la comunicación antes de entregarla a otra red.

Los proveedores que intervengan posteriormente en el tránsito y terminación deberán preservar y suministrar dicha información dentro de las capacidades técnicas y condiciones de interoperabilidad aplicables. La CRC reconoce que la presentación final al usuario podrá depender de la red terminante y de las funcionalidades del equipo receptor; por tanto, no se exigirá al PRST garantizar una visualización uniforme en el ciento por ciento de los terminales. Esta precisión delimita la obligación a las funciones

bajo control razonable de los proveedores, como solicitan **ANDESCO**, **CLARO**, **TIGO** y **ETB**, pero no elimina el deber de aplicar técnicamente el etiquetado en origen.

Tampoco se comparte el argumento de **CLARO** según el cual la medida solo resultaría viable cuando la totalidad de las llamadas sea cursada sobre 4G/IMS, todos los usuarios dispongan de terminales compatibles y toda la base instalada soporte las mismas funcionalidades. La heterogeneidad tecnológica puede limitar la preservación o presentación extremo a extremo en algunos escenarios, pero no demuestra la imposibilidad de aplicar una política de tratamiento en el origen ni justifica condicionar la medida a una compatibilidad tecnológica universal.

Tratándose de llamadas con fines publicitarios, la aplicación en origen resulta particularmente relevante. El productor, proveedor o cliente que realiza la campaña conoce la finalidad del contacto y debe declararla correctamente; el PRST de origen, a partir de esa condición, aplica el tratamiento técnico correspondiente al tráfico. El operador no debe escuchar la comunicación ni realizar una calificación jurídica individual de cada llamada, ni puede exigírsele inferir en destino si el contacto corresponde a publicidad, cobranza, autenticación, atención al cliente o una comunicación transaccional.

Esta precisión permite igualmente atender los comentarios de **ANDESCO** y **TIGO** sobre el RNE. La obligación de etiquetar una llamada publicitaria en origen no convierte al PRST en responsable de validar, llamada a llamada, si existe autorización para contactar al destinatario, si resulta aplicable una excepción legal o si la comunicación puede efectuarse frente a una inscripción en el RNE. Esa información se encuentra en cabeza de quien realiza la actividad de contacto y conoce su finalidad, destinatarios y condiciones jurídicas. En consecuencia, la CRC considera procedente eliminar la obligación de bloqueo a cargo del PRSTM frente al RNE establecida en el numeral 2.1.10.7.2.2.2.1 del artículo 2.1.10.7 del proyecto resolución. En igual sentido, frente a **COLOMBIA FINTECH**, la CRC coincide en que es necesario mantener diferenciadas las comunicaciones cuya finalidad exclusiva sea la gestión de cobranza de las llamadas comerciales o publicitarias. La naturaleza jurídica de la comunicación debe corresponder a la finalidad real de la actividad de contacto y no ser inferida por el PRST a partir de variables técnicas de tráfico. Es por este motivo que, frente a las llamadas publicitarias, el artículo 2.1.10.7.2.2.2.1 ya contiene un mecanismo que permite identificar de manera clara y concreta las llamadas que tengan esa finalidad.

Además, respecto de las llamadas que potencialmente puedan ser consideradas como sospechosas, el artículo 2.1.10.7.2.2.2.2. ya contiene un procedimiento de revisión del etiquetado de llamada sospechosa en el que el interesado puede explicarle al operador el uso legítimo de la línea, como lo podría ser la gestión de cobranzas. En efecto, el usuario titular de una línea de numeración nacional que sea objeto del etiquetado previsto en el presente artículo podrá solicitar al PRST la revisión de la medida dentro de los diez (10) días hábiles siguientes a la notificación del etiquetado, acreditando que su comportamiento de uso responde a una causa legítima. Por lo tanto, no se considera necesario modificar estas disposiciones.

Respecto de los riesgos de falsos positivos planteados por **CLARO** y **ETB**, la CRC reconoce que indicadores como el volumen de llamadas, la duración promedio —ACD— o la tasa de respuesta —ASR— pueden evidenciar comportamientos atípicos sin acreditar por sí solos la existencia de fraude. Por esta razón, la activación del etiquetado de llamada sospechosa deberá sustentarse en criterios objetivos, trazables y susceptibles de revisión, y la indicación conservará una naturaleza informativa y temporal, sin constituir una declaración definitiva de ilicitud.

También en este caso la medida deberá aplicarse en origen. El PRST que controla la originación de la numeración sobre la cual se detectan los patrones previstos deberá aplicar la correspondiente política a las llamadas subsiguientes antes de su entrega a otra red. Esta arquitectura evita que cada red terminante analice segmentos parciales del tráfico y adopte clasificaciones diferentes respecto de una misma numeración.

La CRC no considera procedente acoger la solicitud de **ETB** de incorporar una exoneración general y anticipada de responsabilidad frente a las consecuencias de las medidas de etiquetado o mitigación. La responsabilidad deberá analizarse conforme a las obligaciones aplicables y las circunstancias de cada caso. No obstante, la delimitación de la obligación al ámbito técnico de control del PRST, la definición de criterios objetivos, la trazabilidad y los mecanismos de revisión responden a la preocupación del agente sobre la imposición de resultados absolutos respecto de elementos administrados por terceros.

Frente a **NEXVIA**, la CRC comparte la necesidad de contar con trazabilidad y mecanismos de supervisión sobre la aplicación del etiquetado. Sin embargo, no considera procedente que la Comisión se convierta en una instancia operativa de clasificación de cada llamada o de revisión automática de todas las decisiones adoptadas por los proveedores. Los PRST deberán conservar información que permita identificar la numeración sometida a la medida, el criterio que activó el etiquetado, su periodo de aplicación y el resultado de las solicitudes de revisión, de manera que la CRC pueda requerir y evaluar dicha información en lo que corresponda en ejercicio estricto de sus competencias regulatorias.

Por otra parte, la CRC no acoge la propuesta de **BLIPBLIP** de condicionar el etiquetado a la implementación previa de STIR/SHAKEN o RCD. La autenticación técnica de la identidad llamante y la clasificación informativa de una comunicación atienden finalidades diferentes. La indicación «Llamada con fines publicitarios» informa una finalidad declarada y la expresión «Alerta de llamada sospechosa» comunica la aplicación de una medida sustentada en criterios de monitoreo. Ninguna de ellas constituye, por sí misma, una certificación de autenticidad del CLI. Los mecanismos de identidad e información enriquecida podrán complementar la evolución técnica de las medidas, pero su implementación previa no constituye una condición necesaria para aplicar una política de etiquetado en origen.

Tampoco se considera que la eventual reducción de las tasas de respuesta de las campañas, planteada por **BLIPBLIP**, desvirtúe la finalidad de la medida. La indicación «Llamada con fines publicitarios» tiene naturaleza descriptiva y busca informar al usuario sobre la finalidad del contacto. La decisión de atender o no una comunicación una vez conocida dicha finalidad corresponde precisamente al objetivo informativo perseguido.

Finalmente, la reducción relativa de la utilización de la voz frente a servicios de datos y aplicaciones OTT, señalada por **ANDESCO** y **PTC**, no demuestra por sí sola la falta de proporcionalidad de la medida. Mientras la voz continúe siendo utilizada para contactar usuarios y pueda constituir un medio para campañas publicitarias o eventos de fraude, persiste la necesidad de adoptar mecanismos de información y mitigación. No obstante, la precisión de la arquitectura de etiquetado en origen y las adecuaciones técnicas e interoperabilidad que resulten necesarias deberán considerarse al revisar el plazo de implementación previsto en el proyecto.

Por ultimo y, en atención a las adecuaciones técnicas, administrativas y de interoperabilidad requeridas, en el proyecto publicado la CRC consideró necesario establecer un periodo de implementación de máximo tres (3) meses. Para que la medida pueda ser implementada de manera eficiente y dentro de ese periodo, la Comisión considera necesario precisar que, durante el primer mes, los PRST habilitarán el registro e inscribirán a los clientes y la numeración utilizada con fines publicitarios; en los dos meses siguientes, los PRST realizarán las configuraciones, integraciones y pruebas necesarias para aplicar la indicación «Llamada con fines publicitarios». En consecuencia, se ajustará el artículo 2.1.10.7.2.2.2.1 del proyecto de resolución en ese sentido.

3.4 Lista de No Originación (DNO)

ASOBANCARIA

Indica que, si bien el Proyecto prevé mecanismos de revisión periódica, expiración automática y corrección para el etiquetado de comunicaciones y las listas Do Not Originate (DNO), conviene fortalecer su gobernanza y operación. A tal efecto, debería precisarse la autoridad encargada de administrar, supervisar y actualizar estos registros; los criterios para incluir, excluir, revisar o retirar numeración; y las condiciones de acceso para los PRSTM y demás actores autorizados.

CLARO

Respalda la estrategia integral propuesta por la CRC al abordar el fraude desde múltiples frentes (bloqueo, monitoreo, gobernanza y etiquetado). No obstante, señala que la prohibición total del enmascaramiento de CLI requiere excepciones técnicas claramente definidas (ej. servicios enterprise, contact centers internacionales legítimos, roaming), dado que en entornos SIP/IMS el CLI puede ser manipulado por carriers externos. En virtud de lo anterior, considera necesario que se definan mecanismos de validación progresiva como attestation frameworks (equivalente a STIR/SHAKEN) antes de una prohibición absoluta.

Afirma que esta obligación también obliga a implementar mecanismos de control en sus nodos de interconexión internacional para bloquear de manera perimetral las llamadas con origen internacional que utilicen numeración nacional contenida en esta lista, o que no cumplan estrictamente con el formato

y estructura de la Recomendación UIT-T E.164, conforme a las condiciones establecidas en el artículo 2.1.10.7.2.2.3 de la presente resolución. En virtud de lo anterior, solicita a la CRC que incluya este aspecto en la definición de LISTA DNO (DO NOT ORIGINATE).

Adicionalmente, considera inviable que cada PRSTM tenga su propia lista de no originación. A título de ejemplo, menciona que, si cada operador mantiene su propia base de datos DNO de forma independiente, un banco que desee proteger sus líneas de «Solo Entrada» tendría que hacer un trámite administrativo y técnico individual ante cada PRSTM. Si un operador se demora en actualizar la lista, el delincuente concentrará sus ataques de spoofing a través de esa red vulnerable.

Las altas, bajas y modificaciones de números telefónicos institucionales ocurren diariamente. Las redes móviles necesitan consultar una única fuente de verdad técnica para que los bloqueos perimetrales se ejecuten en tiempo real y de manera uniforme en todo el territorio nacional.

La lista DNO debe ser administrada de forma centralizada por la CRC, tal como se propone en las definiciones iniciales. Los operadores no deben ser los administradores ni los validadores del inventario de números de solo recibo del país; su única función debe ser la de ejecutores del bloqueo técnico en sus redes.

Sobre la obligatoriedad del administrador de recursos de identificación de publicar y mantener actualizada la relación de números que deben ser incluidos obligatoriamente en la lista de no originación, Claro menciona su acuerdo con que la lista en el SIGRI sea administrada por la CRC. No obstante, señala que el SIGRI históricamente ha funcionado como un portal web de registro administrativo para la asignación de recursos escasos (códigos cortos, numeración), no como una plataforma de ciberseguridad de alta disponibilidad. Indica que, si los PRST deben descargar manualmente o mediante scripts básicos la lista del SIGRI, se generarán retrasos en la protección de las redes, por lo que debe actualizarse por parte del regulador.

SUMA

Señala que, como Operador Móvil Virtual (OMV), no tiene control directo sobre los elementos de red relacionados con la originación, interconexión y cursado del tráfico de voz, ya que estos son gestionados por los Operadores Móviles de Red (OMR) mediante las relaciones mayoristas existentes. Por esta razón, considera que la implementación de mecanismos como las listas de no originación (DNO), destinadas a bloquear numeración inválida o no autorizada, depende técnicamente de los OMR, quienes tienen la capacidad sobre la señalización y el enrutamiento del tráfico.

En consecuencia, SUMA plantea que la obligación de administrar, implementar y actualizar las listas DNO debería recaer principalmente en los OMR, debido a que son los actores con capacidad técnica efectiva para ejecutar estas medidas. Según su posición, imponer la misma obligación a los OMV generaría cargas operativas y duplicidades regulatorias sin aportar mayores eficiencias en la prevención del fraude, dada la dependencia de los OMV frente a la infraestructura de los OMR.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En consecuencia, propone a la Comisión precisar en la redacción de la medida que, para efectos de su implementación, la obligación de mantener listas DNO se entiende cumplida por parte de los OMV a través de los mecanismos que, para tal fin, sean implementados por el OMR con el que tienen suscritas relaciones de acceso, sin perjuicio de las obligaciones de colaboración, reporte y control que correspondan a estos agentes.

Respuesta CRC:

ASOBANCARIA, **CLARO** y **SUMA** plantean observaciones sobre su gobernanza, administración y actualización; los criterios de inclusión y retiro de numeración; la necesidad de contar con una fuente común para todos los proveedores; la oportunidad en el acceso a sus actualizaciones; y las condiciones de implementación de la medida en los modelos de operación móvil virtual.

Al respecto, la CRC precisa que la Lista DNO tiene una finalidad específica: identificar numeración E.164 nacional que, por una condición objetiva asociada a su estado o modalidad de uso, no debe presentarse como identificador de línea llamante —CLI— en la originación de llamadas. En tal sentido, la DNO no constituye un mecanismo para autenticar criptográficamente la identidad del originador ni para determinar si este se encuentra legítimamente autorizado para utilizar un determinado CLI. Por ello, las observaciones relacionadas con la implementación previa de esquemas de attestation equivalentes a STIR/SHAKEN y las excepciones para servicios empresariales o centros de contacto internacionales corresponden al análisis de las medidas aplicables al tráfico internacional entrante y no desvirtúan la procedencia de la DNO. Cuando un número se encuentra válidamente clasificado como no habilitado para originar llamadas, su bloqueo deriva de dicha condición objetiva y no de la autenticación de quien presenta el CLI.

La CRC comparte, no obstante, las observaciones de **ASOBANCARIA** y **CLARO** en cuanto a la conveniencia de fortalecer la gobernanza y aplicación uniforme de la lista. El proyecto ya prevé que el Administrador de los Recursos de Identificación publique y mantenga actualizada la numeración que debe incluirse obligatoriamente en las listas DNO de todos los PRST; sin embargo, también permite que cada proveedor incorpore numeración adicional en su propia lista y posteriormente la reporte a la CRC. Esta última posibilidad puede generar diferencias temporales entre redes, de forma que una numeración sea bloqueada por un proveedor mientras continúa siendo admitida por otros. Tratándose de una medida cuya eficacia depende de evitar que numeración no habilitada para originar llamadas sea utilizada como CLI, su aplicación no debe variar en función de la red a través de la cual se curse el tráfico.

Ahora bien, la Comisión reconoce que la posibilidad de que cada PRST incorpore numeración adicional en su propia lista puede generar diferencias temporales entre redes, de manera que determinada numeración sea bloqueada por un proveedor mientras continúa siendo admitida por otros. No obstante, eliminar esta facultad y supeditar cualquier actuación a la actualización previa de la relación publicada

por la CRC podría reducir la capacidad de respuesta inmediata frente a hallazgos obtenidos directamente del monitoreo del tráfico. Desde el punto de vista técnico, los PRST cuentan con visibilidad sobre el comportamiento del tráfico cursado en sus redes y pueden identificar oportunamente eventos o usos anómalos que ameriten la adopción de medidas preventivas.

Por esta razón, la CRC considera procedente mantener un esquema que combine un estándar nacional obligatorio con una capacidad de reacción distribuida. Así, todos los PRST deberán implementar y aplicar la relación de numeración publicada por el Administrador de los Recursos de Identificación, garantizando un nivel mínimo y común de bloqueo en todas las redes, sin perjuicio de que cada proveedor pueda incorporar numeración adicional como resultado de sus actividades de monitoreo. Estas adiciones deberán ser informadas a la CRC dentro de los cinco (5) días hábiles siguientes, lo que permitirá analizar los hallazgos identificados, mantener su trazabilidad y evaluar la procedencia de incorporar dicha numeración a la relación de obligatoria aplicación para todos los PRST. En ese sentido se modificará el artículo 2.1.10.7.2.2.3 de la resolución.

De esta forma, las responsabilidades se mantienen claramente diferenciadas: los PRST identifican y reportan; la CRC administra y actualiza la Lista DNO nacional; y los proveedores ejecutan en sus redes el bloqueo de las llamadas que presenten la numeración incluida en dicha relación. La lista DNO centralizada no sustituye las obligaciones de monitoreo de los PRST ni limita la adopción inmediata de las demás medidas antifraude previstas en la regulación frente a eventos identificados en sus redes.

La CRC considera igualmente necesario que la inclusión y permanencia de la numeración en la DNO responda a la subsistencia de la condición objetiva que la justifica. Para la numeración no atribuida, no asignada o no adjudicada, dicha condición puede determinarse a partir de la información administrada por la propia Comisión. Respecto de la numeración destinada exclusivamente a la recepción de llamadas, deberá mantenerse actualizada la información que permita acreditar esta modalidad de uso y reflejar oportunamente cualquier modificación que habilite posteriormente su utilización para originación. En consecuencia, la lista deberá contar con mecanismos de actualización y corrección cuando cambien las condiciones que dieron lugar a la inclusión de la numeración, sin que resulte necesario establecer una excepción general al bloqueo de números válidamente incorporados en la DNO.

Frente a la observación de **CLARO** sobre la oportunidad de acceso a las actualizaciones, la CRC reconoce que la eficacia de una lista nacional depende de que la información pueda ser conocida y aplicada oportunamente por los proveedores. Por ello, la Comisión revisará la forma operativa y tecnológica más adecuada de disponer, actualizar y permitir la consulta de la Lista DNO, con el propósito de evitar retrasos o impactos en el acceso a la información necesaria para su aplicación, sin predeterminar una arquitectura tecnológica o mecanismo específico.

Ahora bien, la CRC no acoge la solicitud de **CLARO** de incorporar en la definición de Lista DNO las llamadas cuyos identificadores incumplan el formato o estructura de la Recomendación UIT-T E.164. La DNO contiene numeración identificable que, por su estado o condición de uso, no debe presentarse como CLI de una llamada originada. En contraste, el incumplimiento de las reglas de formato, longitud

o estructura corresponde a una validación sobre el identificador presentado en la señalización. Se trata de controles técnicamente diferenciables y regulados separadamente en el proyecto; por tanto, su incorporación en una única definición podría confundir el inventario de numeración no habilitada para originación con las reglas de validación sintáctica aplicables al tráfico.

Finalmente, frente a **SUMA**, la CRC reconoce que, dependiendo de la arquitectura utilizada por un OMV, los elementos de red en los que se analiza la señalización o se ejecuta materialmente el bloqueo pueden encontrarse bajo la administración del OMR anfitrión. Sin embargo, esta circunstancia no justifica establecer una excepción para los OMV ni permite entender cumplida automáticamente su obligación por la sola implementación de la medida en la red del OMR. La distribución técnica de funciones entre ambos agentes no modifica la obligación regulatoria respecto de los servicios prestados por el OMV.

Por tanto, cuando la implementación de la DNO dependa de elementos administrados por el OMR, el OMV deberá acordar y coordinar con su operador anfitrión las condiciones técnicas y operativas necesarias para garantizar que la Lista DNO nacional sea efectivamente aplicada al tráfico asociado a sus servicios. La medida podrá ejecutarse técnicamente a través de la infraestructura del OMR, de acuerdo con la arquitectura y la relación de acceso existente, pero ello no exonera al OMV de las obligaciones de colaboración, reporte, trazabilidad y verificación que le correspondan.

3.5 Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles – CTLFSM

ASOBANCARIA

Destaca como positiva la creación del CTS y del CTLFSM, pero advierte que el diseño puede limitar la participación efectiva de las entidades financieras, directamente afectadas por el fraude, que quedarían subordinadas a la operación de un agente privado y con participación solo como invitadas a sesiones específicas del CTS, lo que podría tensionar el régimen de protección al consumidor financiero (Ley 1328 de 2009), el derecho a la intimidad (Ley 2300 de 2023) y los principios de proporcionalidad, igualdad y debido proceso.

Propone incorporar a los asignatarios de SENDER ID o a un representante del sector financiero, a través de su gremio, como participantes con voz en el CTS e invitados permanentes en el CTLFSM; garantizar la participación permanente del sector financiero y esquemas de intercambio de información en tiempo real; y precisar que la excepción de no publicación de ciertos proyectos de regulación (artículo 16) operará sin perjuicio de mecanismos de socialización previa cuando las decisiones del CTLFSM impongan nuevas cargas a agentes no representados en el comité.

BLIPBLIP

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Solicita que los PCA/IT sean incluidos como miembros permanentes del CTLFSM, con voz y voto en la revisión y aplicación de medidas reglamentarias, reglas de detección y acciones a aplicar. Señala que un comité de regulación sin participación de los regulados no tendría sentido frente al objetivo de incluir a todos los actores involucrados.

Asimismo, solicita a la CRC la creación de mesas de discusión públicas para analizar este tipo de normativas, incluyendo los proyectos regulatorios y los impactos identificados en la industria, costos y libre mercado.

ETB

Considera necesario preservar la diferencia entre coordinación técnica y funciones regulatorias: el CTLFSM debe ser una instancia de articulación, análisis técnico y recomendaciones, y no un mecanismo para introducir obligaciones regulatorias nuevas o adoptar decisiones vinculantes sin surtir el correspondiente Análisis de Impacto Normativo. Advierte que generar obligaciones sin agotar la consulta pública, la participación y el AIN de la Ley 1341 de 2009 afectaría la transparencia, la seguridad jurídica y el debido proceso, por lo que cualquier obligación con costos, inversiones o desarrollos debe someterse previamente a los procedimientos ordinarios de construcción regulatoria.

