Bogotá, 23 de junio de 2026

Doctor
FELIPE AUGUSTO DÍAZ SUAZA
Director Ejecutivo
COMISIÓN DE REGULACIÓN DE COMUNICACIONES – CRC
Calle 59 A Bis No.5-53 piso 9 Edificio Link Siete Sesenta
Bogotá

Asunto: Comentarios COMCEL a los documentos: IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES y a la propuesta de resolución *"Por medio de la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones"*

Estimado Doctor Díaz,

En atención a la publicación para comentarios de los documentos indicados en el Asunto, de manera respetuosa nos permitimos presentar los comentarios de la siguiente manera:

El proyecto regulatorio tiene por objeto central **definir e implementar un conjunto de medidas regulatorias orientadas a prevenir, mitigar y gestionar el fraude en los servicios móviles**, particularmente en comunicaciones de voz y SMS. Para ello, la CRC pretende intervenir en distintos eslabones del ecosistema —PRST, agregadores, plataformas tecnológicas y usuarios— mediante mecanismos que en su criterio mejoran la trazabilidad del tráfico, la identificación de los originadores y el control sobre el uso de la numeración, intentando con ello reducir prácticas como la suplantación, el envío masivo de mensajes fraudulentos y el uso indebido de recursos de red.

En esta oportunidad presenta dos documentos, el primero, un documento soporte titulado: IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES y un proyecto de resolución modificando y adicionando aspectos regulatorios a la Resolución CRC No. 5050 de 2016.

1. **COMENTARIOS AL DOCUMENTO SOPORTE "IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES"**

1.1. Ausencia de análisis económico asociado a la terminación de SMS A2P

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

El proyecto regulatorio fue concebido inicialmente sin incorporar un análisis económico sobre el valor de terminación de los mensajes SMS, a pesar de tratarse de un elemento estructural para el funcionamiento eficiente del mercado. De manera paralela a su desarrollo, la CRC adelantaba otro proceso regulatorio orientado a definir los esquemas de remuneración de los servicios mayoristas en redes móviles, dentro del cual se determinó que la terminación de un SMS tendría un valor de referencia de $0,03.

Posteriormente, a partir de los comentarios presentados por diversos actores del sector al proyecto regulatorio de FRAUDE CIBERNÉTICO, en donde diferentes actores solicitaron expresamente considerar dicha referencia tarifaria y analizar las particularidades del segmento de mensajería empresarial, la Comisión decidió mantener transitoriamente el esquema vigente para los servicios SMS A2P y trasladar el análisis específico de dicho mercado al presente proyecto regulatorio, reconociendo que este segmento presenta características particulares en términos de estructura de mercado, condiciones de prestación, incentivos económicos y riesgos asociados al fraude cibernético.

Sin embargo, en la presente etapa regulatoria la CRC deja nuevamente de lado el análisis de la tarifa de terminación de SMS A2P y de los mecanismos económicos asociados a la prestación de este servicio, mientras propone simultáneamente la adopción de medidas significativamente más exigentes desde el punto de vista técnico, operativo y económico. Entre ellas se encuentran nuevas obligaciones de validación de remitentes, mecanismos de autenticación, sistemas de trazabilidad, controles adicionales sobre el tráfico de mensajes, intercambios de información mediante plataformas tecnológicas y otras exigencias que necesariamente implicarán inversiones relevantes en infraestructura, desarrollos tecnológicos, adecuaciones operativas y mayores cargas administrativas para los agentes involucrados.

Esta aproximación desconoce la relación directa que