EXPERIAN

Valora las medidas (SENDER ID, códigos cortos A2P, validación centralizada, monitoreo, listas DNO, etiquetado y comités) como base relevante frente al smishing, el vishing, el spoofing y la suplantación, y propone ampliar el alcance del proyecto para permitir el acceso restringido, seguro y estandarizado a alertas técnicas no personales, patrones de riesgo e indicadores de fraude asociados a códigos cortos, SENDER ID, CLI, URLs, dominios y plantillas.

Soporta su propuesta en la Ley 2573 de 2026 (artículos 5 y 7, sobre medidas de seguridad digital, validación de identidad, atención de personas suplantadas y marcación de «Víctima de Falsedad Personal») y en la Ley 1266 de 2008, y propone que la información técnica, operativa o agregada derivada de eventos de fraude pueda compartirse, bajo condiciones de seguridad, finalidad, necesidad, proporcionalidad y trazabilidad, con los operadores de información, para fortalecer la identificación de patrones, la atención de reclamaciones por suplantación y la protección del historial crediticio.

CLARO

Señala que el artículo 2.1.10.7.3 crea el CTLFSM y da carácter obligatorio a sus decisiones, pero no define su funcionamiento, administración, competencias, mecanismos de decisión ni procedimientos, lo que genera incertidumbre jurídica y operativa y podría configurar una delegación excesivamente amplia que permita establecer obligaciones y criterios técnicos sin surtir el análisis de impacto, la publicidad y la participación propios del proceso regulatorio. Advierte que, si las decisiones son obligatorias, el comité no puede convertirse en un mecanismo de regulación paralela.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En cuanto a la vinculatoriedad, observa que el comité obliga a la asistencia de los PRST y de los asignatarios de códigos cortos, pero omite incluir como miembro obligatorio a la persona jurídica que operará el validador centralizado, que custodia la base de datos de marcas, contratos KYC y plantillas. Respecto del quórum y la votación por mayoría simple, advierte que, al existir pocos PRSTM y decenas de asignatarios, los integradores pequeños podrían aprobar obligaciones que afecten el núcleo de red de los operadores o bloquear medidas de seguridad, por lo que solicita incluir una regla según la cual, cuando las decisiones impacten la configuración técnica, el enrutamiento, la señalización o la seguridad perimetral de los núcleos de red, el voto favorable de los PRSTM que operen dicha infraestructura sea mandatorio y vinculante.

En virtud de lo anterior, solicita a la CRC que incluya lo siguiente:

«No obstante, cuando las decisiones sometidas a votación impacten directamente la configuración técnica, enrutamiento, señalización o seguridad perimetral de los núcleos de red de telecomunicaciones, el voto favorable de los PRSTM que operen dicha infraestructura será mandatorio y vinculante para la aprobación de la medida, evitando la imposición de cargas técnicas por parte de agentes no operadores de red»

INETUM

Solicita que se aclare, si dentro del CTLFSM no se considerará incluir como participante a la persona jurídica encargada del validador centralizado.

NEXVIA

Respalda el comité como iniciativa valiosa, pues la inteligencia compartida en tiempo real es la herramienta antifraude de mayor efectividad, pero sostiene que su composición no puede limitarse a los PRST, ya que los PCA e IT operan la primera línea de detección (filtrado de contenidos, bloqueo de cuentas, identificación de suplantación, SIM boxing y SMS pumping) y disponen de información que los operadores no ven; excluirlos del órgano donde se acordarán las mejoras a los parámetros mínimos de detección (artículo 2.1.10.7.2.1.4) implica que las reglas que los obligan se negociarán sin ellos, en contra del principio de participación. Propone adicionar al artículo 2.1.10.7.3 que sean miembros permanentes del CTLFSM, con voz y voto, los PCA y los IT inscritos en el RPCAI que manifiesten su voluntad de participar, garantizando la representación equilibrada de todos los segmentos.

En este punto, solicita la siguiente redacción:

> «Adiciónese al artículo 2.1.10.7.3: «Serán miembros permanentes del CTLFSM, con voz y voto en la revisión técnica de medidas y parámetros de detección, los PCA y los Integradores Tecnológicos inscritos en el RPCAI que manifiesten su voluntad de participar, así como las autoridades que la CRC convoque. La CRC garantizará la representación equilibrada de todos los segmentos del ecosistema en las decisiones del Comité.»

PTC

Está de acuerdo con la creación del CTLFSM como instancia de intercambio de alertas, identificación de patrones y revisión técnica, pero pide precisar dos aspectos. Primero, sobre la periodicidad y convocatoria (artículo 2.1.10.7.3.2), solicita aclarar la expresión «atención urgente» que habilita las sesiones extraordinarias y si la convocatoria puede promoverse a solicitud de parte por los agentes del comité o solo de oficio por la CRC.

Segundo, sobre la vinculatoriedad (artículo 2.1.10.7.3.4), advierte que las decisiones del CTLFSM sobre parámetros técnicos serían de cumplimiento obligatorio para los PRST y podrían incorporarse a la regulación mediante resoluciones que el artículo 16 exceptúa de publicación; considera que ello puede resultar gravoso al permitir modificaciones técnicas por decisión de la Comisión sin discusión sectorial ni Análisis de Impacto Normativo previo, especialmente cuando impliquen desarrollos tecnológicos, ajustes de sistemas o inversiones adicionales.

SCAMZERO

Coincide en que el desconocimiento de los usuarios es una de las causas del problema, pero sostiene que el principal obstáculo no es la falta de disposición del usuario, sino la ausencia de herramientas concretas que le permitan verificar en tiempo real si un mensaje o enlace es sospechoso, pues las campañas educativas por sí solas resultan insuficientes frente al incremento del smishing. Propone que las medidas pedagógicas incluyan la divulgación de herramientas de verificación de enlaces, mensajes y números disponibles en el mercado, bajo un enfoque de neutralidad tecnológica que no favorezca una herramienta específica.

Respuesta CRC:

Sobre esta temática se pronunciaron **ASOBANCARIA**, **BLIP BLIP**, **ETB**, **EXPERIAN**, **CLARO**, **INETUM**, **NEXVIA**, **PTC** y **SCAMZERO**. Revisadas las intervenciones, la Comisión identifica una tendencia mayoritaria y convergente que valora positivamente la creación del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles (en adelante, CTLFSM) como instancia permanente de coordinación, intercambio de alertas e identificación de patrones de fraude, y que reconoce en el intercambio de inteligencia en tiempo real una de las herramientas antifraude de mayor efectividad. Dentro de esa valoración favorable, los comentarios se agrupan en dos grandes líneas argumentativas, que la Comisión aborda a continuación de manera diferenciada.

La primera línea, de carácter mayoritario, solicita ampliar la participación en el Comité. **ASOBANCARIA** propone incorporar a los asignatarios de SENDER ID y a un representante del sector financiero, a través de su gremio, como invitados permanentes en el CTLFSM. **BLIPBLIP** y **NEXVIA** solicitan que los Proveedores de Contenidos y Aplicaciones (PCA) y los Integradores Tecnológicos (IT) inscritos en el

RPCAI sean miembros permanentes con voz y voto en la revisión técnica de las medidas y de los parámetros de detección. **INETUM** y **CLARO** plantean que se aclare si la persona jurídica que operará el validador centralizado será integrante del Comité, señalando **CLARO** que, por custodiar la base de datos de marcas, contratos KYC y plantillas, resulta técnicamente necesario incorporarla. **SCAMZERO** propone incluir la perspectiva del usuario mediante la participación de organizaciones de protección al consumidor digital y de desarrolladores de soluciones ciudadanas de mitigación del fraude. Por su parte, **EXPERIAN** propone ampliar el alcance del proyecto para permitir el acceso restringido y estandarizado a alertas técnicas no personales, patrones de riesgo e indicadores de fraude, y su intercambio con los operadores de información, con fundamento en la Ley 1266 de 2008 y en la Ley 2573 de 2026.

La segunda línea, sin oponerse a la existencia del Comité, advierte sobre el riesgo de que sus decisiones se conviertan en un mecanismo de regulación paralela adoptado sin surtir el Análisis de Impacto Normativo (AIN), la publicidad y la participación propios del proceso regulatorio. **ETB** sostiene que el Comité debe circunscribirse a funciones de articulación, análisis técnico y generación de recomendaciones, sin habilitación para introducir obligaciones regulatorias nuevas sin AIN. **CLARO** añade que la propuesta no define con suficiencia el funcionamiento, las competencias ni los mecanismos de decisión del Comité, y advierte que, bajo un esquema de mayoría simple, los asignatarios de código corto de menor tamaño podrían imponer o bloquear medidas que afecten el núcleo de red de los PRSTM, proponiendo que el voto favorable de los PRSTM sea mandatorio cuando la decisión impacte la configuración técnica, el enrutamiento, la señalización o la seguridad perimetral de sus redes. **PTC**, que respalda la creación del Comité, solicita precisiones puntuales sobre la expresión «atención urgente» del artículo 2.1.10.7.3.2, sobre el alcance de la vinculatoriedad del artículo 2.1.10.7.3.4 en relación con la excepción de publicación, y sobre la remisión oficiosa a la SIC o al MinTIC prevista en el parágrafo del artículo 2.1.10.7.3.16, respecto de la cual pide incorporar reglas asociadas al incumplimiento injustificado o atribuible exclusivamente al obligado.

Sobre la fusión del CTS en el CTLFSM

Antes de abordar las dos líneas de comentarios, la Comisión precisa que, como resultado del análisis conjunto de las intervenciones recibidas sobre este Comité y sobre el Comité Técnico de Seguimiento (CTS) previsto en el artículo 6.13.5.1 del proyecto publicado, se suprime el CTS como instancia autónoma y se consolidan la integridad de sus funciones en el CTLFSM, que subsiste como única instancia permanente de coordinación técnica del proyecto. Las razones de esta decisión y su alcance se exponen en el capítulo denominado «Comité Técnico de Seguimiento y coordinación operativa», al que se remite.

En lo que interesa a este capítulo, la fusión implica que el CTLFSM asume, además de las funciones que ya tenía en materia de intercambio de alertas, identificación de patrones de fraude y revisión técnica de las medidas frente al fraude en voz móvil y SMS, el seguimiento a la implementación y operación del régimen de código corto A2P, SENDER ID y plantillas de contenido A2P, y la coordinación de la respuesta del ecosistema frente a incidentes de fraude.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Sobre el diseño del CTLFSM contenido en el proyecto y en el documento soporte

Conviene recordar que el documento soporte concibió el CTLFSM como una instancia permanente de coordinación para el intercambio de alertas, la identificación de patrones de fraude y la actualización técnica de las medidas producto de la mutación del fraude. El proyecto publicado, al modificar el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016, distinguía dos categorías de intervinientes: de una parte, los participantes obligatorios, integrados por los representantes de los PRST (para las temáticas de fraude en voz y SMS, en los ecosistemas P2P y A2P), por los asignatarios del recurso de identificación denominado código corto A2P (para las temáticas del ecosistema A2P) y por la CRC, que preside el Comité y ejerce su secretaría técnica; y de otra parte, los invitados a sesiones específicas.

Sobre esa base, y en atención a los comentarios recibidos, la Comisión ajusta el diseño del Comité en tres dimensiones: la conformación, que pasa a estructurarse en función de la temática de cada sesión; la naturaleza de sus decisiones, que se precisa como recomendación técnica no vinculante; y la periodicidad, que se ordena en una regla única y predecible.

Sobre la ampliación de la participación en el CTLFSM

La Comisión acoge parcialmente los comentarios orientados a fortalecer la participación en el Comité. Comparte la conveniencia de enriquecer el intercambio técnico con la visión de los distintos segmentos del ecosistema y de los sujetos afectados por el fraude, y encuentra que ello es compatible con la naturaleza del CTLFSM como espacio de coordinación e inteligencia compartida. La fusión permite atender esa preocupación mediante una solución estructural: la participación según la temática, prevista en el numeral 2.1.10.7.3.2.

Conforme a esa regla, la CRC cita a cada sesión únicamente a los agentes obligados al cumplimiento de las medidas que constituyan su objeto. Cuando la sesión tenga por objeto la revisión, actualización o mejora de las medidas aplicables al servicio de voz móvil o al tráfico P2P, serán citados con voz y voto los PRST obligados al cumplimiento de tales medidas. Cuando tenga por objeto la revisión técnica, la implementación o la operación del ecosistema A2P, serán citados con voz y voto los Integradores Tecnológicos —en su calidad de asignatarios del recurso de identificación denominado código corto A2P— y los PRSTM, y será citada en todo caso la persona jurídica que opere el validador centralizado, como invitada permanente con voz y sin voto. Y cuando tenga por objeto materias distintas, tales como el intercambio de información, la construcción de estadísticas agregadas o la gestión de alertas de fraude, la CRC citará a los agentes, entidades o autoridades cuya concurrencia resulte pertinente en función de la necesidad que se pretenda abordar.

Con esta solución, la Comisión atiende la solicitud de **NEXVIA** y de **BLIPBLIP** en cuanto a los Integradores Tecnológicos inscritos en el RPCAI: estos agentes no son invitados, sino participantes obligatorios con voz y voto en las sesiones que tengan por objeto el ecosistema A2P, que es precisamente donde se revisan las reglas que los obligan. No se acoge, en cambio, la solicitud de reconocer voto a los PCA que no ostenten la calidad de asignatarios de código corto A2P, quienes podrán

ser citados como invitados con voz y sin voto cuando manifiesten su voluntad de participar y los temas de la agenda así lo ameriten: el derecho de voto se reserva a los destinatarios directos de las obligaciones objeto de la respectiva sesión, y su extensión a un número indeterminado de agentes alteraría el equilibrio del quórum previsto en el numeral 2.1.10.7.3.11.

Se atiende igualmente la solicitud de **INETUM** y de **CLARO** respecto del validador centralizado, cuya citación es obligatoria en toda sesión sobre el ecosistema A2P, con voz y sin voto. La Comisión no le reconoce voto por cuanto el validador es el operador del sistema de validación cuya actuación se sujeta a las obligaciones del Capítulo 13 del TÍTULO VI y a los contratos que suscriba con los agentes; reconocerle voto sobre las reglas que rigen su propia operación introduciría un conflicto de interés que las salvaguardas de gobernanza del proyecto buscan precisamente evitar.

Se acogen, asimismo, las solicitudes de **ASOBANCARIA** y de **SCAMZERO**: el numeral 2.1.10.7.3.2 habilita a la CRC para citar como invitados, con voz y sin voto, a un representante del sector financiero a través de su gremio, a los asignatarios de SENDER ID, a las asociaciones gremiales del sector, a organismos internacionales de referencia y a organizaciones representativas de los usuarios y de la protección al consumidor digital. Asimismo, y con el propósito de fortalecer la articulación institucional en materia de ciberseguridad, se ajusta el numeral 2.1.10.7.3.2 para prever que el COLCERT será invitado a las sesiones del CTLFSM conforme a las temáticas particulares que se sometan a consideración del Comité. La propuesta de **SCAMZERO** sobre unificación de variables y criterios de detección encuentra cauce natural en la función de recomendación de actualización de los parámetros de detección prevista en el numeral 2.1.10.7.3.1.

Sobre el riesgo de «regulación paralela» y la naturaleza de las decisiones del Comité

La Comisión acoge los comentarios de **ETB** y de **CLARO** en esta materia. Coincide con **ETB** en que debe preservarse la diferencia entre la coordinación técnica y el ejercicio de la función regulatoria, y en que el Comité debe ser una instancia de articulación, análisis técnico y recomendación, y no un mecanismo para introducir obligaciones regulatorias nuevas ni para adoptar decisiones vinculantes. En consecuencia, se modifica el numeral 2.1.10.7.3.4 para disponer que las decisiones del CTLFSM tienen, en todos los casos, el carácter de recomendaciones técnicas dirigidas a sus miembros y a la CRC y no constituyen imposiciones regulatorias autónomas adoptadas por vía de acta. Bajo esa redacción: (i) no son vinculantes para la CRC ni afectan sus competencias en materia de regulación; y (ii) no crean, modifican, adicionan, degradan ni derogan obligaciones regulatorias, y en ningún caso pueden desmejorar los parámetros técnicos mínimos del artículo 2.1.10.7 ni las obligaciones del Capítulo 13 del TÍTULO VI.

Cuando la CRC, en ejercicio de su autonomía regulatoria, acoja total o parcialmente una recomendación técnica del Comité, la incorporará al marco regulatorio mediante resolución. En ausencia de recomendaciones acogidas por la CRC, aplican los parámetros y estándares mínimos ya establecidos en la resolución.

La propuesta de **CLARO** de exigir el voto mandatorio y vinculante de los PRSTM para las decisiones que impacten la configuración técnica, el enrutamiento, la señalización o la seguridad perimetral de los núcleos de red no se acoge como cláusula autónoma, por cuanto pierde su objeto con el diseño adoptado. El supuesto que la motivaba —que agentes no operadores de red pudieran imponer, por vía de acta y por mayoría simple, cargas técnicas sobre el núcleo de red de los PRSTM— desaparece por dos vías concurrentes: primera, porque ninguna decisión del Comité es vinculante para agente alguno, de modo que ninguna carga técnica puede nacer del acta; y segunda, porque la regla de participación según la temática garantiza que en toda sesión que verse sobre el ecosistema A2P los PRSTM concurran con voz y voto. A ello se suman la presidencia y la secretaría técnica en cabeza de la CRC y la circunstancia de que la incorporación de cualquier recomendación a la regulación general se efectúa mediante resolución.

Sobre la periodicidad y la convocatoria del Comité

La Comisión considera necesario dotar al Comité de una regla de periodicidad predecible que permita a los agentes planear su participación y preparar la información que deban aportar. En consecuencia, se modifica el numeral 2.1.10.7.3.3 para disponer que el CTLFSM se reunirá ordinariamente dentro de los primeros cinco (5) días hábiles de cada mes, cuando la CRC lo considere necesario y previa convocatoria efectuada con una antelación no inferior a quince (15) días calendario a la fecha de la sesión. Las sesiones podrán ser presenciales o virtuales, según lo determine la CRC en la respectiva convocatoria.
Se conserva la posibilidad de convocar sesiones extraordinarias, en cualquier tiempo y por fuera de dicho término, cuando se presenten incidentes de fraude que requieran atención urgente o cuando las circunstancias del ecosistema así lo demanden, con una antelación no inferior a dos (2) días hábiles. Los agentes obligados podrán solicitar la convocatoria, ordinaria o extraordinaria, exponiendo la temática y su justificación, siendo potestativo de la CRC acceder a la solicitud.

La convocatoria determinará, para cada sesión, la temática a tratar, los participantes obligatorios citados con voz y voto, los invitados citados con voz y sin voto, el orden del día, el requerimiento de la información que cada participante deberá presentar y la documentación que será analizada, y estará disponible en la página web de la CRC. Las actas, por su parte, se conservarán en archivo de libre consulta para los participantes y serán publicadas en la página web de la CRC dentro de los diez (10) días hábiles siguientes a la sesión, salvo la información que tenga carácter confidencial o reservado.

Sobre las precisiones puntuales solicitadas por PTC

Respecto de la expresión «atención urgente», ahora contenida en el numeral 2.1.10.7.3.3, la Comisión precisa que se refiere a incidentes de fraude cuya materialización o inminencia demande una respuesta coordinada e inmediata para prevenir o contener afectaciones al ecosistema o a los usuarios, sin que resulte procedente ni conveniente enumerar taxativamente tales circunstancias, dada la evolución permanente de las modalidades de fraude. Se confirma que, conforme al mismo numeral, los agentes obligados pueden solicitar a la CRC la convocatoria a sesión extraordinaria, siendo potestativo de la Comisión acceder a ella.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En cuanto a la solicitud de **PTC** de incorporar reglas sobre el incumplimiento injustificado o atribuible exclusivamente al obligado, la Comisión la acoge parcialmente. El numeral 2.1.10.7.3.16 circunscribe expresamente el traslado a las entidades de control y vigilancia al incumplimiento injustificado del deber de concurrir a las sesiones para las que el agente haya sido citado como participante obligatorio, de modo que la existencia de una causa que justifique la inasistencia excluye la remisión. Respecto de la remisión oficiosa a la SIC o al MinTIC prevista en el parágrafo del artículo 2.1.10.7, la Comisión precisa que opera frente a presuntos incumplimientos de las obligaciones de dicho artículo y se surte en ejercicio de las competencias de la Comisión, sin que ello prejuzgue sobre la existencia del incumplimiento ni sobre su carácter justificado, valoración que corresponde a la autoridad competente en el marco de la actuación administrativa respectiva.

Sobre la propuesta de EXPERIAN de intercambio de información con operadores de información

La Comisión no acoge la solicitud de **EXPERIAN** de ampliar el alcance del proyecto para habilitar, en el marco del CTLFSM, el intercambio de alertas, patrones e indicadores de fraude con los operadores de información. Dicha propuesta excede el objeto del presente proyecto regulatorio y la finalidad del Comité, y se inscribe en un régimen distinto —el de administración de datos personales de contenido crediticio y financiero— que cuenta con su propio marco normativo y con autoridades competentes específicas. Adicionalmente, el numeral 2.1.10.7.3.5 dispone que en el marco del CTLFSM no se compartirá información comercialmente sensible entre competidores ni información que contenga datos personales de los usuarios, lo que resultaría incompatible con el intercambio propuesto. Sin perjuicio de lo anterior, la articulación con otras autoridades e instrumentos legales podrá canalizarse a través de la citación de entidades y autoridades prevista en el numeral 2.1.10.7.3.2.

4 Sobre las temáticas enfocadas en la educación de la ciudadanía

ANDESCO

Objeta la obligación de que los PRST modifiquen sus contratos con entidades del sector financiero para incorporar deberes de la regulación, pues la obligación de registrar o reportar la información recae directamente sobre la entidad financiera, titular de la relación con el usuario y sujeto obligado; considera que no es razonable exigir a los PRST gestionar modificaciones contractuales con terceros para asegurar el cumplimiento de obligaciones que no les corresponden, y que ello, ante la ausencia de facultades de la CRC sobre las entidades financieras, traslada a los PRST responsabilidades de imposible o difícil cumplimiento.

ANDI

Pide que las campañas pedagógicas incorporen enfoques diferenciales para las poblaciones más expuestas o vulnerables (adultos mayores, personas con menor alfabetización digital y personas con discapacidad), con lenguaje claro, formatos accesibles y canales adecuados, pues la prevención requiere que los usuarios identifiquen señales de alerta, reconozcan los canales oficiales y sepan reportar. Advierte, además, riesgos no intencionados desde la perspectiva del usuario final —pérdida de acceso a servicios financieros por fallas en la recepción de códigos de autenticación, dificultad para distinguir comunicaciones legítimas de fraudulentas ante etiquetado inconsistente y disminución de la confianza en los canales oficiales— que podrían empujar a los usuarios a canales alternativos no seguros.

ASOBANCARIA

Describe que el Capítulo 14 crea obligaciones para los asignatarios de recursos de identificación y los PRST que contratan con entidades financieras (registrar códigos cortos, SENDER ID y numeración en un portal público de la CRC y apoyar campañas de prevención), y pide precisar si esas responsabilidades contractuales recaen directamente sobre ellos cuando actúan como PCA o IT, incluida la obligación de mantener actualizado en tiempo real el listado de las líneas de sus call centers propios o tercerizados y de sus canales de SMS. Reitera la conveniencia de incorporar enfoques diferenciales para las poblaciones vulnerables en las campañas pedagógicas.

CLARO

Considera improcedente que la regulación traslade a los PRSTM la obligación de modificar sus contratos con entidades financieras para incorporar deberes que corresponden a estas, en su calidad de titulares de la relación con el usuario y sujetos obligados. Sostiene que, por eficiencia regulatoria, cualquier obligación de inscripción o actualización de información ante la CRC debe exigirse directamente a las entidades financieras, evitando cargas innecesarias e intermediarios regulatorios ajenos a la relación jurídica que da origen a la obligación, so pena de generar complejidades, costos y riesgos de incumplimiento atribuibles a factores ajenos a los PRSTM.

COLOMBIA FINTECH

Observa que la obligación de reporte trimestral del cumplimiento de los programas de formación (artículo 6.14.1.5) se dirige a los asignatarios de recursos y a los PRST, y pide aclarar si aplica directamente a las entidades financieras que usan mensajería A2P sin ser asignatarias directas o si recae en el integrador o en el asignatario del código corto, precisando la cadena de responsabilidad cuando la entidad financiera es asignataria de SENDER ID pero no de código corto A2P. Advierte que la obligación de publicar cuatro campañas anuales en redes sociales con el hashtag de la CRC puede entrar en tensión con los lineamientos de comunicación digital que la SFC impone a las entidades vigiladas, por lo que pide aclarar la articulación y la posibilidad de un cumplimiento conjunto, delegado o alternativo. Adicionalmente, propone que los PRST y los asignatarios de código corto incorporen en sus sistemas de atención un mecanismo estandarizado de reporte de fraude por los propios usuarios (por

ejemplo, una opción de «reportar mensaje fraudulento» desde el SMS o por USSD) que alimente al CTLFSM.

SAEM

Advierte que la suma de obligaciones —al menos cuatro campañas pedagógicas anuales (6.14.1.3), cuatro sesiones anuales de formación interna con reporte trimestral (6.14.1.5) y reportes de información (Formato T.5.9, artículo 17)— representa para un IT mediano una carga administrativa fija desproporcionada frente a su aporte marginal a la prevención, dado que no tiene relación directa con el usuario final. Propone aplicar proporcionalidad por tamaño y por relación con el usuario (que las campañas masivas recaigan sobre PRST y PCA con relación directa y que el IT pueda cumplir difundiendo el micrositio de la CRC), pasar a una periodicidad anual o semestral en lugar de trimestral, y unificar los formatos de reporte para evitar duplicidades entre validador, IT y PRST.

SCAMZERO

Sostiene que las campañas educativas por sí solas son insuficientes —el smishing multiplicó por nueve sus reclamaciones en un año— y que el obstáculo real es la falta de herramientas de verificación en tiempo real, por lo que propone que las medidas pedagógicas incluyan la divulgación de herramientas de verificación de enlaces, mensajes y números disponibles en el mercado, bajo neutralidad tecnológica.

TIGO

Considera que fijar criterios mínimos trimestre a trimestre sobre contenido, alcance y medios genera rigideces, y que sería más efectivo que la CRC establezca lineamientos generales y permanentes que cada agente adopte con flexibilidad (guías, ejemplos reales anonimizados, alertas sobre modalidades emergentes y mensajes de autocuidado), favoreciendo la innovación y la comparación de campañas. Respecto de la formación interna (artículo 6.14.1.5), señala que la efectividad no es proporcional al número de sesiones, sino a su calidad y apropiación, y sugiere reducir la periodicidad de cuatro a un mínimo de dos sesiones al año (una por semestre), manteniendo los contenidos definidos por la Comisión y complementándolas con divulgación continua cuando surjan nuevas amenazas.

PTC

Advierte que la obligación de realizar al menos cuatro campañas pedagógicas difundidas en redes y páginas web puede resultar subjetiva en cuanto a cuándo se entiende cumplida, dado el nivel de detalle que exige el artículo 6.14.1.3, por lo que sugiere que la CRC fije un modelo estándar de contenido cuya publicación tenga por cumplida la obligación y elimine interpretaciones subjetivas. Pide, además, que entidades como el MinTIC adelanten asistencia especial para los grupos con baja alfabetización digital, en línea con el artículo 12 de la Ley 2573 de 2026. Considera razonable la formación interna trimestral, pero solicita aclarar qué se entiende por «cobertura por área funcional», si se creará un formato y un

canal específicos para el reporte, y que la obligación del artículo 6.14.1.5 sea exigible a partir del trimestre siguiente a la entrada en vigencia de la norma.

Respuesta CRC:

Sobre esta temática se pronunciaron **ANDESCO**, **ANDI**, **ASOBANCARIA**, **COLOMBIA FINTECH**, **CLARO**, **SAEM**, **SCAMZERO**, **TIGO** y **PTC**. Revisadas las intervenciones, la Comisión identifica cinco tendencias: (i) los cuestionamientos a las obligaciones de modificación contractual con las entidades del sector financiero previstas en los artículos 6.14.2.2 y 6.14.3.1 (**ANDESCO**, **ASOBANCARIA** y **CLARO**); (ii) las solicitudes de enfoque diferencial y de mejoras al contenido de las campañas pedagógicas (**ANDI**, **ASOBANCARIA**, **SCAMZERO** y **PTC**); (iii) las solicitudes de flexibilización de la periodicidad y de la forma de acreditación de las campañas y de la formación interna (**TIGO**, **SAEM**, **PTC** y **COLOMBIA FINTECH**); (iv) las solicitudes de precisión sobre la cadena de responsabilidad y la articulación con el régimen de las entidades vigiladas por la Superintendencia Financiera (**COLOMBIA FINTECH**); y (v) la propuesta de mecanismos de reporte de fraude por parte de los usuarios (**COLOMBIA FINTECH**). A continuación, la Comisión responde cada tendencia.

Sobre las obligaciones de modificación contractual con entidades del sector financiero (artículos 6.14.2.2 y 6.14.3.1)

ANDESCO sostiene que la obligación de registrar o reportar la información de contacto recae directamente sobre la entidad financiera, en su calidad de titular de la relación con el usuario, y que no resulta razonable ni jurídicamente adecuado exigir a los asignatarios y a los PRST gestionar modificaciones contractuales con terceros para asegurar el cumplimiento de obligaciones que no les corresponden, configurando obligaciones de imposible o difícil cumplimiento, en tanto la CRC carece de facultades para imponer deberes a las entidades financieras. En sentido similar se pronunció **CLARO**. Por su parte, **ASOBANCARIA** describe el alcance de la medida y sugiere precisar las responsabilidades contractuales de los asignatarios y de los PRST, incluyendo la actualización en tiempo real del listado de líneas de call centers y canales de SMS.

En el documento soporte, la Comisión justificó los artículos 6.14.2.2 y 6.14.3.1 en la conveniencia de que los ciudadanos pudieran verificar, a través de un portal de consulta pública, si un código corto, un SENDER ID o una numeración E.164 que los contacta corresponde efectivamente a una entidad financiera legítima, como mecanismo pedagógico y de verificación complementario a las medidas técnicas del proyecto.

Analizados los comentarios, la Comisión los acepta y, en consecuencia, elimina de la resolución los artículos 6.14.2.2 y 6.14.3.1, por las siguientes razones. En primer lugar, respecto del artículo 6.14.2.2, las medidas adoptadas en el ecosistema SMS A2P, en particular, la creación del SENDER ID como recurso de identificación asociado al responsable del contenido, el proceso de conocimiento del cliente (KYC), el registro de plantillas y la trazabilidad de extremo a extremo del tráfico, ya permitirán identificar con claridad y de manera verificable a los generadores de contenido del sector financiero, de modo que

la finalidad de verificación de la legitimidad del remitente que perseguía la inscripción contractual queda satisfecha por el propio diseño del régimen, sin necesidad de una capa adicional de registro. En segundo lugar, respecto del artículo 6.14.3.1, las medidas de etiquetado de llamadas con fines publicitarios y el registro de numeración asociado a dicho esquema ya permitirán que las entidades financieras reporten la numeración desde la cual contactan a sus usuarios, cumpliendo la misma finalidad de identificación y verificación en el canal de voz. En tercer lugar, mantener ambas disposiciones generaría una duplicidad de esfuerzos y de cargas (contractuales, operativas y de reporte) sobre los asignatarios, los PRST y las propias entidades financieras, en contravía del principio de simplificación regulatoria previsto en el artículo 19 de la Ley 1341 de 2009, modificado por el artículo 15 de la Ley 1978 de 2019, que orienta el presente proyecto. Finalmente, la eliminación resuelve de raíz la objeción de **ANDESCO** sobre la estructura de la obligación, pues desaparece el deber de gestionar modificaciones contractuales cuyo cumplimiento dependía de la conducta de terceros no sujetos a la regulación de esta Comisión.

Para introducir este cambio, se suprimirán los artículos 6.14.2.2 y 6.14.3.1 del texto del Capítulo 14 propuesto, se elimina la Sección 3 (Medidas pedagógicas específicas para voz), que quedaría sin contenido, y se ajustará la numeración interna de la Sección 2, así como las remisiones cruzadas del articulado y del régimen de transición que refieran a dichas disposiciones. Como consecuencia de esta decisión, las observaciones de **ASOBANCARIA** y de otros agentes sobre el alcance, la actualización y los riesgos de la inscripción pública de identificadores pierden objeto y no requieren pronunciamiento adicional.

Sobre el enfoque diferencial y el contenido de las campañas pedagógicas

La **ANDI** y **ASOBANCARIA** solicitan que las campañas pedagógicas incorporen enfoques diferenciales para las poblaciones más expuestas o vulnerables (adultos mayores, personas con menor alfabetización digital y personas con discapacidad), con lenguaje claro, formatos accesibles y canales adecuados para cada población objetivo. La **ANDI** añade que deben mitigarse los riesgos no intencionados sobre el usuario final, como la pérdida de acceso a servicios por fallas en la recepción de códigos de autenticación o la confusión derivada de un etiquetado inconsistente. **SCAMZERO** propone que las medidas pedagógicas incluyan la divulgación de herramientas de verificación disponibles en el mercado para enlaces, mensajes y números, bajo un enfoque de neutralidad tecnológica y sin favorecer una herramienta específica. **PTC** solicita que el MinTIC adelante asistencia especial para grupos con bajos índices de alfabetización digital.

Sobre el particular, la Comisión precisa que el enfoque diferencial solicitado por la **ANDI** y **ASOBANCARIA** ya se encuentra expresamente incorporado en el inciso segundo del artículo 6.14.1.3 propuesto, conforme al cual las campañas «deben tener un enfoque diferencial para usuarios en condición de vulnerabilidad, incluyendo adultos mayores, usuarios con bajos niveles de alfabetización digital y usuarios en zonas con menor acceso a servicios digitales». En consecuencia, se acepta el comentario en el sentido de que su finalidad ya está recogida en el articulado, y la Comisión lo complementará incluyendo de manera expresa a las personas con discapacidad dentro de los grupos

que exigen enfoque diferencial, así como la referencia a la utilización de lenguaje claro y formatos accesibles, ajuste que se introduce en el mismo inciso segundo del artículo 6.14.1.3.

En cuanto a la propuesta de **SCAMZERO**, la Comisión la acepta por encontrarla técnicamente razonable y de bajo costo de implementación: la divulgación de la existencia de herramientas de verificación de enlaces, mensajes y números fortalece la capacidad de autoprotección del usuario, que es precisamente la finalidad del eje pedagógico, y su formulación bajo neutralidad tecnológica evita cualquier favorecimiento comercial. El cambio se introduce adicionando, en el inciso segundo del artículo 6.14.1.3, dentro del contenido mínimo de las campañas, la divulgación de la existencia de herramientas y mecanismos de verificación de mensajes, enlaces y números disponibles para los usuarios, sin promover proveedores o soluciones específicas.

Frente a los riesgos no intencionados señalados por la **ANDI**, la Comisión advierte que estos se predican de medidas específicas del proyecto (continuidad de mensajes de autenticación y consistencia del etiquetado) que fueron abordadas en los capítulos denominados «Tratamiento de mensajes OTP, autenticación, seguridad y comunicaciones críticas », «Bloqueo o etiquetado de mensajes» y «Monitoreo de llamadas que derivan en la etiqueta de Alerta de llamada sospechosa», a los cuales se remite. Finalmente, en cuanto a la solicitud de **PTC** relativa a la asistencia del MinTIC, la Comisión comparte la conveniencia de la articulación pedagógica interinstitucional, la cual se canaliza a través de los espacios previstos en el artículo 6.14.1.4 propuesto, que contemplan la participación del MinTIC; no obstante, no es procedente incorporar en la resolución mandatos dirigidos a dicho Ministerio, por carecer la CRC de competencia para imponer una obligación en tal sentido a dicha autoridad.

Sobre la periodicidad, la forma de acreditación y la proporcionalidad de las campañas y de la formación interna

TIGO considera que el establecimiento de criterios mínimos trimestre a trimestre genera rigideces innecesarias y propone que la CRC expida lineamientos generales y orientadores de carácter permanente; asimismo, solicita reducir la periodicidad mínima de la formación interna de cuatro a dos sesiones anuales, argumentando que la efectividad de la formación depende de su calidad y pertinencia y no del número de sesiones. **SAEM** solicita aplicar proporcionalidad por tamaño y por relación con el usuario final, de modo que las campañas masivas recaigan principalmente sobre los PRST y los PCA con relación directa con el usuario y que el IT pueda cumplir mediante la difusión del micrositio de la CRC, así como periodicidad anual o semestral para la formación y los reportes, y formatos unificados que eviten duplicidades. **PTC** estima razonable la obligación de formación interna, pero solicita que la CRC fije un modelo estándar de contenido para las campañas que elimine la subjetividad en la verificación del cumplimiento, que aclare la expresión «cobertura por área funcional», que indique si existirá un formato y un canal específico para la remisión de los reportes, y que la obligación sea exigible a partir del trimestre siguiente a la entrada en vigencia de la norma. **COLOMBIA FINTECH** solicita incorporar reportes periódicos de desempeño con indicadores mínimos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En el documento soporte, la Comisión justificó las medidas pedagógicas en la causa del problema asociada al desconocimiento de los usuarios sobre las modalidades de ataque y las acciones de prevención, y diseñó las obligaciones de los artículos 6.14.1.3 y 6.14.1.5 con periodicidad trimestral y acreditación documental ante la CRC.

Evaluados los comentarios, la Comisión encuentra que varios de ellos tienen sentido lógico, técnico y económico, en tanto permiten alcanzar la misma finalidad pedagógica con menores cargas administrativas y mayor seguridad jurídica sobre la forma de acreditar el cumplimiento, en línea con el principio de simplificación regulatoria del artículo 19 de la Ley 1341 de 2009. En consecuencia, se aceptan parcialmente, con el siguiente alcance:

Primero, se acepta la solicitud de **TIGO** y **SAEM** de reducir la periodicidad mínima de la formación interna prevista en el artículo 6.14.1.5, que pasará de cuatro sesiones anuales a dos sesiones anuales, una por cada semestre calendario, manteniendo la obligación de cubrir los contenidos definidos por la Comisión. Correlativamente, el reporte de acreditación pasará de trimestral a semestral, y deberá remitirse dentro de los quince (15) días hábiles siguientes a la finalización de cada semestre. La Comisión coincide en que la efectividad de la formación depende de la calidad, pertinencia y actualización de los contenidos más que de la frecuencia de las sesiones, y en que dos jornadas anuales estructuradas, complementadas con divulgación interna ante amenazas emergentes, permiten cubrir integralmente los contenidos exigidos con una carga administrativa proporcionada.

Segundo, se acepta la solicitud de **TIGO** en el sentido de que los criterios que expida la CRC mediante circular conforme al inciso tercero del artículo 6.14.1.3 tendrán el carácter de lineamientos generales y orientadores de carácter permanente, actualizables cuando las modalidades de fraude o la evidencia disponible lo ameriten, en lugar de criterios definidos trimestre a trimestre. Este ajuste preserva la flexibilidad para innovar en las estrategias de comunicación y focaliza la verificación en la efectividad de los mensajes, tal como lo propone el agente. Para introducir el cambio, se ajusta la redacción del inciso tercero del artículo 6.14.1.3 en el sentido indicado.

Tercero, se acepta la solicitud de **PTC** de dotar de objetividad la verificación del cumplimiento. En la circular a que refiere el artículo 6.14.1.3, la CRC incluirá un modelo estándar de contenidos mínimos cuya publicación permitirá tener por cumplida la obligación en su componente de contenido, sin perjuicio de que los agentes puedan desarrollar contenidos adicionales. En la misma línea, y respecto del artículo 6.14.1.5, la circular precisará el alcance de la expresión «cobertura por área funcional» —entendida como la indicación de las áreas o dependencias de la organización cuyos equipos fueron capacitados— y definirá el formato y el canal de remisión de los reportes de acreditación. Estos ajustes no requieren modificación del articulado, pues el propio proyecto defirió a la circular la definición de los criterios de cumplimiento; no obstante, para mayor claridad, se ajusta el inciso tercero del artículo 6.14.1.3 y el inciso final del artículo 6.14.1.5 para señalar expresamente que la circular contendrá el modelo estándar de contenidos, el formato y el canal de reporte.

Cuarto, se acepta la solicitud de **PTC** sobre la exigibilidad de las obligaciones pedagógicas: tanto la obligación de campañas del artículo 6.14.1.3 como la de formación del artículo 6.14.1.5 serán exigibles a partir del primer período completo —trimestre o semestre calendario, según corresponda— siguiente a la entrada en vigencia de la respectiva disposición, lo cual permite a los agentes estructurar sus planes de trabajo y contenidos. El ajuste se introduce en la regla de exigibilidad de los artículos mencionados, en armonía con el artículo de vigencias de la resolución.

Quinto, se acepta parcialmente la solicitud de **SAEM** sobre proporcionalidad por relación con el usuario final. En consecuencia, se precisará en el artículo 6.14.1.3 que los asignatarios cuya actividad no comporte relación directa con usuarios finales podrán cumplir la obligación mediante la difusión, en sus redes sociales, páginas web y canales de relacionamiento con sus clientes, de los contenidos oficiales elaborados por la CRC y de los materiales del micrositio institucional, conservando el deber de acreditación. No se acepta, en cambio, trasladar la periodicidad de las campañas a un esquema anual, pues la naturaleza dinámica de las modalidades de fraude exige presencia pedagógica sostenida a lo largo del año, y la carga asociada queda sustancialmente mitigada con la habilitación del cumplimiento mediante contenidos oficiales.

Sobre la cadena de responsabilidad y la articulación con el régimen de las entidades vigiladas por la Superintendencia Financiera

COLOMBIA FINTECH solicita precisar si la obligación de formación y reporte del artículo 6.14.1.5 aplica directamente a las entidades financieras que usan mensajería A2P sin ser asignatarias de código corto, o si recae en el integrador tecnológico o en el asignatario del código corto, particularmente cuando la entidad financiera es asignataria de SENDER ID. Asimismo, plantea que la obligación de publicar campañas en redes sociales con el hashtag oficial de la CRC puede entrar en tensión con los lineamientos de comunicación digital que la Superintendencia Financiera impone a sus vigiladas, y solicita aclarar la articulación o habilitar mecanismos de cumplimiento conjunto o delegado.

La Comisión acepta la solicitud de precisión y aclara la cadena de responsabilidad en los siguientes términos: las obligaciones de los artículos 6.14.1.3 y 6.14.1.5 recaen sobre los asignatarios de recursos de identificación que hagan parte del ecosistema A2P y sobre los PRST, cada uno respecto de su propia organización y canales. En consecuencia, la entidad que sea asignataria de un SENDER ID es destinataria directa de las obligaciones en su condición de asignataria de un recurso de identificación, sin que dicha carga se traslade ni se delegue en el asignatario del código corto A2P ni en el integrador tecnológico, cuyas obligaciones son propias e independientes. Para eliminar cualquier ambigüedad, se ajustará la redacción de los artículos 6.14.1.3 y 6.14.1.5 para señalar que cada agente obligado responde por el cumplimiento respecto de su propia organización, canales y equipos de trabajo.

En cuanto a la alegada tensión con los lineamientos de la Superintendencia Financiera, la Comisión no encuentra configurado un conflicto normativo: las campañas pedagógicas de prevención del fraude no constituyen publicidad de productos o servicios financieros, sino información de interés general para la protección de los usuarios, y su difusión se realiza en los canales propios del agente conforme a su

régimen aplicable. En todo caso, los lineamientos generales que la CRC expida mediante circular considerarán las particularidades de los agentes sujetos a regímenes sectoriales de comunicación, y la habilitación de cumplimiento mediante los contenidos oficiales de la CRC ofrece a estas entidades una vía de cumplimiento estandarizada que minimiza cualquier riesgo de interpretación frente a su supervisor. Con este alcance, se acepta parcialmente el comentario.

Sobre los mecanismos de reporte de fraude por parte de los usuarios

COLOMBIA FINTECH solicita establecer una obligación complementaria consistente en que los PRST y los asignatarios de código corto A2P incorporen en sus sistemas de atención un mecanismo estandarizado de reporte de fraude por parte de los usuarios —por ejemplo, una opción de reporte accesible desde el propio SMS o mediante un canal USSD—, cuyos datos alimenten el CTLFSM como insumo de inteligencia.

La Comisión valora la propuesta, cuya finalidad comparte: la retroalimentación proveniente de los usuarios constituye un insumo relevante de inteligencia antifraude. No obstante, no se acepta su incorporación como obligación en el articulado, por tres razones. Primero, la definición técnica de un mecanismo estandarizado de reporte —canal, formato, integración con los sistemas de monitoreo y con las listas compartidas— exige un nivel de detalle operativo y de coordinación entre agentes que no es propio del articulado de la resolución, sino del trabajo técnico del ecosistema. Segundo, imponer en esta instancia una obligación no sometida a consideración del sector en el proyecto publicado desbordaría el objeto de la presente actuación. Tercero, y principalmente, el diseño institucional del proyecto ya contempla el escenario natural para desarrollar esta propuesta: el CTLFSM tiene dentro de sus funciones la coordinación operativa y la definición de mecanismos de intercambio de información e inteligencia sobre el fraude, de modo que la estandarización de los canales de reporte ciudadano podrá ser evaluada y adoptada en dicha instancia, con la participación de los agentes obligados. La Comisión llevará la propuesta a consideración del CTLFSM una vez este se instale.

5 Sobre las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

5.1 Consecuencia para reincidentes

ALDEAMO

Advierte que permitir a los operadores móviles suspender o terminar la relación de acceso con una empresa (artículo 6.1.1.8) ignora que ellos también venden soluciones basadas en mensajería de texto, de modo que el operador actuaría como juez y parte, con la consiguiente preocupación por el mantenimiento de condiciones de competencia justa.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

ASOBANCARIA

Señala que la recuperación de códigos cortos y la eventual desconexión pueden afectar a terceros (clientes finales) y la continuidad de servicios financieros, por lo que sugiere esquemas de transición reforzada para servicios críticos, la notificación previa a los usuarios en casos relevantes y la coordinación con la SFC cuando se afecten servicios financieros.

Advierte que el artículo 8 faculta a la CRC a suspender preventivamente un código corto hasta por seis meses y a los operadores a suspender por un mes la relación con un PCA/IT ante dos recuperaciones y a iniciar la desconexión definitiva ante la tercera, con impacto colateral sobre entidades financieras ajenas a la conducta si su proveedor de mensajería incurre en malas prácticas con otros clientes; por ello pide una alternativa que garantice que la suspensión del código corto no afecte a la entidad financiera ajena a la conducta sancionada.

BLIPBLIP, NEXVIA e INALAMBRIA

Consideran que el Parágrafo 4 del artículo 6.1.1.8 —que autoriza al PRST a suspender por un mes la relación de acceso ante la segunda recuperación y a solicitar la terminación definitiva ante la tercera— es la disposición de mayor gravedad del proyecto, por cuanto: (i) constituye una sanción sin debido proceso, ya que priva al agente de su capacidad operativa e inflige un daño reputacional y económico irreversible sin procedimiento previo de defensa; (ii) delega el poder coercitivo del Estado en un competidor, pues el PRST es a la vez titular de la instalación esencial, asignatario de códigos cortos y competidor en el mercado A2P; (iii) instaura una regla de «tres strikes» activable con quejas mal intencionadas, que bastarían para desconectar a un integrador del que dependen miles de empresas; (iv) penaliza automáticamente ignorando que se puede cumplir la regulación y aun así el fraude encuentra caminos nuevos, por lo que la recuperación no debería operar de manera automática sino solo cuando, con debido proceso, se demuestre negligencia o incumplimiento imputable; y (v) duplica innecesariamente una potestad estatal, pues la CRC ya conserva la facultad de suspender preventivamente el recurso.

INALAMBRIA

Sostiene que la recuperación de códigos cortos ha operado sobre distintos tipos de asignatarios, incluidos los PRST (cita la Resolución CRC 8218 de 2026 sobre el código 85377 de Movistar, la Resolución 8190 sobre el código 55100 de Partners Telecom y la Resolución 8199 de 2026 sobre Colombia Móvil, esta última no disponible en la página de la CRC), por lo que concluye que la recuperación es un instrumento inefectivo para cambiar la conducta y que no es razonable construir un esquema que imponga cargas extraordinarias a los IT bajo la premisa de que son el principal foco de riesgo mientras se asume a los PRST inmunes, lo que generaría un trato diferenciado injustificado. Pide incorporar en la memoria justificativa y el análisis de impacto un estudio comparativo de las recuperaciones de los últimos años que identifique el tipo de asignatario, las condiciones técnicas y el porcentaje atribuible a

IT, PCA y PRST, así como el porcentaje de SMS maliciosos sobre el tráfico total, advirtiendo que, sin esa evidencia, la regulación se fundaría en una presunción generalizada de riesgo contra los IT no soportada en datos.

NEXVIA

Reitera que el Parágrafo 4 del artículo 6.1.1.8 es innecesario conforme al test de proporcionalidad (Sentencia C-022 de 1996), pues la CRC ya conserva en el Parágrafo 3 la facultad de suspender preventivamente el recurso, de modo que duplicarla en un privado interesado solo añade un instrumento de exclusión comercial. Advierte que, combinada con la unicidad del artículo 6.4.1.4, la medida produce la desaparición operativa de una empresa de un momento a otro —al recuperarse el código único se invalidan de forma masiva y automática todos los SENDER ID vinculados— y que, como la reconexión con un operador puede tardar más de un año, la suspensión de treinta días equivale a una «muerte súbita» empresarial.

Objeta la asimetría a favor del duopolio (tras la integración Tigo–Movistar) y sostiene que el proyecto contradice la Resolución CRC 8144 de 2026, que corrige asimetrías, al amplificarlas. Respecto del numeral 4.1.2.6.5, denuncia un doble estándar indeterminado («medidas suficientes» y «medidas necesarias para demostrar que no volverá a incurrir») cuya calificación inicial corresponde al PRST competidor, con inversión de la carga de la prueba en contra del solicitante (prueba de un hecho negativo indefinido), en tensión con los artículos 29, 334 y 365 de la Constitución y con la doctrina de instalaciones esenciales. Añade objeciones a otras causales: la del numeral 6.12.3.2.6 (envío en nombre de terceros), que sumada a la exigencia de NIT o sucursal eliminaría el modelo de agregación de la mensajería internacional y suprimiría los OTP internacionales; la del numeral 6.12.3.2.7, que debe armonizarse con el RNE y excluir el tráfico transaccional amparado por el vínculo servicio-usuario, exigiendo dolo o reiteración verificada; y la del numeral 6.12.3.2.11, que haría recaer sobre el asignatario una decisión sobrevenida del Administrador (responsabilidad objetiva), por lo que debe operar hacia futuro con un régimen de transición. Frente al numeral 6.13.4.7.2 pide que la regla general sea el etiquetado y el bloqueo la excepción reglada reservada al fraude identificado, y frente al numeral 6.13.4.7.4 que la suspensión provenga de un acto administrativo motivado y notificado de la CRC.

SAEM

Afirma que la suspensión unilateral del acceso por el PRST —que puede ser competidor del IT— sin control previo de la CRC, y las causales de oposición, otorgan al PRST una herramienta con potencial anticompetitivo que afecta la estabilidad de la interconexión, insumo esencial del IT. Propone que toda suspensión o desconexión esté precedida de control de la CRC y del debido proceso, con oportunidad de descargos; que la suspensión unilateral solo proceda ante riesgo grave e inminente acreditado y por el tiempo estrictamente necesario; y que las causales de oposición se interpreten de forma restrictiva y temporal, con la carga de la prueba a cargo del PRST que se opone.

SINCH

Sostiene que empoderar a los operadores para suspender o terminar los contratos con integradores reincidentes descentraliza la vigilancia y obliga a los integradores a ejercer un control estricto sobre sus propios clientes, creando una cadena de custodia digital, con los riesgos y cargas que ello implica.

Respuesta CRC:

Sobre esta temática se pronunciaron **ALDEAMO**, **ASOBANCARIA**, **INALAMBRIA**, **NEXVIA**, **SAEM**, **SINCH** y, de manera conjunta, **BLIPBLIP**, **NEXVIA** e **INALAMBRIA**. Revisadas las intervenciones, la Comisión identifica una tendencia claramente convergente en la objeción al Parágrafo 4 del artículo 6.1.1.8 propuesto, en cuanto faculta a los PRST para suspender unilateralmente, por un mes, la relación de acceso con el PCA/IT al que la CRC le haya recuperado por segunda vez un código corto por las causales de los numerales 6.4.3.2.2, 6.4.3.2.8 y 6.4.3.2.9. Los agentes coinciden en que dicha facultad: (i) constituye materialmente una sanción impuesta sin procedimiento previo que garantice el derecho de defensa; (ii) configura una delegación de poder coercitivo en un particular que es, simultáneamente, titular de la instalación esencial, asignatario de códigos cortos y competidor directo en el mercado A2P, generando un escenario de juez y parte con potencial anticompetitivo (**ALDEAMO**, **INALAMBRIA**, **NEXVIA**, **SAEM**, **SINCH** y el escrito conjunto); (iii) resulta innecesaria conforme al test de proporcionalidad, pues la propia CRC conserva la facultad de suspensión preventiva del recurso; y (iv) puede producir efectos desproporcionados sobre terceros ajenos a la conducta (entidades financieras, prestadores de salud y usuarios finales) cuyas comunicaciones dependen del agente suspendido (**ASOBANCARIA**, **NEXVIA**). Como tendencias complementarias, **INALAMBRIA** propone que toda suspensión permanezca en cabeza de la CRC mediante un procedimiento sumario con decisión en veinticuatro horas; **SAEM** solicita que toda suspensión o desconexión esté precedida de control de la CRC y del debido proceso, con interpretación restrictiva de las causales de oposición; **SINCH** solicita umbrales de tolerancia de quejas, espacios de discusión previa y procedimientos ágiles de reactivación; e **INALAMBRIA** y **NEXVIA** cuestionan la asimetría del régimen frente a los PRST, quienes también son asignatarios de códigos cortos y también han sido objeto de recuperaciones.

En el documento soporte, la Comisión justificó la medida señalando que la recuperación de un código corto puntual puede resultar insuficiente cuando el PCA/IT puede continuar cursando tráfico riesgoso a través de otros códigos dentro de la misma relación de acceso, que la suspensión operaría como mecanismo de contención e incentivo de correctivos, que la medida se apoya en un criterio objetivo y verificable (la segunda y tercera recuperación por causales asociadas a uso indebido), y que la terminación definitiva no se activa automáticamente sino que exige autorización de la CRC, lo que introduce un control efectivo contra la arbitrariedad.

Evaluados los comentarios, la Comisión los acepta parcialmente, en los términos que siguen.

En primer lugar, la Comisión acepta la objeción central y, en consecuencia, elimina del Parágrafo 4 del artículo 6.1.1.8 la facultad de los PRST de suspender unilateralmente, por un mes, la relación de acceso con el PCA/IT ante la segunda recuperación de un código corto. La Comisión reconoce que, si bien la

medida se apoyaba en un supuesto objetivo (la segunda recuperación decretada por la propia CRC), su ejecución quedaba en cabeza de un agente privado que concurre al mercado A2P como competidor de los destinatarios de la medida, y que sus efectos materiales (la interrupción total de la capacidad operativa del agente durante un mes) son de tal intensidad que exigen las garantías propias de una actuación administrativa: contradicción previa, decisión motivada de autoridad y recursos. La supresión de esta facultad restablece plenamente la coherencia del régimen con los derechos fundamentales al debido proceso y a la defensa consagrados en el artículo 29 de la Constitución Política, elimina el riesgo señalado de instrumentalización anticompetitiva de la relación de acceso y despeja la preocupación por los efectos colaterales inmediatos sobre terceros de buena fe, en tanto ninguna interrupción de la relación de acceso podrá producirse por decisión unilateral de un particular. Con esta supresión quedan igualmente atendidas las solicitudes de **SAEM** e **INALAMBRIA** de someter toda medida restrictiva al control previo de la CRC, y pierde objeto la propuesta de **INALAMBRIA** de un procedimiento sumario de veinticuatro horas para validar suspensiones de origen privado.

En segundo lugar, la Comisión mantiene la segunda parte del Parágrafo 4, esto es, la posibilidad de que, ante la tercera recuperación de un código corto por las causales indicadas, el PRST solicite a la CRC la autorización para la terminación definitiva de la relación de acceso, decisión que solo podrá adoptarse por esta Comisión en el marco de un trámite administrativo. La Comisión considera que esta medida, así depurada, supera el juicio de proporcionalidad por las siguientes razones. Es idónea, porque interrumpe la continuidad del riesgo frente a agentes que, en tres ocasiones y mediante actos administrativos ejecutoriados, han visto recuperados sus recursos por causales asociadas al uso indebido, lo que evidencia una falla estructural y reiterada de sus controles internos. Es necesaria, porque la recuperación de códigos individuales ha demostrado ser insuficiente cuando el agente puede continuar cursando tráfico riesgoso mediante otros recursos dentro de la misma relación de acceso, y porque no existe una medida menos gravosa que proteja con la misma eficacia a los usuarios frente a la reincidencia consolidada. Y es proporcional en sentido estricto, precisamente porque no opera de manera automática ni unilateral: la terminación exige un trámite administrativo ante la CRC (autoridad imparcial a la que la Ley 1341 de 2009 confía la solución de las controversias de este tipo), adelantado conforme al Código de Procedimiento Administrativo y de lo Contencioso Administrativo, en el cual el PCA/IT concernido podrá ejercer plenamente sus derechos de contradicción y defensa, aportar y controvertir pruebas e interponer los recursos de ley, y en el cual la Comisión, antes de decidir, valorará la situación de los terceros que puedan resultar afectados (incluidos los clientes de los asignatarios involucrados y los usuarios finales de las comunicaciones cursadas), pudiendo adoptar las medidas y condiciones necesarias para salvaguardar sus derechos y garantizar la continuidad de las comunicaciones legítimas durante la transición. De este modo, ninguna consecuencia restrictiva del régimen de reincidencia se produce por fuera de una actuación administrativa con plenas garantías, lo que responde íntegramente a la línea argumentativa de los agentes que comentaron: la potestad coercitiva permanece en cabeza del Estado.

Para introducir estos cambios, se modificará el Parágrafo 4 del artículo 6.1.1.8 del proyecto en el siguiente sentido: (i) se suprimirá su inciso primero, relativo a la suspensión provisional unilateral por un mes; y (ii) se ajustará el inciso restante para disponer que, cuando la CRC haya recuperado por

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

tercera vez un código corto a un mismo PCA/IT por las causales contenidas en los numerales 6.4.3.2.2, 6.4.3.2.8 y 6.4.3.2.9, los PRST con los que dicho agente tenga relación de acceso vigente podrán solicitar a la CRC autorización para su terminación definitiva, la cual se tramitará como actuación administrativa conforme al CPACA, con garantía de los derechos de contradicción y defensa del PCA/IT, vinculación de los terceros interesados y adopción de las medidas necesarias para proteger la continuidad de las comunicaciones legítimas de terceros de buena fe. Se ajustarán, en consecuencia, las remisiones que el articulado y el documento de respuestas hagan al esquema de suspensión suprimido. En tercer lugar, frente a la crítica de asimetría formulada por **INALAMBRIA** y **NEXVIA**, según la cual los PRST también son asignatarios de códigos cortos y también han sido objeto de recuperaciones, sin que el régimen agravado los cobije, la Comisión formula dos precisiones. La primera es que el régimen de administración de recursos de identificación, incluidas las causales de recuperación del artículo 6.4.3.2 y las obligaciones de los asignatarios del artículo 6.1.1.6, se aplica por igual a todos los asignatarios, sean PRST, PCA o IT, sin distinción alguna; los antecedentes de recuperación que citan los agentes confirman, precisamente, que la Comisión ejerce esa potestad frente a los PRST con el mismo rigor. La segunda es que la consecuencia adicional prevista en el Parágrafo 4 se estructura sobre la relación de acceso, que es el vínculo mediante el cual los PCA/IT se conectan a las redes de los PRST; se trata de una medida cuya arquitectura corresponde a la posición que cada agente ocupa en esa relación, y no de un privilegio subjetivo. En todo caso, la supresión de la facultad unilateral de suspensión elimina el componente de la medida que generaba el riesgo de ejercicio asimétrico por parte de los PRST, pues la única consecuencia subsistente (la terminación definitiva) queda reservada a la decisión de la CRC, autoridad ante la cual el PRST solicitante y el PCA/IT concernido concurren en igualdad de condiciones procesales. Con este alcance, no se acepta la solicitud de extender textualmente el Parágrafo 4 a los PRST, por sustracción de materia frente al nuevo diseño.

Finalmente, la Comisión precisa que el Parágrafo 4 del artículo 6.1.1.8 tendrá vigencia temporal. Conforme al artículo de vigencia y derogatorias de la resolución, dicho parágrafo estará vigente hasta la finalización del período de transición previsto en el artículo 18 y, una vez vencido este, se entenderá derogado. Esta vigencia limitada refuerza la proporcionalidad de la medida y atiende las observaciones de los agentes sobre su carácter gravoso, pues la consecuencia aplicable a los agentes reincidentes opera exclusivamente durante la etapa de tránsito hacia el nuevo régimen del ecosistema A2P, período en el cual coexisten los códigos cortos del régimen anterior con los códigos cortos A2P y resulta necesario contar con una herramienta frente a la reincidencia en el mal uso de los recursos de identificación.

En cuarto lugar, frente a las solicitudes de **ASOBANCARIA** relativas a esquemas de transición reforzada para servicios críticos, notificación previa a los usuarios y coordinación con la Superintendencia Financiera cuando se afecten servicios financieros, la Comisión precisa que la protección de los terceros de buena fe queda incorporada como condición del trámite de autorización de terminación, en los términos ya señalados. En otras palabras, la protección de los terceros y de los usuarios finales es un aspecto que, por esencia, la CRC está obligada a tener en cuenta de cara a los trámites administrativos que adelanta.

En quinto lugar, frente a la solicitud de **SINCH** de establecer umbrales o métricas de tolerancia de quejas antes de cualquier medida, la Comisión no la acepta, por cuanto las causales de recuperación del artículo 6.4.3.2 no operan por la mera acumulación de reclamaciones: su configuración se verifica en una actuación administrativa reglada, con valoración probatoria y derecho de contradicción, de modo que la garantía que el agente persigue (que incidentes aislados no deriven en la pérdida del recurso) está asegurada por la naturaleza misma del procedimiento y por el estándar probatorio a cargo de la Comisión, sin necesidad de umbrales numéricos que, además, podrían ser instrumentalizados por los defraudadores para operar sistemáticamente por debajo de ellos.

En sexto lugar, frente a la solicitud de **INALAMBRIA** de incorporar en la memoria justificativa un estudio comparativo de las recuperaciones de códigos cortos de los últimos años, con identificación del tipo de asignatario, condiciones técnicas y porcentajes por categoría de agente, la Comisión no la acepta como condición de la presente decisión, por cuanto el fundamento del régimen de reincidencia no es una presunción generalizada de riesgo contra los integradores tecnológicos, sino un supuesto objetivo, individual y verificado en cada caso: la existencia de recuperaciones reiteradas decretadas mediante actos administrativos ejecutoriados respecto de un mismo agente, cualquiera que sea su naturaleza.

Finalmente, es menester aclarar a todos los agentes que la medida acá analizada, así como las causales de oposición, únicamente estarán vigentes durante el periodo de transición al que hace referencia el proyecto de resolución que fue publicado. Una vez ese periodo de transición finalice, la medida acá discutida perdería eficacia y utilidad debido a la entrada en operación del nuevo ecosistema A2P.

5.2 Oposición a la interconexión

CLARO

Solicita adicionar como complemento un numeral 4.1.2.6.6 que diga lo siguiente:

«4.1.2.6.6. Cancelación o Terminación por Incumplimiento Grave y Reincidencia en Fraude. El proveedor de redes y servicios de telecomunicaciones (PRST) podrá solicitar ante la CRC la autorización para la terminación unilateral y cancelación definitiva del contrato de acceso o interconexión vigente con un PCA o IT, cuando se configure la totalidad de las siguientes condiciones:

i) Evidencia técnica de fraude: Que el PRST demuestre y documente a través de sus sistemas de monitoreo la concurrencia o reincidencia en el envío de tráfico de mensajería corta de texto (SMS) con contenido presuntamente fraudulento, engañoso o de suplantación, cursado a través de los códigos cortos asignados al PCA/IT.

ii) Requerimiento previo desatendido: Que el PRST haya notificado formalmente y por escrito al PCA o IT sobre los patrones atípicos o fraudulentos detectados, solicitando la implementación perentoria de medidas técnicas de mitigación o la suspensión de los originadores de contenido (marcas/Sender ID)

infractores, y que el PCA/IT no haya aplicado tales medidas o no haya cesado la conducta infractora dentro de los plazos establecidos contractualmente o por la regulación.

iii) Historial de afectación al recurso: Que el asignatario (PCA/IT) registre antecedentes en el año inmediatamente anterior de suspensiones provisionales o procesos de recuperación de recursos de identificación por parte de la CRC asociados a fraudes o uso diferente al autorizado.

Para la aplicación de esta medida, el PRST deberá poner en conocimiento de la CRC y de la Superintendencia de Industria y Comercio (SIC) el inicio del trámite, aportando el acervo probatorio correspondiente. La CRC resolverá de plano sobre la autorización de la terminación definitiva del contrato en un plazo no mayor a quince (15) días hábiles, garantizando el derecho de contradicción del PCA/IT en lo que respecta estrictamente a la rigurosidad de las pruebas técnicas presentadas por el operador».

En resumen, solicita adicionar un numeral 4.1.2.6.6 que consagre una causal de cancelación o terminación por incumplimiento grave y reincidencia en fraude, activable por el PRST cuando concurran: (i) evidencia técnica documentada de concurrencia o reincidencia en el envío de SMS presuntamente fraudulentos por los códigos cortos del PCA/IT; (ii) un requerimiento previo formal desatendido para implementar medidas de mitigación o suspender los originadores infractores; y (iii) antecedentes, en el año anterior, de suspensiones provisionales o recuperaciones por parte de la CRC. Propone que el PRST ponga el trámite en conocimiento de la CRC y de la SIC, aportando el acervo probatorio, y que la CRC resuelva de plano en un plazo no mayor a quince días hábiles, con contradicción del PCA/IT limitada a la rigurosidad de las pruebas técnicas.

HABLAME

Señala que el artículo 8, al modificar el artículo 6.1.1.8, faculta al PRSTM para suspender la relación de acceso y, ante la reincidencia, para solicitar la desconexión definitiva del integrador o del PCA. El artículo 5 completa ese esquema con dos causales nuevas, los numerales 4.1.2.6.4 y 4.1.2.6.5, que le permiten oponerse a un nuevo acceso. El efecto combinado es que un particular queda habilitado para suspender, terminar o impedir el acceso de otro agente a la red, esto es, para sacarlo del mercado. Y ese particular no es neutral: en el ecosistema A2P el PRSTM es a la vez competidor y árbitro, porque el propio proyecto lo habilita como asignatario de código corto A2P y de SENDER ID. Ninguna razón de política pública justifica poner una decisión de esa magnitud en manos de quien tiene un interés directo en el resultado.

El acceso y la interconexión no son una concesión del operador, sino una obligación legal que la Comisión regula y vigila. El artículo 50 de la Ley 1341 de 2009 obliga a permitir el acceso a todo proveedor que lo solicite, en condiciones no discriminatorias y bajo las reglas que fija la CRC, y los artículos 42 y 43 reservan a la Comisión la solución de las controversias de acceso. El proyecto invierte ese diseño y traslada al operador una facultad decisoria que la ley puso en cabeza del regulador. Que un PRSTM resuelva por su cuenta suspender o terminar el acceso no es un asunto de orden técnico, es una decisión que la ley no le permite tomar.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Indica que otorgar al operador la facultad de desconectar a otros agentes es, en sí mismo, dotarlo de un instrumento de abuso de posición dominante. El régimen de protección de la competencia, contenido en la Ley 1340 de 2009 y en el artículo 50 del Decreto 2153 de 1992, califica como abuso de la posición dominante, entre otras conductas, obstruir o impedir a terceros el acceso a los mercados o a los canales de comercialización y aplicar condiciones discriminatorias que dejen a un competidor en desventaja. Esa lista no es taxativa: lo que la norma persigue es impedir que quien tiene poder de mercado lo use para excluir a sus rivales. Una facultad de desconexión en manos del operador es, por definición, una herramienta de exclusión, porque le permite cortarle el acceso a la red a un competidor, degradar su operación o expulsarlo del mercado. El proyecto, entonces, no solo deja de cumplir el mandato que la ley le da a la CRC de prevenir el abuso de posición dominante (numeral 5 del artículo 22 y artículo 19 de la Ley 1341), sino que le entrega al operador el medio para cometerlo.

Afirma que el operador de mayor peso ya fue declarado dominante. La CRC calificó a Claro (Comcel) como operador con posición dominante en el mercado de servicios móviles mediante la Resolución CRC 6146 de 2021, confirmada en reposición, y por esa razón le impuso medidas asimétricas en la Resolución CRC 7285 de 2024. La posición dominante es justamente el presupuesto que la ley de competencia exige para que una conducta exclusoria se califique como abuso. Dicho de otro modo, el agente sobre el que recaería esta facultad ya reúne la condición que convierte su uso en abuso de posición dominante. El marco asimétrico que la propia Comisión construyó para contener a Claro quedaría contradicho por una resolución que le entrega una herramienta nueva para excluir competidores. La CRC estaría desarmando con una mano lo que reforzó con la otra.

Por todo lo anterior, indica que la desconexión de un integrador tecnológico no cabe en ningún escenario y debe salir del proyecto. La función del integrador es técnica y consiste en proveer la infraestructura que hace posible la interoperabilidad de los mensajes. Excluirlo no combate el fraude; el fraude se combate identificando y rastreando al originador. Y si pese a todo la Comisión considerara mantener alguna forma de desconexión como medida regulatoria, los principios de igualdad, neutralidad, proporcionalidad y no discriminación obligan a aplicarla al PRSTM en las mismas condiciones en que se pretenda aplicar al integrador o al PCA. No es admisible un régimen en el que el PRSTM pueda desconectar o limitar a otros agentes y, al mismo tiempo, quede exento de esa consecuencia. La asimetría es, en sí misma, el vicio que debe corregirse. En consecuencia, el parágrafo que faculta al PRSTM para suspender el acceso y solicitar la desconexión, en cuanto el artículo 8 modifica el 6.1.1.8, y los numerales 4.1.2.6.4 y 4.1.2.6.5 del artículo 4.1.2.6 deben eliminarse.

Respuesta CRC:

Sobre esta temática se pronunciaron **CLARO** y **HABLAME**, con posiciones abiertamente disidentes entre sí. **CLARO** solicita adicionar un numeral 4.1.2.6.6 que consagre una causal de cancelación o terminación por incumplimiento grave y reincidencia en fraude, activable por el PRST previa evidencia técnica documentada, requerimiento previo desatendido e historial de afectación del recurso en el año anterior, con puesta en conocimiento de la CRC y de la SIC, y decisión de plano de la CRC en un plazo

no mayor a quince días hábiles, con contradicción del PCA/IT limitada a la rigurosidad de las pruebas técnicas. **HABLAME**, en el extremo opuesto, solicita eliminar tanto el Parágrafo 4 del artículo 6.1.1.8 como los numerales 4.1.2.6.4 y 4.1.2.6.5, por considerar que trasladan al operador una facultad decisoria que los artículos 42, 43 y 50 de la Ley 1341 de 2009 reservan a la CRC, que dotan de un instrumento de exclusión a agentes con posición dominante declarada, y que la asimetría del régimen, que no prevé consecuencias equivalentes para el PRSTM, es en sí misma el vicio a corregir; subsidiariamente, solicita que cualquier régimen de desconexión se aplique al PRSTM en las mismas condiciones.

En el documento soporte, la Comisión justificó las dos nuevas causales de oposición como el complemento lógico del esquema de reincidencia: la primera (numeral 4.1.2.6.4) permite al PRST negarse a otorgar un nuevo acceso, durante un año, al PCA/IT cuya desconexión definitiva fue autorizada por la CRC; la segunda (numeral 4.1.2.6.5) permite oponerse cuando el agente desconectado no haya adoptado medidas para prevenir el envío de contenido fraudulento ni para evitar la reincidencia. Evaluados los comentarios, la Comisión responde en los siguientes términos.

Frente a la solicitud de **HABLAME**, se acepta parcialmente. Como se explicó en el numeral 5.1 precedente, la Comisión eliminará la facultad de suspensión unilateral del Parágrafo 4 del artículo 6.1.1.8, con lo cual desaparece del proyecto toda posibilidad de que un PRST interrumpa por decisión propia la relación de acceso de otro agente; la premisa central del comentario (que un particular queda habilitado para sacar del mercado a otro) pierde así su soporte. No se acepta, en cambio, la eliminación del mecanismo de terminación definitiva autorizada por la CRC ni la de las causales de oposición de los numerales 4.1.2.6.4 y 4.1.2.6.5, precisamente porque su diseño es coherente con la arquitectura legal que el propio agente invoca: en ambos casos la decisión no corresponde al PRST sino a la CRC. En el esquema de terminación, el PRST únicamente solicita, y es la Comisión quien autoriza o niega dentro de una actuación administrativa con plenas garantías; y en el régimen de oposición, el artículo 4.1.2.6 de la Resolución CRC 5050 de 2016 exige desde siempre que el PRST demuestre la causal «fundada y razonablemente ante la CRC», de modo que la oposición no es un veto privado sino un supuesto habilitante cuya configuración valora la autoridad al resolver la controversia de acceso, conforme a los artículos 42 y 43 de la Ley 1341 de 2009. Lejos de invertir el diseño legal, el esquema lo confirma ya que toda decisión con efectos restrictivos queda en cabeza del regulador. Por la misma razón, el argumento fundado en el régimen de protección de la competencia no conduce a la eliminación de las causales. La intermediación decisoria de la CRC es, justamente, la salvaguarda institucional que impide que la oposición se emplee como instrumento de exclusión anticompetitiva.

Sin perjuicio de lo anterior, la Comisión acepta la crítica de indeterminación formulada contra el numeral 4.1.2.6.5 (planteada también por **NEXVIA** en el capítulo de reincidentes), en cuanto las expresiones «medidas suficientes» y «medidas necesarias para demostrar que no volverá a incurrir», sumadas a la estructura de la carga probatoria, podrían generar inseguridad jurídica sobre el estándar aplicable. En consecuencia, se ajustará la redacción del numeral 4.1.2.6.5 para: (i) precisar que la valoración corresponde exclusivamente a la CRC dentro del respectivo trámite administrativo; (ii) sustituir el estándar indeterminado por un criterio objetivo, consistente en la acreditación, por parte del PCA/IT

solicitante del acceso, de un plan de correctivos verificable respecto de las fallas de control que dieron lugar a las recuperaciones que motivaron la desconexión (incluyendo, según corresponda, los procesos de debida diligencia sobre sus clientes, los controles de trazabilidad y los mecanismos de atención de reportes de uso indebido); y (iii) garantizar expresamente la oportunidad del PCA/IT de acreditar dichos correctivos en el trámite, sin exigirle la prueba de hechos negativos indefinidos. Con esta redacción, la causal conserva su finalidad preventiva, que es evitar el reingreso inmediato de agentes cuya desconexión obedeció a fallas estructurales no corregidas, y queda depurada de los reparos de tipicidad formulados. El numeral 4.1.2.6.4 se mantiene sin modificaciones, por tratarse de una causal objetiva, de vigencia limitada a un año y anclada a una desconexión previamente autorizada por la propia CRC.

Es importante en este punto aclarar que el numeral 4.2.2.1.2. del artículo 4.2.2.1. de la Resolución CRC 5050 de 2016 dispone que los PRST solo podrán oponerse al acceso solicitado por los PCA/IT de conformidad con lo dispuesto en el artículo 4.1.2.6. del CAPÍTULO 2 del TÍTULO IV. Por esta razón, la propuesta publicada indicaba que serían añadidas dos causales de oposición en los términos explicados. Sin embargo, producto de los comentarios analizados, la CRC considera que, por razones de claridad, es más eficiente u optimo que las referidas causales de oposición sean adicionadas por vía de los nuevos incisos 4.2.2.1.2.1. y 4.2.2.1.2.2 al numeral 4.2.2.1.2. del artículo 4.2.2.1. de la Resolución CRC 5050 de 2016. En esas causales quedarán finalmente contenidas, en la versión final de la resolución, las causales que han sido objeto de pronunciamiento y ajuste.

En el mismo sentido, la Comisión precisa que los incisos 4.2.2.1.2.1 y 4.2.2.1.2.2 tendrán vigencia temporal. Conforme al artículo de vigencia y derogatorias de la resolución, dichos incisos estarán vigentes hasta la finalización del período de transición previsto en el artículo 18 y, una vez vencido este, se entenderán derogados. Con ello se atiende, en lo sustancial, la preocupación de **HABLAME** y de **NEXVIA** sobre el carácter gravoso de las causales de oposición al acceso, pues su aplicación se circunscribe al período de tránsito hacia el nuevo régimen del ecosistema A2P.

Finalmente, frente a la solicitud de aplicar el régimen de desconexión al PRSTM «en las mismas condiciones», la Comisión se remite a lo expuesto en el numeral 5.1 precedente sobre la aplicación uniforme del régimen de recuperación a todos los asignatarios y sobre la arquitectura de la relación de acceso, y reitera que, suprimida la facultad unilateral de suspensión, no subsiste en el proyecto ninguna potestad restrictiva en cabeza de los PRST cuyo ejercicio asimétrico deba conjurarse.

Frente a la solicitud de **CLARO**, no se acepta la adición del numeral 4.1.2.6.6 propuesto, por dos razones. Primera, por duplicidad ya que la finalidad que persigue, que es habilitar la terminación de la relación de acceso frente a agentes con historial verificado de uso fraudulento de los recursos, previa autorización de la CRC, ya está satisfecha por el Parágrafo 4 del artículo 6.1.1.8, en su versión ajustada conforme al numeral 5.1 de este documento, que condiciona la terminación a un supuesto objetivo (la tercera recuperación por causales tasadas) y a la autorización de la Comisión en actuación administrativa; crear una causal paralela en el régimen de oposición, fundada en la valoración probatoria de patrones de tráfico «presuntamente» fraudulentos documentados por el propio PRST, reintroduciría por otra vía el estándar subjetivo y el riesgo de instrumentalización que este documento ha depurado

del esquema. Segunda, por razones de debido proceso: la propuesta contempla que la CRC resuelva «de plano» en quince días hábiles y que la contradicción del PCA/IT se limite «estrictamente a la rigurosidad de las pruebas técnicas presentadas por el operador», restricciones incompatibles con la plenitud de las garantías de defensa que, conforme al CPACA y al artículo 29 constitucional, deben regir una actuación cuyo resultado puede ser la exclusión definitiva de un agente del mercado. La Comisión destaca, en todo caso, que la propuesta de **CLARO** converge con el diseño adoptado en un punto esencial: la terminación definitiva requiere siempre autorización previa de la CRC, con conocimiento del acervo probatorio, lo que confirma la razonabilidad del esquema que se mantiene.

6 Otras temáticas

6.1 Régimen de transición

ANDESCO

Solicita, para el período de transición del sistema A2P (Art. 19), establecer un cronograma mínimo garantizado de 6 meses contados desde la publicación de la presente resolución para que los agentes puedan iniciar los procesos internos de preparación, independientemente de la fecha de la Fase II.

CAMPAIGN REGISTRY

Reseña que el período de transición de seis meses desde la firmeza de la resolución tarifaria de la Fase II se estructura en cuatro fases (selección del validador en los meses 1–2, KYC y solicitud de recursos en los meses 3–4, carga y pruebas de plantillas en el mes 5 y entrada en vigencia en los meses 5–6) y señala que, para garantizar el cronograma, es necesario identificar los actores de cada operador, fijar calendarios estrictos de reuniones y coordinación mediante planes de proyecto por operador y realizar seguimientos con los responsables, manifestando experiencia en este tipo de actividades.

CLARO

Considera insuficiente el plazo de tres meses del artículo 2.1.10.7.2.1.5 para implementar los sistemas de monitoreo y control del tráfico P2P, pues las funcionalidades exigidas implican diseñar, desarrollar o adaptar sistemas especializados (detección de A2P simulado como P2P, granjas de SIM, volúmenes inusuales, dispersión de destinatarios y homogeneidad de contenido), integrarlos, calibrar modelos y umbrales para minimizar falsos positivos y realizar inversiones y pruebas que requieren varios meses. Añade que el proyecto no aporta evidencia de que tres meses sean suficientes para todos los PRSTM ni analiza sus diferencias de infraestructura y madurez, por lo que solicita ampliar el plazo a un mínimo de seis meses (con reporte de cumplimiento a los doce meses).

Advierte, además, que el período de transición del artículo 19 no es claro porque otras obligaciones aplican desde la publicación en el Diario Oficial, por lo que insiste en expedir un solo acto administrativo

que comprenda también la remuneración del SMS A2P, y concluye que el plazo de seis meses es imposible de cumplir y que las adecuaciones de red requerirían dieciocho meses desde la publicación.

ETB

Señala que los plazos de implementación propuestos no reflejan adecuadamente la complejidad técnica, operativa y económica de las medidas previstas en el proyecto. Argumenta que la implementación de sistemas de monitoreo en tiempo real, motores de analítica antifraude, integraciones con el validador centralizado, adecuaciones de plataformas de mensajería, ajustes de señalización, modificaciones contractuales, desarrollos tecnológicos, pruebas de interoperabilidad y procesos de capacitación requiere horizontes temporales significativamente superiores a los contemplados actualmente.

Considera indispensable la realización de mesas técnicas previas a la expedición de la resolución definitiva que permitan definir la Fases I y la Fase II en una sola, los impactos a diferentes sectores transaccionales, así como la validación de estándares de interoperabilidad, especificaciones funcionales, modelos de integración mediante APIs, criterios de validación y procedimientos operativos comunes para toda la industria.

Asimismo, solicita un plazo mínimo de veinticuatro (24) meses para su implementación contados a partir de la definición definitiva de los estándares técnicos y de la disponibilidad efectiva de las plataformas requeridas. De igual forma, considera necesario establecer cronogramas diferenciados para operadores con dependencia tecnológica de terceros como los OMV, así como desarrollar esquemas graduales de implementación acompañados de ambientes de prueba, pilotos controlados y periodos de estabilización operacional antes de la exigibilidad plena de las obligaciones.

INETUM

Consulta si el plazo de implementación de 3 meses indicado en el documento de proyecto fue acordado con la industria. Esto debido a que, por su experiencia en proyectos de la misma índole, dicho tiempo podría considerarse ajustado.

JULIO NULDEMAR

Solicita sustituir los plazos de adecuación por un término técnicamente viable para realización de desarrollos de software y pruebas, al respecto propone el siguiente texto «RÉGIMEN DE TRANSICIÓN: Las obligaciones derivadas del uso del validador centralizado y la verificación de plantillas entrarán en vigencia plena transcurrido un plazo no inferior a doce (12) meses, contados a partir de la fecha en que la CRC publique de manera oficial los manuales técnicos definitivos y las APIs de integración del validador centralizado. Durante los primeros seis (6) meses de dicho plazo, se adelantará una fase piloto obligatoria y no sancionatoria entre todos los agentes del mercado para la calibración del sistema.»

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

NEXVIA

Indica que el numeral 19.1.5 del proyecto publicado es la ejecución transitoria de la unicidad cuya eliminación se solicita en su comunicación en los puntos 3.3, 3.4 y 3.6, y debe correr su misma suerte. Afirma que el propio texto publicado admite la magnitud del daño que ordena, exige estimar el «número de usuarios activos afectados por cada código corto a devolver», esto es, reconoce que la medida afecta servicios en operación con usuarios reales, sin que el documento soporte cuantifique ese impacto ni lo pondere contra beneficio antifraude alguno, ninguna modalidad de fraude documentada se origina en la pluralidad de códigos de asignatarios formales.

Señala que la consolidación es además internamente contradictoria con el propio proyecto, tras la migración forzosa, el código único concentrará exactamente la mezcla de contenidos heterogéneos que la naturaleza del recurso prohíbe, y los asignatarios que no acrediten conexión directa (la mayoría de los PCA, conforme a las definiciones vigentes) ni siquiera podrán conservar código alguno, expulsándolos del mercado por vía transitoria.

SAEM

Solicita ampliar el período de transición a 12–18 meses; permitir más de un código corto A2P por IT ante necesidad técnica acreditada; y reconocer plenamente la continuidad del consentimiento migrado.

TIGO

Señala que el período de seis meses estructurado en cuatro fases, con una selección del validador limitada a 54 días (artículos 18 y 19), es insuficiente frente al alcance real de las medidas, y que el propio documento soporte reconoce que las plataformas SMSC desplegadas no cuentan con APIs para la administración dinámica del código corto (parametrización manual con SLA cercanos a tres días hábiles) ni con mecanismos nativos de autenticación criptográfica o validación centralizada, de modo que no se trata de parametrizar lo existente sino de desarrollar e integrar capacidades nuevas en sistemas críticos de red. Advierte que los hitos están concatenados y dependen de terceros (seleccionar y contratar al validador, que este se constituya e integre sus APIs, que los PRST y los asignatarios realicen las adecuaciones e integraciones y el redimensionamiento, registrar y aprobar plantillas y consolidar y migrar la numeración sin afectar a los usuarios) y que la falla de cualquiera de ellos arrastra a toda la cadena, con incertidumbre técnica aún no resuelta (arquitectura de interoperabilidad de APIs, tiempos de respuesta y disponibilidad). Por ello solicita que la transición y la entrada en vigencia plena del régimen A2P no sea inferior a dieciocho meses, con fases que prevean márgenes razonables para contratación, desarrollo, integración y pruebas y sin encadenar hitos críticos en ventanas de pocos días.

SINCH

Dice que la viabilidad del nuevo marco técnico dependerá de un periodo de transición realista que permita integrar a los operadores y registrar a las marcas sin interrumpir las comunicaciones críticas de

las empresas. El enfoque debe ser en un despliegue por fases evita fallos masivos en el servicio y protege el tráfico SMS legítimo. No obstante, el desafío radica en que un plazo de adaptación demasiado largo mantendrá la vulnerabilidad al fraude y postergará la definición de las tarifas A2P, prolongando la incertidumbre financiera en el sector.

TRANSUNION

Indica que el proyecto contempla un período de transición de seis meses, dentro del cual se concentrarían la selección del validador centralizado, la habilitación de su infraestructura, y la integración con los PRST. Aunque se comprende la necesidad de implementar oportunamente medidas de prevención del fraude, dice que los plazos en el cronograma propuesto pueden resultar insuficientes frente a la complejidad técnica, contractual y operativa del modelo.

Afirma que el proceso para la selección de un proveedor, la suscripción de contratos, la implementación, las pruebas no productivas y el despliegue controlado de una plataforma crítica para el ecosistema requieren tiempos suficientes para asegurar calidad, seguridad y continuidad del servicio. En consecuencia, se solicita a la CRC evaluar la ampliación del cronograma propuesto y establecer un esquema de implementación gradual. Este esquema debería supeditar la entrada en operación plena del régimen a la verificación de hitos objetivos de preparación técnica, pruebas de interoperabilidad, continuidad operacional, seguridad de la información y capacidad de atención de incidentes.

Respuesta CRC:

Sobre esta temática se pronunciaron **ANDESCO**, **CAMPAIGN REGISTRY**, **CLARO**, **ETB**, **INETUM**, **JULIO NULDEMAR**, **NEXVIA**, **SAEM**, **TIGO**, **SINCH** y **TRANSUNION**. Revisadas las intervenciones, la Comisión identifica una tendencia claramente convergente ya que la mayoría de los agentes considera que el período de transición de seis (6) meses previsto para la adopción del nuevo régimen del ecosistema A2P resulta insuficiente frente a la complejidad técnica, contractual y operativa de las medidas, y solicita su ampliación. Las intervenciones difieren, sin embargo, en la magnitud y en la forma de contar el plazo.

En efecto, **ANDESCO** solicita garantizar un cronograma mínimo de seis (6) meses contados desde la publicación de la resolución, con independencia de la fecha de la Fase II. **CAMPAIGN REGISTRY** describe las cuatro fases del cronograma (selección del validador, procesos de KYC y solicitud de recursos, carga y pruebas de plantillas y entrada en vigencia) y propone mecanismos de coordinación por operador. **CLARO** solicita ampliar a dieciocho (18) meses, contados desde la publicación en el Diario Oficial, las adecuaciones de red, y de manera específica ampliar de tres (3) a seis (6) meses el plazo de implementación de los sistemas de monitoreo del tráfico P2P del artículo 2.1.10.7.2.1.5. **ETB** solicita un plazo mínimo de veinticuatro (24) meses, la unificación de las Fases I y II y cronogramas diferenciados para los OMV. **JULIO NULDEMAR** propone doce (12) meses contados desde la publicación de los manuales técnicos y las APIs del validador centralizado, con una fase piloto no sancionatoria durante los primeros seis (6) meses. **SAEM** solicita ampliar el período a un rango de doce (12) a dieciocho (18)

meses. **TIGO** solicita que el período no sea inferior a dieciocho (18) meses, atendiendo a la secuencia de hitos concatenados y dependientes de terceros (en particular del validador) y a la incertidumbre técnica aún existente. **TRANSUNION** solicita ampliar el cronograma y supeditar la entrada en operación plena a la verificación de hitos objetivos de preparación. **NEXVIA** plantea que el numeral 19.1.5, relativo a la ejecución transitoria de la unicidad, debe correr la misma suerte que su solicitud de eliminación de la regla de único código corto. En contraste, **SINCH** advierte que un plazo de adaptación demasiado extenso mantendría la vulnerabilidad al fraude y prolongaría la incertidumbre financiera asociada a la definición de las tarifas A2P, por lo que aboga por un despliegue por fases realista pero acotado.

Sobre el período de transición contenido en el proyecto y en el documento soporte

El documento soporte previó un período de transición de seis (6) meses para la subrogación del Capítulo 4 del Título VI de la Resolución CRC 5050 de 2016 y para la adición de los Capítulos 12 y 13, período que empezaría a contarse a partir de la publicación en el Diario Oficial de la resolución mediante la cual la CRC defina la nueva remuneración aplicable al ecosistema A2P. Dicho período se estructuró en cuatro fases sucesivas y contempló, para la selección del validador centralizado, una ventana inicial acotada. La finalidad de este diseño fue garantizar un tránsito ordenado y sin traumatismos hacia el nuevo régimen.

Así las cosas, la Comisión acepta parcialmente los comentarios y, en consecuencia, amplía el período de transición. La revisión de las intervenciones evidencia que la implementación del nuevo régimen no consiste en la mera parametrización de las plataformas existentes, sino en el desarrollo e integración de capacidades nuevas en sistemas críticos de red, y que la ejecución depende de una secuencia de hitos concatenados (la selección, constitución e integración del validador centralizado, las adecuaciones e integraciones por API de los PRST y de los asignatarios de código corto, el registro y prueba de plantillas y la migración de la numeración existente sin afectar a los usuarios) en la que la demora de cualquier eslabón, especialmente la del tercero que opere como validador, arrastra a toda la cadena.

Ponderando lo anterior con la advertencia de **SINCH** sobre los riesgos de una transición excesivamente prolongada, la Comisión considera que un plazo de veinticuatro (24) meses, como el solicitado por **ETB**, resultaría desproporcionado frente a la urgencia de la problemática, mientras que el plazo original de seis (6) meses se podría considerar insuficiente. En consecuencia, se modificará el régimen de transición para ampliar el período de transición del nuevo régimen del ecosistema A2P de seis (6) a doce (12) meses. Este plazo ofrece un margen razonable para la contratación, el desarrollo, la integración y las pruebas, sin encadenar hitos críticos en ventanas de pocos días, y equilibra la necesidad de los agentes con el objetivo de no dilatar la entrada en vigencia de las medidas antifraude.

Como consecuencia de la ampliación del período de transición, la Comisión reestructura las fases previstas en el artículo 19 del proyecto publicado, que corresponde al artículo 18 producto de la nueva numeración, en los siguientes términos: (i) la Fase 1, correspondiente a la selección del validador centralizado, pasa de un plazo máximo de cincuenta y cuatro (54) días calendario a un plazo máximo

de cinco (5) meses, el cual comprende de manera integral los tiempos y plazos establecidos en el artículo 17 de la resolución, incluidas las etapas subsidiarias a cargo de los PRSTM y de la CRC previstas en los numerales 17.1.5 y 17.1.6; (ii) la Fase 2, de registro de potenciales asignatarios y solicitud de recursos, tendrá una duración máxima de tres (3) meses contados a partir del hito de inicio de que trata el numeral 18.1.1.3; (iii) la Fase 3, de registro de plantillas y pruebas técnicas, tendrá una duración máxima de dos (2) meses contados a partir de la finalización de la Fase 2; y (iv) la Fase 4, de consolidación de códigos cortos y entrada en plena vigencia del nuevo régimen, iniciará de manera concurrente con el último mes de la Fase 3 y concluirá al vencimiento del período de transición.

Adicionalmente, con el fin de evitar cualquier duda interpretativa sobre el cómputo de los plazos, se precisa en el numeral 18.1 que los rangos de meses señalados en los numerales 18.1.1 a 18.1.4 corresponden al escenario de duración máxima de la Fase 1. Cuando esta concluya con anterioridad, los plazos máximos de las Fases 2, 3 y 4 se contarán desde el hito de inicio previsto en el numeral 18.1.1.3, sin que ello altere la duración total del período de transición ni su fecha de vencimiento. Con esta reestructuración, la Comisión atiende de manera concreta la observación de **ETB** sobre la insuficiencia de una ventana de cincuenta y cuatro (54) días calendario para la selección del validador centralizado, así como las observaciones sobre el carácter concatenado de los hitos de implementación, y dota a los agentes obligados de certeza sobre el plazo aplicable a cada fase.

Sobre los demás aspectos planteados

En relación con la solicitud de **NEXVIA** de eliminar el numeral 19.1.5 del proyecto publicado relativo a la ejecución transitoria de la unicidad, la Comisión reitera que la regla de un único código corto A2P por agente se mantiene, según se motiva en el capítulo denominado «Código Corto A2P», por lo que el régimen de transición se limita a ejecutar de manera ordenada dicha regla y no procede su eliminación. La solicitud de **SAEM** de permitir más de un código corto A2P por Integrador Tecnológico se atiende igualmente en el capítulo denominado «Código Corto A2P»; y su solicitud de reconocer la continuidad del consentimiento de los usuarios migrados se acoge, precisándose que la migración de la numeración y de los recursos existentes al nuevo régimen no afecta la validez del consentimiento previamente otorgado por los usuarios. Por las razones expuestas por el agente se acepta la solicitud de **CLARO** de ampliar el plazo de implementación de los sistemas de monitoreo del tráfico P2P del artículo 2.1.10.7.2.1.5, el cual se amplía de tres (3) a seis (6) meses contados a partir de la publicación en el Diario Oficial de la resolución que adopta los sistemas de monitoreo, con el fin de que estos se implementen en un plazo técnicamente viable. En consecuencia, el informe técnico de acreditación deberá presentarse al vencimiento de dicho plazo y el segundo informe dentro de los seis (6) meses siguientes a la presentación del primero. Las solicitudes de **ETB** y **CLARO** de unificar las Fases I y II en un solo acto administrativo, así como la relación entre el período de transición y la resolución de remuneración, se abordan en el capítulo denominado «Remuneración/fases del proyecto/AIN». Los cronogramas diferenciados solicitados por **ETB** para los operadores móviles virtuales se atienden en el capítulo denominado «Sobre los OMV». Finalmente, las consideraciones sobre la selección y disponibilidad del validador centralizado, de cuya ejecución depende buena parte del cronograma, se desarrollan en el capítulo denominado «Validador centralizado: forma de selección, competencias y funciones».

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

De otra parte, la Comisión se pronuncia sobre la solicitud de **COLOMBIA FINTECH** consistente en incorporar una cláusula de continuidad operativa para la mensajería crítica del sector financiero durante la transición, acompañada de una prórroga individual para las entidades que acrediten encontrarse en proceso de migración. Al respecto, la CRC no acoge la solicitud. En primer lugar, la ampliación general del período de transición adoptada en este capítulo, sumada al condicionamiento de la entrada en vigencia de las medidas técnicas asociadas a la mensajería A2P a la publicación en el Diario Oficial del acto administrativo mediante el cual se defina la nueva remuneración aplicable al ecosistema A2P, otorga a todos los agentes —incluidas las entidades del sector financiero— un margen suficiente y uniforme para adelantar sus procesos de adecuación. En segundo lugar, un régimen de prórrogas individuales acreditadas caso a caso fragmentaría la aplicación del nuevo esquema, generaría asimetrías entre agentes que compiten por los mismos recursos de identificación y postergaría de manera indefinida la trazabilidad del tráfico A2P precisamente respecto de las comunicaciones que registran mayor exposición al fraude. En tercer lugar, la continuidad de la mensajería crítica se encuentra atendida mediante instrumentos específicos previstos en la decisión, tales como el registro simplificado, categórico o parametrizado de plantillas para mensajes de autenticación y seguridad, desarrollado en el capítulo denominado «Tratamiento de mensajes OTP, autenticación, seguridad y comunicaciones críticas», y la posibilidad de asignación de oficio del SENDER ID reconocida en este capítulo. En consecuencia, no se acepta la solicitud y se mantiene el régimen de transición en los términos expuestos.

Por otro lado, la CRC considera pertinente incorporar una precisión en el régimen de transición y en las reglas generales del SENDER ID, con el fin de reconocer expresamente la posibilidad de asignar de oficio este recurso cuando ello sea necesario para garantizar el cumplimiento de obligaciones regulatorias. Esta precisión resulta consistente con el artículo 6.1.1.5 de la Resolución CRC 5050 de 2016, según la modificación propuesta, en el que se establece que el Administrador de los Recursos de Identificación podrá asignar recursos de identificación de oficio o a petición de los solicitantes, teniendo en cuenta las atribuciones definidas para cada recurso registradas en el SIGRI.

Para tal efecto, la CRC realizará dos ajustes específicos en la resolución. En primer lugar, se adicionará un parágrafo al artículo 6.12.1.2 —Asignatarios del SENDER ID—, con el propósito de establecer una regla general conforme a la cual el Administrador de los Recursos de Identificación podrá asignar de oficio un SENDER ID cuando ello resulte necesario para garantizar el cumplimiento de obligaciones regulatorias, la adecuada identificación de comunicaciones de interés público, la continuidad de servicios o la trazabilidad de comunicaciones exigidas por la regulación. En segundo lugar, se incorporará un parágrafo específico en el artículo 19 —Régimen de transición— (ahora artículo 18 producto de la nueva numeración), para prever la asignación de oficio de un SENDER ID al administrador de la base de datos de portabilidad numérica, cuando dicho identificador sea necesario para el envío de comunicaciones asociadas al cumplimiento de obligaciones regulatorias previstas en la Resolución CRC 5050 de 2016.

En particular, la CRC considera conveniente prever, dentro del artículo 19 —Régimen de transición— (ahora artículo 18 producto de la nueva numeración), la asignación de oficio de un SENDER ID al administrador de la base de datos de portabilidad numérica. Lo anterior permitirá asegurar que las

comunicaciones asociadas al cumplimiento de obligaciones regulatorias se encuentren debidamente identificadas frente al usuario y se integren al nuevo esquema de trazabilidad del tráfico A2P, sin generar cargas procedimentales innecesarias durante la implementación del régimen.

Esta asignación de oficio no implica una excepción general al régimen A2P ni habilita el uso del SENDER ID para finalidades distintas a aquellas asociadas al cumplimiento de obligaciones regulatorias. Por el contrario, el SENDER ID asignado deberá utilizarse exclusivamente para las comunicaciones vinculadas a la función regulatoria correspondiente y estará sujeto a las condiciones de uso, trazabilidad, seguridad, validación y demás reglas aplicables al recurso.

6.2 Remuneración/fases del proyecto/AIN

ANDESCO

Manifiesta que la desregulación de la tarifa mayorista del SMS A2P debe abordarse como una primera fase del proceso, o bien en que ambas medidas, el régimen antifraude y la definición o desregulación tarifaria del SMS A2P, se adopten de manera simultánea, de modo que las nuevas obligaciones cuenten con una fuente cierta de financiación y el modelo resulte sostenible.

En complemento, **ANDESCO** sostiene que el artículo 2.2.13.3.2 del Decreto 1078 de 2015 exige que los proyectos regulatorios vayan acompañados de documentos soporte que incluyan la evaluación de impactos económicos de las medidas propuestas. En este contexto, que el proyecto no incorpora un modelo económico verificable que permita acreditar el cumplimiento de los principios de eficiencia y bienestar social previstos en la Ley 1341 de 2009, ni de los requisitos del Análisis de Impacto Normativo (AIN), pues considera que separar el análisis técnico (Fase I) del análisis económico (Fase II) fragmenta la intervención regulatoria y elimina la posibilidad de realizar un genuino análisis costo-beneficio..

En consecuencia, considera que la CRC debe publicar el análisis económico del mercado de terminación de SMS A2P, incluyendo:

(i) estructura de costos del validador centralizado;
(ii) esquema de recuperación de costos para los asignatarios del código corto;
(iii) análisis de impacto sobre PCA/IT por tamaño;
(iv) proyección de traslado de costos a usuarios finales.

Alternativamente, **ANDESCO** dice que la entrada en vigor de los artículos 12, 13, 14 y 19 debe quedar explícitamente condicionada a la publicación de ese análisis, no solo a la expedición del acto de remuneración A2P.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Por otro lado, **ANDESCO** cuestiona que la evaluación multicriterio no haya considerado como alternativa el fortalecimiento de los mecanismos actualmente existentes, por estimar que esta omisión afecta la conclusión según la cual el validador centralizado constituye la mejor alternativa regulatoria.

Por otra parte, considera que el proyecto de resolución incluye obligaciones relacionadas con la modificación de los contratos de los PRST con entidades del sector financiero para incorporar deberes derivados de la regulación, señala que la obligación de registrar o reportar la información correspondiente recae directamente sobre la entidad financiera, en su calidad de titular de la relación contractual con el usuario y de sujeto obligado por la regulación que establezca dicho deber. En consecuencia, a su parecer no resulta razonable ni jurídicamente adecuado exigir a los PRST que gestionen modificaciones contractuales con terceros para asegurar el cumplimiento de obligaciones que no les corresponden. Dice que la CRC, ante la ausencia de facultades para imponer obligaciones a las entidades financieras, traslada a los PRST responsabilidades sobre actuaciones que dependen exclusivamente de la voluntad y gestión de terceros, generando obligaciones de imposible o difícil cumplimiento.

CLARO

Señala que diferir el análisis económico para una fase posterior fragmenta la intervención regulatoria, genera riesgos de inconsistencias normativas e impide evaluar de manera integral los impactos técnicos, operativos y económicos de las medidas propuestas. Indica que, si la propia CRC reconoce que aún requiere información para comprender el funcionamiento del mercado de mensajería SMS A2P, resulta prematuro adoptar obligaciones regulatorias que impactan directamente dicho mercado. En consecuencia, considera que la regulación definitiva debe estar acompañada de un análisis integral que incorpore simultáneamente los aspectos técnicos, operativos y económicos del ecosistema, de manera que sea posible verificar la proporcionalidad de las medidas, la adecuada asignación de incentivos y la sostenibilidad del modelo. En particular, sostiene que la adopción de obligaciones relacionadas con la validación de remitentes, la autenticación de mensajes y las nuevas exigencias operativas no puede analizarse de manera aislada de la estructura económica que soportará el funcionamiento del esquema.

Adicionalmente, cuestiona que la CRC no haya realizado un análisis de fondo de las observaciones formuladas por la industria sobre el Validador Centralizado y el Sender ID. Afirma que las respuestas publicadas se limitan a resumir los comentarios recibidos sin efectuar una valoración técnica individual ni explicar las razones para adoptar, modificar o descartar las alternativas planteadas. Solicita que, antes de imponer estas obligaciones, la Comisión publique un análisis detallado de sus impactos técnicos, operativos, económicos y competitivos y responda de manera sustantiva los cuestionamientos formulados por los agentes.

Así mismo, manifiesta que el documento soporte no demuestra que el esquema centralizado de validación y autenticación sea la alternativa más eficiente para mitigar el fraude, pues no incorpora una comparación rigurosa con mecanismos regulatorios existentes, como la suspensión provisional de códigos cortos, el bloqueo de tráfico irregular, los sistemas de monitoreo y detección temprana o las

actuaciones coordinadas entre operadores y autoridades. Señala igualmente que no existe un análisis cuantitativo de costos y beneficios que permita demostrar que el Validador Centralizado constituye la medida menos gravosa y más eficiente, considerando que su implementación implica nuevas infraestructuras tecnológicas, mecanismos de gobernanza, procesos de validación, auditoría, administración de información y responsabilidades operativas para todos los actores.

Finalmente, solicita que la CRC realice una evaluación exhaustiva de la efectividad de las medidas actualmente vigentes, identifique oportunidades de mejora y demuestre, con evidencia técnica y económica suficiente, que la alternativa propuesta genera beneficios netos superiores a los obtenidos mediante el fortalecimiento de las herramientas regulatorias existentes. En particular, solicita:

- El esquema de remuneración aplicable a la terminación de tráfico asociado a códigos cortos.
- La metodología de recuperación de costos.
- Los responsables de asumir las inversiones requeridas.
- Los mecanismos de compensación económica asociados a nuevas obligaciones regulatorias.

Así mismo, considera que no es posible evaluar la viabilidad y proporcionalidad de las medidas mientras no exista claridad sobre el esquema de remuneración de la terminación de SMS A2P, la metodología de recuperación de costos, los responsables de asumir las inversiones y los mecanismos de compensación económica asociados a las nuevas obligaciones regulatorias, pues la ausencia de esta información impide valorar adecuadamente el impacto económico del proyecto y demostrar que la regulación propuesta resulta eficiente y proporcionada.

COLOMBIA FINTECH

Señala que los artículos 2.1.10.7.2.1.5 y 2.1.10.7.2.2.4 fijan tres (3) meses para implementar los sistemas de monitoreo P2P y de voz respectivamente, y el artículo 19 establece seis (6) meses de transición para el ecosistema A2P. Manifiesta que estos plazos son difícilmente compatibles con la realidad técnica de la implementación. Indica que el propio documento soporte de la CRC reconoce que los SMSC actuales no cuentan con APIs para la integración con sistemas externos y que los cambios en esas plataformas se gestionan con SLA de hasta tres (3) días hábiles.

Solicita que la CRC replantee el cronograma, contemplando un mínimo de seis (6) meses para las medidas de voz y P2P, y de doce (12) meses para el ecosistema A2P completo, considerando la carga tecnológica real de la implementación.

ETB

Considera que el AIN presenta desafíos estructurales relacionados con la proporcionalidad de las obligaciones propuestas, su sostenibilidad económica, sus impactos competitivos y la adecuada

distribución de las cargas regulatorias. En particular, cuestiona la fragmentación entre la Fase I y la Fase II del proyecto, al señalar que las obligaciones técnicas implican una elevada carga tecnológica, operativa y financiera, mientras que la revisión del esquema de remuneración del servicio SMS A2P fue trasladada a una etapa posterior. A su juicio, esta separación genera un desbalance regulatorio, pues las inversiones y costos de operación son exigibles antes de definir los mecanismos que permitirían recuperar dichos costos. En consecuencia, solicita que la entrada en vigencia de las obligaciones técnicas más complejas quede condicionada a la definición y entrada en operación de los mecanismos económicos que garanticen su sostenibilidad y que ambas fases sean evaluadas como una única unidad económica y regulatoria.

Adicionalmente, considera que el AIN debe profundizar el análisis de los impactos económicos, operativos y competitivos de las medidas propuestas, particularmente sobre los Operadores Móviles Virtuales (OMV). Señala que las obligaciones pueden resultar razonables para operadores con infraestructura propia, economías de escala e integración vertical, pero generan un impacto significativamente mayor sobre los OMV, debido a su dependencia tecnológica de terceros, la ausencia de infraestructura propia y la falta de ingresos mayoristas que les permitan financiar inversiones en monitoreo, validación, integración tecnológica y gestión antifraude. En este contexto, sostiene que la imposición de obligaciones homogéneas sobre agentes con capacidades económicas, tecnológicas y operativas diferentes puede producir efectos anticompetitivos, reforzar la concentración existente y consolidar las ventajas competitivas de los operadores dominantes. Por ello, solicita que el AIN incorpore una evaluación expresa sobre el impacto de las medidas en la competencia, las asimetrías entre operadores, el efecto diferenciado sobre los OMV, los riesgos derivados del actual «duopolio táctico» y la competencia ejercida por las plataformas OTT, las cuales ofrecen servicios sustitutos sin estar sujetas a obligaciones regulatorias equivalentes.

Finalmente, manifiesta que el proyecto incorpora nuevas obligaciones de monitoreo, reporte, intercambio de información y generación de estadísticas, mientras la CRC adelanta iniciativas de simplificación administrativa y reducción de cargas regulatorias. En consecuencia, solicita que el AIN incorpore una valoración integral de las cargas administrativas derivadas del presente proyecto y de otras iniciativas regulatorias en curso, analice su efectividad y evalúe posibles mecanismos de simplificación o sustitución de reportes existentes para evitar duplicidades regulatorias.

INALAMBRIA

Indica que la existencia de fraude en determinados segmentos del mercado no constituye evidencia suficiente para concluir que todos los actores del ecosistema presentan niveles equivalentes de riesgo. Por el contrario, considera que una regulación eficiente debería orientarse a identificar y corregir los puntos específicos donde efectivamente se concentra el fraude, en lugar de asumir que todos los Integradores Tecnológicos, Proveedores de Contenidos y Aplicaciones o asignatarios de códigos cortos presentan el mismo nivel de riesgo.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En este contexto, señala que la regulación debería privilegiar mecanismos de evaluación basados en resultados verificables, tales como las tasas efectivas de fraude, el volumen de tráfico malicioso detectado, el número de reclamaciones asociadas a campañas fraudulentas o la efectividad de los mecanismos de mitigación, antes que esquemas uniformes de cumplimiento formal. A su juicio, la imposición de cargas regulatorias idénticas para todos los participantes, independientemente de su desempeño real en materia de prevención del fraude, puede generar efectos contraproducentes y de selección adversa, trasladando costos significativos a aquellos actores que ya han realizado inversiones en herramientas tecnológicas, inteligencia artificial, monitoreo y controles preventivos, sin generar incentivos adicionales para mejorar los resultados efectivos de seguridad.

Por lo anterior, solicita que la CRC evalúe si las medidas propuestas reconocen adecuadamente las diferencias existentes entre los distintos segmentos del mercado y si los costos regulatorios son asignados de manera proporcional al riesgo efectivamente identificado, privilegiando mecanismos focalizados en los segmentos donde se concentra el fraude sobre esquemas uniformes de cumplimiento formal generalizado.

SAEM

Dice que el artículo 19 de la Ley 1341 de 2009 (modificado por la Ley 1978 de 2019) ordena que la regulación promueva la inversión, la simplificación regulatoria y la protección al usuario, y la metodología de Análisis de Impacto Normativo (AIN) promovida por la OCDE exige soportar las decisiones en un análisis costo-beneficio. Afirma que el proyecto, sin embargo, no cuantifica: (i) el costo de implementación y operación del validador centralizado que recaerá sobre los IT; (ii) la reducción de ingresos ya causada por la Ley 2300 de 2023; (iii) el costo de las obligaciones de KYC, integración por APIs, reportería, campañas pedagógicas y formación interna; ni (iv) la relación entre ese costo agregado y la reducción efectiva de fraude esperada. Por lo tanto, solicita que el documento soporte incorpore esa cuantificación antes de adoptar las medidas.

En complemento de lo anterior, dice que, según el proyecto, la entrada en vigencia de las medidas técnicas de A2P se condiciona a la publicación del acto que defina la nueva remuneración del ecosistema A2P (Fase II), y todo el período de transición se cuenta desde ese hito. Al respecto, sostiene que la viabilidad económica del IT depende directamente de la remuneración. Adoptar las cargas técnicas y operativas sin conocer la remuneración impide a **SAEM** evaluar la sostenibilidad del modelo y planear su inversión. La separación en fases no debe traducirse en incertidumbre sobre los costos que la propia resolución traslada al IT. Propone lo siguiente: (i) Que la Fase II resuelva también, de manera explícita, cómo se remunera o se reconoce el costo del validador y del cumplimiento del nuevo régimen en la cadena de valor; (ii) que el AIN integre el análisis económico de ambas fases, de modo que las cargas técnicas y su financiación se evalúen conjuntamente con la remuneración.

De manera concreta solicita realizar y publicar, antes de adoptar las medidas, un Análisis de Impacto Normativo que cuantifique los costos del nuevo régimen (validador, KYC, integración por APIs,

reportería, campañas y formación) sobre los IT y la relación de esos costos con la reducción efectiva de fraude.

SINCH

Solicita a la CRC considerar la desregulación total de los precios para la terminación de mensajes SMS A2P, permitiendo que estos sean definidos por las dinámicas de libre competencia del mercado. Esta solicitud la fundamenta en los siguientes 4 puntos:

1. Protección contra el fraude cibernético (Smishing y Spam): Un modelo de precios regulados a la baja incentiva el envío masivo de mensajes fraudulentos, poniendo en riesgo directo a los usuarios del sistema financiero, comercial y de telecomunicaciones.

2. Incentivo a la inversión en seguridad: La desregulación de los precios A2P permite a los operadores generar los ingresos necesarios para sostener, actualizar y fortalecer esta infraestructura crítica de seguridad.

3. Naturaleza del mercado B2B: El ecosistema A2P es un entorno netamente corporativo (Business-to-Business) en el que participan grandes empresas, agregadores e instituciones. En este contexto, los precios responden al valor agregado, la calidad del enrutamiento y la seguridad garantizada en la entrega del mensaje, por lo que el mercado tiene la madurez suficiente para autorregularse sin necesidad de topes artificiales.

4. Migración a canales OTT: Un esquema de precios regulados destruyen la operatividad del SMS y lo hacen inviable frente a sus competidores. Esta asimetría competitiva provocará una migración masiva e irreversible de los clientes hacia WhatsApp.

Concluye que el objetivo de la CRC de proteger a los usuarios. Sin embargo, considera que la mejor forma de lograrlo no es forzando una tarifa a la baja que precarice el servicio, sino permitiendo que el mercado A2P opere bajo libre competencia.

SSC

Señala que el documento soporte contiene un Análisis de Impacto Normativo (AIN) con metodología multicriterio y análisis costo-beneficio. Precisa que no objeta su existencia, sino su contenido, al considerar que, respecto de la medida de bloqueo de llamadas internacionales con CLI nacional, el AIN presenta omisiones concretas y verificables que vician su conclusión.

1. El AIN no cuantificó el tráfico legítimo con CLI nacional cursado por los operadores de LDI. **SSC** sostiene que el análisis costo-beneficio de la alternativa de prohibición total del enmascaramiento del CLI presenta dos defectos: (i) el beneficio se estimó por analogía con experiencias internacionales, sin utilizar información del tráfico internacional entrante en Colombia; y (ii) el costo del bloqueo no incluyó

el tráfico legítimo que quedaría suprimido, pese a que el principal efecto de la medida sería la eliminación de comunicaciones empresariales legítimas. En consecuencia, afirma que el cálculo está estructuralmente sesgado, pues contabiliza el beneficio de bloquear el fraude, pero omite el costo más relevante de la medida. Adicionalmente, señala que el AIN se construyó con información de operadores móviles, sin incluir a los operadores de LDI ni el tráfico internacional entrante, por lo que careció de los datos necesarios para valorar adecuadamente el impacto del bloqueo.

2. El propio AIN reconoce que el monitoreo con etiquetado es la mejor alternativa en materia de voz. Indica que el documento soporte concluye que la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño global. Sin embargo, cuestiona que el AIN no explique por qué ese mismo enfoque no se extendió al tráfico internacional, donde finalmente se optó por el bloqueo, lo que, a su juicio, evidencia una contradicción interna dentro del propio análisis.

3. No se evaluó la pertinencia de reglas diferenciales para los operadores de LDI. Señala que la evaluación realizada sobre cargas diferenciales, en aplicación del artículo 31 de la Ley 1978 de 2019, se limitó a los operadores del ecosistema SMS, A2P y terminación móvil, sin analizar el perfil de los operadores de LDI de voz, cuya estructura y posición en la cadena de valor son diferentes. En consecuencia, considera que la CRC no agotó el análisis de reglas diferenciales respecto de esta categoría de operadores.

TIGO

Manifiesta que la desregulación tarifaria del mercado SMS A2P permitiría generar una señal económica más adecuada para sostener las inversiones exigidas por el nuevo régimen de mitigación del fraude cibernético. A diferencia del SMS P2P y de la voz tradicional, el A2P corresponde a un servicio corporativo B2B con mayor valor agregado, mayores exigencias de calidad, trazabilidad, seguridad, integración y capacidad, y con dinámicas comerciales distintas frente a bancos, plataformas digitales, comercios, entidades públicas, agregadores e integradores. Así mismo indica que permitir la libre negociación de tarifas y capacidades en este mercado facilitaría que los operadores recuperen parte de las inversiones requeridas en firewalls, monitoreo, filtros antifraude, analítica, integración y soporte operativo, evitando que dichas obligaciones deban financiarse exclusivamente con servicios regulados, de bajo margen o en declive. Por ello, señala que la desregulación del SMS A2P no debe entenderse únicamente como una medida de eficiencia comercial, sino como un mecanismo necesario para alinear la política regulatoria antifraude con la sostenibilidad económica de las redes y plataformas que la soportan.

Por el contrario, señala que mantener una tarifa A2P regulada ex ante genera una señal económica equivocada: reduce los ingresos que permiten financiar las plataformas de mensajería, la capacidad adicional, el monitoreo permanente y, precisamente, las herramientas antifraude y los desarrollos de integración que este mismo proyecto exige; y transfiere rentas a los eslabones aguas arriba —PCA, integradores y plataformas globales— sin garantía de traslado al usuario final ni a las empresas que utilizan el servicio. Existe, por tanto, una incoherencia que conviene resolver: no es razonable imponer

al PRST nuevas obligaciones de inversión e integración mientras se congela la remuneración del insumo que debe financiarlas. La sostenibilidad del canal A2P y la viabilidad misma de las inversiones antifraude requieren libertad tarifaria y negociación de capacidades.

Por lo anterior, TIGO solicita que la CRC avance hacia la desregulación tarifaria del SMS A2P, sustituyendo el esquema de tarifa regulada ex ante por un modelo de libre negociación comercial entre PRST, PCA/IT, integradores y originadores de tráfico, con intervención regulatoria únicamente en caso de controversia o de conductas abusivas. En este mismo sentido, solicita que esta definición debería ser concomitante con la entrada en vigencia del nuevo régimen A2P, de modo que las obligaciones de inversión y la señal de remuneración queden alineadas en el tiempo.

En este sentido, puntualmente solicita acompañar el nuevo régimen A2P de la desregulación de la tarifa mayorista del SMS A2P, sustituyendo la tarifa regulada ex ante por un esquema de libre negociación comercial entre PRST, PCA/IT, integradores y originadores, con intervención regulatoria únicamente ante controversia o conductas abusivas, idealmente concomitante con la entrada en vigencia del nuevo régimen, de forma anterior a la entrada en vigencia de las normas aquí dispuestas con por lo menos 6 meses, a su efectiva implementación.

PTC

Señala que, si bien el documento soporte indica que la CRC aplicó metodologías de Análisis Multicriterio, Costo-Beneficio, Costos Administrativos y Simplificación Normativa, estas se limitaron a determinadas temáticas y no se aplicó un análisis de costo-beneficio cuantificado a las medidas más onerosas del proyecto, particularmente la creación del SENDER ID, el Validador Centralizado y el régimen de KYC. Considera que esta omisión resulta contraria a los artículos 2.2.13.3.2 y 2.2.13.3.3 del Decreto 1078 de 2015, pues impide demostrar la proporcionalidad y eficiencia de dichas medidas. En consecuencia, solicita que, antes de expedir la resolución definitiva, la CRC realice un análisis de costo-beneficio específico para estas medidas, que incluya una estimación de la inversión requerida, el impacto esperado en la reducción del fraude y los agentes llamados a asumir cada costo.

Adicionalmente, manifiesta que el negocio A2P se desarrolla dentro de un marco de remuneración regulada, en el que los PRST no cuentan con plena libertad para definir el precio por el uso de su red, pese a que sobre ellos recaen obligaciones técnicas, operativas, de seguridad y gestión del tráfico. En este contexto, sostiene que el crecimiento del tráfico A2P no necesariamente se traduce en una mayor rentabilidad, por lo que las nuevas obligaciones regulatorias deben guardar correspondencia con la remuneración reconocida y preservar el equilibrio económico del negocio regulado. Afirma que la lucha contra el fraude no puede traducirse en la imposición de cargas ilimitadas a los PRST y que toda nueva obligación debe ser técnicamente viable, económicamente eficiente y asignada al agente que se encuentre en mejor posición para prevenir, controlar o corregir el riesgo correspondiente.

Finalmente, señala que la Resolución CRC 8183 de 2026 mantuvo el cargo de acceso para SMS A2P mientras se adelantaba la revisión integral del ecosistema en el marco del presente proyecto regulatorio.

Sin embargo, indica que la Fase I incorpora un conjunto de nuevas obligaciones técnicas y operativas cuyos costos no fueron incorporados a la base de costos que sustenta dicho cargo, la cual solo será revisada en la Fase II. En consecuencia, solicita que la CRC incluya una manifestación expresa indicando que los costos derivados de las obligaciones adoptadas en la Fase I, incluida la tarifa del Validador Centralizado, serán considerados dentro de la base de costos que se evalúe en la revisión de la remuneración del ecosistema A2P. De manera subsidiaria, solicita valorar la procedencia de un mecanismo transitorio de reconocimiento de costos para los PRST, en línea con el principio de causalidad de costos que orienta la regulación de cargos mayoristas.

Respuesta CRC:

Frente a los comentarios presentados por **ANDESCO**, **CLARO**, **ETB**, **SAEM**, **PTC**, **TIGO** y **SINCH**, en los que se cuestiona la decisión de dividir el proyecto regulatorio en dos fases —una primera asociada a la adopción de medidas técnicas para la mitigación del fraude y una segunda dedicada al análisis económico y de remuneración del SMS A2P—, la Comisión considera necesario reiterar la posición expuesta en el documento soporte.

En primer lugar, la CRC reconoce que la remuneración del servicio SMS A2P guarda relación con las medidas antifraude que se adopten sobre dicho ecosistema. Precisamente por ello, en el documento soporte se explicó que, en el marco del proyecto «Esquemas de Remuneración Mayorista de Redes Móviles», la Comisión decidió mantener transitoriamente el esquema de remuneración vigente para SMS A2P, mientras adelantaba una revisión integral de este segmento dentro del presente proyecto, considerando las responsabilidades e incentivos de los agentes que participan en la cadena de valor.

No obstante, la Comisión considera que ello no implica que las medidas técnicas orientadas a prevenir y mitigar el fraude deban postergarse hasta culminar integralmente el análisis económico del mercado A2P. El documento soporte evidencia que el problema regulatorio identificado corresponde a la baja efectividad de las herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto, y que este fenómeno genera afectaciones relevantes para los usuarios, los agentes económicos y la confianza en los servicios de comunicaciones.

En ese sentido, la división del proyecto en dos fases no busca fragmentar artificialmente el análisis regulatorio, sino ordenar la intervención de manera secuencial y coherente. La Fase I está orientada a evaluar y adoptar las medidas regulatorias y técnicas necesarias para prevenir y mitigar el fraude cibernético mediante servicios móviles, incluidas aquellas aplicables al ecosistema SMS A2P. La Fase II, por su parte, estará enfocada en el análisis económico y competitivo del mercado de mensajería SMS A2P y en la evaluación de alternativas regulatorias relacionadas con su esquema de remuneración, incorporando los costos, inversiones, beneficios e impactos derivados de las medidas antifraude que resulten adoptadas.

Esta decisión se justifica, además, porque la Comisión identificó la necesidad de contar con información actualizada sobre la prestación del servicio de mensajería SMS A2P, sus condiciones operativas, económicas y comerciales. Por esta razón, la CRC requirió información adicional a los agentes del mercado, con el propósito de que la evaluación de la remuneración A2P se realice con una base empírica suficiente y no únicamente a partir de supuestos generales. Así, los comentarios relacionados con la remuneración del servicio SMS A2P no son descartados ni diferidos indefinidamente, sino que serán considerados como insumo central de la segunda fase regulatoria. Esta fase contará con un documento independiente de propuesta regulatoria, en el que se evaluarán las alternativas de remuneración aplicables a la terminación de mensajes SMS A2P, considerando las condiciones de competencia, los incentivos a la inversión, la eficiencia, la mitigación de riesgos en el ecosistema digital y la información solicitada por la CRC.

Adicionalmente, para evitar el desbalance señalado por varios agentes entre la adopción de obligaciones técnicas y la definición de su sostenibilidad económica, la Comisión precisó que las medidas técnicas contenidas en la resolución que tienen relación directa con la mensajería A2P quedarán condicionadas en su entrada en vigencia a la publicación en el Diario Oficial del acto administrativo mediante el cual la CRC defina la nueva remuneración aplicable al ecosistema A2P.

En consecuencia, la CRC mantiene la decisión de estructurar el proyecto en dos fases complementarias. Esta aproximación permite avanzar oportunamente en la mitigación del fraude, sin desconocer que la remuneración del SMS A2P requiere un análisis económico específico, soportado en información actualizada y en los costos e impactos derivados de las medidas antifraude que finalmente sean adoptadas.

Frente a los comentarios presentados por **ANDESCO**, **CLARO**, **ETB**, **PTC**, **SAEM** y **SSC**, en los que se manifiesta que el Análisis de Impacto Normativo (AIN) no evaluó un conjunto suficientemente amplio de alternativas regulatorias o que la Comisión debió profundizar en determinados análisis técnicos, económicos o de mercado antes de adoptar las medidas propuestas, la CRC considera pertinente reiterar lo expuesto en el documento soporte.

En primer lugar, es importante recordar que el presente proyecto regulatorio fue desarrollado siguiendo la metodología de Análisis de Impacto Normativo prevista por la Comisión, la cual comprendió las etapas de identificación del problema, definición de objetivos regulatorios, identificación y evaluación de alternativas, consulta pública y análisis de comentarios recibidos. Como resultado de este proceso, la Comisión evaluó diferentes alternativas regulatorias para cada una de las problemáticas identificadas, considerando su efectividad para reducir el fraude, su viabilidad técnica y operativa, así como los costos y beneficios esperados para los distintos agentes involucrados.

En particular, para cada uno de los ejes temáticos analizados, voz y mensajería SMS, el documento soporte expone las alternativas regulatorias consideradas, incluyendo la alternativa de mantener el statu quo, así como distintas opciones regulatorias construidas a partir de la información recopilada durante las mesas técnicas, la participación sectorial, las respuestas a los requerimientos de información y las

observaciones recibidas durante el desarrollo del proyecto. Posteriormente, dichas alternativas fueron sometidas a una evaluación multicriterio que permitió comparar su desempeño frente a criterios de efectividad, eficiencia, proporcionalidad, implementación y consistencia con los objetivos regulatorios.

Así mismo, la Comisión considera importante precisar que el alcance del presente proyecto regulatorio se circunscribe a la adopción de medidas orientadas a fortalecer la prevención y mitigación del fraude mediante servicios tradicionales de voz y SMS. En consecuencia, el análisis desarrollado en el AIN se concentró en aquellas alternativas que guardan una relación directa con el problema regulatorio identificado, razón por la cual no resulta necesario incorporar estudios adicionales sobre aspectos que exceden dicho alcance o que corresponden a otros proyectos regulatorios.

Por otra parte, la CRC observa que varios de los comentarios no proponen alternativas regulatorias nuevas, sino que plantean diferentes aproximaciones para implementar medidas que ya fueron consideradas durante la estructuración del proyecto. En estos casos, las observaciones fueron analizadas como insumos para perfeccionar el diseño regulatorio y la implementación de las medidas, sin que ello implique la necesidad de replantear la totalidad del AIN o de reiniciar el proceso de evaluación de alternativas.

Finalmente, la Comisión considera que la evidencia recopilada durante el desarrollo del proyecto, complementada con la información obtenida mediante los requerimientos de información, los espacios de participación con la industria y los comentarios recibidos durante la consulta pública, constituye un soporte técnico suficiente para adoptar las decisiones regulatorias contenidas en la presente resolución. En consecuencia, la CRC no encuentra necesario realizar estudios adicionales o ampliar el AIN sobre aspectos que ya fueron suficientemente analizados dentro del alcance de este proyecto regulatorio, sin perjuicio de que continúe realizando seguimiento a la efectividad de las medidas adoptadas y evalúe, de ser necesario, la pertinencia de futuras intervenciones regulatorias.

Frente a los comentarios de **ANDESCO**, **CLARO**, **ETB**, **PTC**, **SAEM**, **SINCH** y **TIGO**, en los que se señala que las medidas regulatorias propuestas podrían generar cargas económicas para los agentes del ecosistema A2P y que, por tanto, la definición de la remuneración debería preceder la adopción de dichas obligaciones, la Comisión considera pertinente realizar las siguientes precisiones.

La CRC coincide en que la sostenibilidad económica del ecosistema A2P constituye un elemento esencial para el éxito de la intervención regulatoria. Precisamente por esta razón, la Comisión decidió trasladar el análisis de la remuneración del servicio SMS A2P a una segunda fase del presente proyecto regulatorio, con el propósito de que dicho análisis incorpore los costos, inversiones y beneficios asociados a las medidas técnicas que finalmente sean adoptadas para la mitigación del fraude.

Esta aproximación responde a un criterio metodológico propio del Análisis de Impacto Normativo. En efecto, la remuneración constituye un instrumento económico para soportar la implementación de las obligaciones regulatorias, mas no un elemento que determine cuáles medidas son necesarias para corregir el problema regulatorio identificado. Por ello, resulta técnicamente más consistente definir

primero las medidas orientadas a mitigar el fraude y, posteriormente, evaluar el esquema de remuneración que permita financiarlas de manera eficiente y sostenible.

En ese sentido, la Comisión reitera que el análisis que se desarrollará en la segunda fase incorporará los costos de implementación, operación y mantenimiento derivados de las medidas regulatorias adoptadas, así como los beneficios esperados en términos de reducción del fraude, fortalecimiento de la confianza en el ecosistema y mejora en la eficiencia del servicio.

Finalmente, la CRC recuerda que el proyecto prevé que las medidas regulatorias cuya implementación depende del nuevo esquema de remuneración del ecosistema A2P quedarán condicionadas a la expedición del acto administrativo mediante el cual se defina dicha remuneración. De esta manera, se garantiza la coherencia entre las obligaciones regulatorias y el esquema económico que soportará su implementación, preservando la sostenibilidad del ecosistema A2P.

Frente a los comentarios de **TIGO**, **SINCH** y **ANDESCO**, en los que se propone sustituir el esquema de remuneración regulada por un modelo de libre negociación o desregular total o parcialmente la remuneración del servicio SMS A2P, la Comisión considera que dichas propuestas corresponden al análisis económico y competitivo propio del mercado de mensajería A2P y, por tanto, exceden el alcance de la presente fase del proyecto regulatorio.

Como se explicó previamente, la presente actuación regulatoria tiene por objeto evaluar y adoptar las medidas regulatorias y técnicas orientadas a fortalecer la prevención y mitigación del fraude mediante servicios móviles. En consecuencia, las propuestas relacionadas con la modificación del esquema de remuneración, incluyendo aquellas que plantean la desregulación total o parcial del servicio SMS A2P, serán analizadas en la segunda fase del proyecto regulatorio, la cual estará dedicada exclusivamente a evaluar las distintas alternativas regulatorias aplicables al mercado de mensajería A2P.

En dicho escenario, la Comisión analizará, con fundamento en la información recopilada mediante los requerimientos de información, los comentarios recibidos durante la consulta pública y el correspondiente Análisis de Impacto Normativo, las diferentes alternativas de remuneración, incluyendo el mantenimiento del esquema vigente, su modificación o la eventual adopción de mecanismos de libre negociación, evaluando para cada una de ellas sus efectos sobre la competencia, la eficiencia económica, la inversión, la sostenibilidad del ecosistema y los incentivos para la mitigación del fraude.

En consecuencia, la CRC no acoge en esta fase las solicitudes orientadas a modificar el esquema de remuneración del servicio SMS A2P, por cuanto dicha discusión será objeto de evaluación integral dentro de la segunda fase del presente proyecto regulatorio, en el marco del documento específico que se expedirá para ese propósito.

Frente a los comentarios de **ETB**, **INALAMBRIA** y **Colombia Fintech**, en los que se solicita establecer obligaciones diferenciadas para determinados agentes del mercado o ampliar los plazos previstos para

la implementación del nuevo ecosistema A2P, la Comisión considera pertinente realizar las siguientes precisiones.

En primer lugar, la CRC comparte la importancia de que la implementación de las medidas regulatorias se realice de manera gradual y con plazos que permitan a los diferentes actores adelantar los desarrollos tecnológicos, operativos y contractuales requeridos. En atención a estas observaciones, la Comisión ajusta el cronograma previsto en el proyecto regulatorio y amplía a doce (12) meses el plazo para la implementación del validador centralizado y de las obligaciones asociadas al nuevo ecosistema A2P, plazo que se considera suficiente para adelantar el proceso de selección del Validador, el desarrollo de las interfaces tecnológicas, las pruebas de interoperabilidad, la integración de los diferentes actores y la puesta en operación del modelo.

Por otra parte, la Comisión no considera procedente establecer esquemas regulatorios diferenciados entre los distintos agentes del ecosistema. Las medidas adoptadas buscan garantizar la autenticidad de los remitentes, la integridad de la información y la trazabilidad de las comunicaciones A2P, objetivos que únicamente pueden alcanzarse mediante la participación coordinada de todos los actores que intervienen en la cadena de valor. En consecuencia, la aplicación uniforme de las obligaciones constituye un elemento esencial para asegurar la interoperabilidad del modelo y evitar la generación de brechas que puedan ser aprovechadas para la materialización de actividades fraudulentas. Lo anterior no desconoce las diferencias existentes entre los agentes del mercado. Precisamente por ello, el modelo regulatorio concentra las actividades especializadas de validación en un único validador centralizado y establece un periodo de transición suficiente para facilitar la adaptación de todos los participantes al nuevo esquema operativo, reduciendo los costos de implementación y favoreciendo economías de escala en beneficio del ecosistema.

En consecuencia, la Comisión acoge parcialmente las observaciones recibidas, en consistencia con lo establecido por esta Comisión en la sección 6.1 denominado «Régimen de transición», ampliando el plazo de implementación del modelo regulatorio, pero mantiene la aplicación uniforme de las obligaciones previstas para los agentes que participan en el ecosistema A2P, por considerar que ello resulta necesario para garantizar la efectividad de las medidas de mitigación del fraude, la interoperabilidad del sistema y condiciones homogéneas de operación para todos los participantes.

6.3 Definiciones

CLARO

Sobre la definición de CODIGO CORTO A2P: Señala que el proyecto no discrimina sectores y solicita que la industria bancaria, el gobierno y los servicios de salud, por tratarse de tráfico crítico, utilicen códigos cortos A2P exclusivos y dedicados, prohibiendo que compartan el mismo código con mensajes de marketing o entretenimiento.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Sobre la definición de INTEGRADOR TECNOLÓGICO: Manifiesta que la regulación debe prohibir expresamente la «subagregación» ciega o exigir que el Integrador Tecnológico responda solidariamente por los terceros intermedios, pues de lo contrario se rompe la trazabilidad del fraude al permitir que «subagregadores» utilicen la conexión del Integrador sin un proceso individual de KYC ante el Validador Centralizado. Así mismo, considera que la definición presenta una inconsistencia, al indicar que el Integrador Tecnológico no tiene conexión directa con los PRSTM. Afirma que, técnicamente, el Integrador Tecnológico sí tiene conexión directa con la red del operador móvil y que quienes carecen de dicha conexión son los PCA. En consecuencia, solicita ajustar la definición para evitar que se confunda la figura del Integrador Tecnológico con la de un subagregador o revendedor informal.

Sobre la definición de PROVEEDOR DE CONTENIDOS Y APLICACIONES (PCA): Señala que la definición debería establecer expresamente que la condición de PCA está sujeta a la aprobación previa del procedimiento de KYC ante el Validador Centralizado, con el fin de evitar que actores maliciosos puedan acceder al ecosistema A2P. Adicionalmente, advierte sobre el riesgo de los PCA internacionales («Offshore PCA»), al considerar que el proyecto no define cómo estos actores obtendrán un SENDER ID ni exige la existencia de un representante legal en Colombia o un mecanismo de homologación internacional para el KYC. En consecuencia, solicita que la regulación incorpore reglas específicas para garantizar la identificación y trazabilidad de estos proveedores internacionales.

SIC

Se sugiere la inclusión en el «proyecto» de las definiciones de los siguientes conceptos:

- MECANISMO DE VALIDACIÓN.
- MECANISMO DE AUTENTICACIÓN.

Se considera importante crear una definición general, sin ser restrictiva de lo que se entiende por mecanismo de validación y mecanismo de autenticación, dependiendo el contexto. El primero de ellos aplicaría para el tráfico (A2P), el segundo, para el tráfico (P2P) y otros trámites.

Lo anterior, con el fin de que, para aquellas transacciones o trámites que requieran la plena verificación de la identidad del usuario o suscriptor, se utilicen herramientas robustas como la biometría obligatoria, por ejemplo, si se trata de trámites presenciales.

Respuesta CRC:

Frente a los comentarios presentados por **CLARO** sobre las definiciones de Código Corto A2P, Integrador Tecnológico y Proveedor de Contenidos y Aplicaciones (PCA), la Comisión considera pertinente realizar las siguientes precisiones.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En primer lugar, las definiciones contenidas en el proyecto de resolución tienen como finalidad establecer el alcance conceptual de los actores y recursos que participan en el ecosistema A2P, procurando que estas sean claras, técnicamente consistentes y suficientemente generales para permitir la evolución del mercado y de las tecnologías asociadas. Por esta razón, la Comisión considera que las definiciones no constituyen el escenario adecuado para incorporar obligaciones regulatorias específicas, condiciones de operación o requisitos cuyo desarrollo corresponde a otros apartados de la regulación. En ese sentido, la CRC no considera procedente incorporar dentro de la definición de Código Corto A2P aspectos relacionados con la exclusividad de determinados sectores económicos o con restricciones sobre el uso compartido de los códigos cortos, por cuanto tales decisiones corresponden al diseño del régimen de asignación y utilización de los recursos de identificación, y no a su definición conceptual.

Así mismo, la Comisión no acoge la propuesta de incorporar una diferenciación regulatoria entre Integradores Tecnológicos y Subagregadores, por cuanto el modelo regulatorio adoptado no contempla esquemas de subagregación del tráfico SMS A2P. En consecuencia, todo Integrador Tecnológico que participe en el ecosistema deberá cumplir directamente las obligaciones previstas en la regulación, incluyendo aquellas relacionadas con la identificación y validación de los agentes con los que mantiene relaciones comerciales, preservando así la trazabilidad del tráfico y la efectividad de las medidas orientadas a la mitigación del fraude.

Finalmente, en relación con la definición de Proveedor de Contenidos y Aplicaciones (PCA), la Comisión considera que esta debe limitarse a identificar el rol funcional que desempeña dicho agente dentro del ecosistema, sin incorporar requisitos asociados a su habilitación para operar. En consecuencia, la calidad de PCA no depende de la definición contenida en la regulación, sino del cumplimiento de las obligaciones previstas en el nuevo régimen A2P, incluyendo los procesos de identificación, validación documental y conocimiento del cliente (KYC), así como las demás condiciones establecidas para acceder y permanecer en el ecosistema.

En consecuencia, la Comisión no acoge las modificaciones propuestas a las definiciones de Integrador Tecnológico y Proveedor de Contenidos y Aplicaciones, por considerar que estas reflejan adecuadamente el alcance conceptual de dichos agentes y que las obligaciones relacionadas con el KYC, la trazabilidad, las responsabilidades de los Integradores Tecnológicos y las condiciones para operar en el ecosistema A2P se encuentran desarrolladas en las disposiciones sustantivas del Capítulo 13. Por su parte, la Comisión no considera procedente incorporar restricciones adicionales dentro de la definición de Código Corto A2P, por corresponder estas al régimen de administración y utilización de los recursos de identificación y no a su definición conceptual.

Frente a los comentarios de **CLARO** relacionados con la subagregación, los procesos de conocimiento del cliente (KYC), el tratamiento de los Proveedores de Contenidos y Aplicaciones (PCA) internacionales y la trazabilidad del tráfico SMS A2P, la Comisión considera que estos aspectos no corresponden al alcance de las definiciones contenidas en el proyecto de resolución, sino al régimen de obligaciones aplicable a los diferentes agentes del ecosistema.

En efecto, el Capítulo 13 establece las obligaciones que deben cumplir los Integradores Tecnológicos y los PCA para operar en el ecosistema A2P, incluyendo los procesos de identificación, validación documental y conocimiento del cliente (KYC), así como las medidas orientadas a garantizar la trazabilidad de las comunicaciones y la autenticidad de los remitentes. De igual forma, el modelo regulatorio no contempla esquemas de subagregación del tráfico SMS A2P, razón por la cual no resulta procedente incorporar disposiciones específicas sobre dicha figura dentro de las definiciones. En consecuencia, la Comisión no acoge las modificaciones propuestas, por considerar que las materias planteadas ya se encuentran desarrolladas en las disposiciones sustantivas del proyecto regulatorio y no corresponden al objeto de las definiciones incorporadas en la regulación.

Frente a los comentarios de la **SIC**, mediante los cuales se propone incorporar las definiciones de «mecanismo de validación» y «mecanismo de autenticación», así como hacer referencia a tecnologías específicas como la biometría para determinados trámites, la Comisión considera pertinente realizar las siguientes precisiones.

La CRC comparte la importancia de que los mecanismos de validación y autenticación proporcionen niveles adecuados de seguridad y confiabilidad. No obstante, considera que las definiciones regulatorias deben preservar el principio de neutralidad tecnológica, evitando hacer referencia a tecnologías o soluciones específicas que puedan limitar la innovación o requerir modificaciones regulatorias cada vez que evolucionen las tecnologías disponibles.

En este sentido, la regulación establece las funcionalidades y objetivos que deben cumplir los mecanismos de validación y autenticación, dejando a los agentes la posibilidad de implementar las soluciones tecnológicas que resulten más adecuadas, siempre que satisfagan los requisitos de seguridad, confiabilidad y trazabilidad previstos en la regulación.

En consecuencia, la Comisión no acoge la incorporación de referencias expresas a tecnologías específicas dentro de las definiciones, por considerar que ello podría restringir la evolución tecnológica del ecosistema y resultar incompatible con el principio de neutralidad tecnológica que orienta la actuación regulatoria de la CRC. No obstante, la utilización de mecanismos robustos de autenticación podrá implementarse cuando ello resulte necesario para dar cumplimiento a las obligaciones previstas en la regulación o en otras disposiciones legales aplicables.

6.4 Portabilidad

CLARO

El proyecto regulatorio sometido a consulta tiene como objetivo fortalecer las medidas de prevención y mitigación del fraude en las redes y servicios de telecomunicaciones, así como incrementar la seguridad de las comunicaciones electrónicas utilizadas por los usuarios para acceder a servicios financieros, comerciales, gubernamentales y digitales.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En este contexto, se considera necesario que la CRC incorpore una disposición específica orientada a garantizar que los Proveedores de Contenidos y Aplicaciones (PCA), así como los demás agentes que originan tráfico de mensajería asociado a procesos de autenticación, validación o seguridad, consulten de manera permanente la información de portabilidad numérica disponible en la Base de Datos Administrativa (ABD), preferiblemente en tiempo real y, como mínimo, mediante actualizaciones diarias.

Actualmente se ha evidenciado que algunos agentes realizan consultas a la ABD con periodicidades amplias, incluso quincenales, situación que genera desfases entre la red a la que efectivamente pertenece un usuario y la información utilizada para el enrutamiento de mensajes. Como consecuencia, los usuarios que han ejercido su derecho a la portabilidad numérica pueden experimentar fallas en la recepción de mensajes de texto esenciales para su interacción con diferentes servicios.

Esta situación resulta especialmente crítica cuando se trata de mensajes utilizados para autenticación de identidad, códigos de verificación de doble factor, confirmación de transacciones financieras, alertas de seguridad bancaria, validación de operaciones comerciales, recuperación de credenciales de acceso y demás comunicaciones asociadas a la protección de los usuarios frente a posibles fraudes.

La no entrega oportuna de este tipo de mensajes no solo afecta la experiencia del usuario, sino que puede generar riesgos de seguridad, impedir la ejecución de operaciones legítimas, dificultar la autenticación de identidad y afectar la confianza en los mecanismos de protección implementados por las entidades financieras, los proveedores de servicios digitales y los propios operadores de telecomunicaciones.

Resulta contradictorio que un proyecto regulatorio orientado a fortalecer la lucha contra el fraude no contemple medidas que garanticen la correcta entrega de los mensajes utilizados precisamente para la autenticación, validación y protección de los usuarios. La actualización oportuna de la información de portabilidad constituye un elemento esencial para asegurar la efectividad de dichos mecanismos de seguridad.

Por lo anterior, se solicita a la CRC evaluar la inclusión de una disposición que obligue a los agentes que originan tráfico de mensajería hacia usuarios móviles a consultar la información de portabilidad numérica disponible en la ABD en tiempo real o, en su defecto, con una periodicidad máxima diaria, garantizando así la correcta identificación de la red de destino y la entrega efectiva de los mensajes asociados a procesos de autenticación, seguridad y validación de transacciones.

Esta medida contribuiría de manera directa al cumplimiento de los objetivos perseguidos por el proyecto regulatorio, fortaleciendo la protección de los usuarios y reduciendo riesgos derivados de la no recepción de comunicaciones críticas para la prevención del fraude.

Respuesta CRC:

Frente al comentario presentado por **CLARO**, mediante el cual se propone incorporar una obligación para que los agentes que originan tráfico de mensajería consulten de manera permanente la información de portabilidad numérica contenida en la Base de Datos Administrativa (ABD), con el propósito de garantizar la correcta entrega de mensajes utilizados en procesos de autenticación, validación y seguridad, la Comisión considera pertinente realizar las siguientes precisiones.

La CRC observa que la obligación propuesta regula aspectos relacionados con el encaminamiento del tráfico y el uso de la Base de Datos Administrativa de Portabilidad Numérica, materias que hacen parte del régimen regulatorio específico de la Portabilidad Numérica Móvil. En este sentido, el objeto del presente proyecto regulatorio consiste en identificar e implementar medidas orientadas a prevenir y mitigar el fraude cibernético mediante servicios móviles, particularmente a través de mecanismos de autenticación, validación, trazabilidad e intercambio de información entre los diferentes actores del ecosistema. Por lo tanto, la incorporación de nuevas obligaciones relacionadas con la frecuencia de consulta de la Base de Datos Administrativa excede el alcance de esta actuación regulatoria y requeriría un análisis específico dentro del marco regulatorio aplicable a la Portabilidad Numérica Móvil.

En consecuencia, la Comisión no acoge la propuesta presentada, sin perjuicio de que la temática pueda ser objeto de evaluación en el marco de futuros proyectos regulatorios relacionados con la administración y funcionamiento de la Portabilidad Numérica Móvil.

6.5 Sobre los OMV

ETB

Solicita a la Comisión considerar de manera expresa las particularidades técnicas, operativas y económicas de los Operadores Móviles Virtuales (OMV) dentro del diseño regulatorio, al señalar que, aunque son responsables del cumplimiento de las obligaciones regulatorias, su capacidad de implementación material difiere sustancialmente de la de los operadores con infraestructura propia. Indica que funcionalidades como la señalización, el transporte de tráfico, la mensajería, el monitoreo en tiempo real, la detección de patrones de fraude, la autenticación de comunicaciones, la validación de identificadores y la ejecución de bloqueos o etiquetados preventivos dependen de plataformas y sistemas sobre los cuales el OMV no tiene administración ni control directo, sino que requieren desarrollos tecnológicos, integraciones, adecuaciones de red y procesos de interoperabilidad que deben ser ejecutados por los Operadores Móviles de Red (OMR).

En este contexto, considera necesario que la regulación incorpore expresamente el principio de control efectivo de la red, de manera que las obligaciones técnicas recaigan sobre el actor que efectivamente administra los elementos de red y las plataformas donde deben ejecutarse las funcionalidades exigidas

por la regulación, evitando imponer a los OMV responsabilidades respecto de actividades que dependen materialmente de terceros y que podrían generar escenarios de incumplimiento involuntario.

Finalmente, señala que los plazos de implementación propuestos no reflejan la complejidad técnica que implica coordinar desarrollos entre OMV, OMR, carriers internacionales, proveedores tecnológicos, PCA, actores financieros y demás participantes del ecosistema. En consecuencia, solicita que la CRC contemple esquemas de implementación diferenciados para los OMV, reconozca expresamente las limitaciones derivadas de su dependencia tecnológica respecto de terceros y adopte plazos de transición acordes con la complejidad de los desarrollos requeridos.

Respuesta CRC:

Frente a los comentarios presentados por **ETB**, mediante los cuales solicita establecer un tratamiento regulatorio diferenciado para los Operadores Móviles Virtuales (OMV), reconocer expresamente las limitaciones derivadas de su dependencia tecnológica respecto de los Operadores Móviles de Red (OMR) y ampliar los plazos de implementación de las medidas propuestas, la Comisión considera pertinente realizar las siguientes precisiones.

En primer lugar, la CRC reconoce que los OMV presentan particularidades operativas derivadas de su modelo de negocio y de la utilización de infraestructura provista por terceros. No obstante, el proyecto regulatorio distribuye las obligaciones entre los distintos actores del ecosistema conforme a las funciones que cada uno desempeña y al ámbito de control que ejercen sobre los procesos regulados. En consecuencia, las obligaciones previstas en la resolución recaen sobre el agente que cuenta con la capacidad técnica, operativa o contractual para su cumplimiento, sin trasladar responsabilidades respecto de actividades que materialmente corresponden a otros participantes del ecosistema.

Así mismo, la Comisión no considera procedente establecer un régimen regulatorio diferenciado para los OMV. Las medidas adoptadas tienen como finalidad garantizar la autenticidad, trazabilidad y seguridad de las comunicaciones, objetivos que requieren una implementación homogénea por parte de todos los agentes que intervienen en el ecosistema A2P, sin perjuicio de que cada uno las materialice conforme a su modelo operativo y a las relaciones contractuales que mantenga con los demás participantes.

Por otra parte, la CRC comparte la necesidad de contar con un periodo de transición suficiente para adelantar los desarrollos tecnológicos, contractuales y operativos requeridos para la implementación del nuevo modelo. En atención a los comentarios recibidos durante la consulta pública, la Comisión ajustó el cronograma previsto en el proyecto regulatorio, ampliando a doce (12) meses el plazo para la implementación del validador centralizado y de las medidas asociadas al ecosistema A2P, término que se considera razonable para realizar las adecuaciones necesarias y coordinar las actividades entre los diferentes actores involucrados.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

En consecuencia, la Comisión acoge parcialmente el comentario, en el sentido de ampliar el plazo de implementación del modelo regulatorio; sin embargo, no acoge la solicitud de establecer un esquema regulatorio diferenciado para los OMV, por considerar que las obligaciones previstas en el proyecto ya se encuentran distribuidas de acuerdo con las competencias y funciones de cada agente, y que la efectividad de las medidas de mitigación del fraude requiere un marco regulatorio uniforme para todos los participantes del ecosistema.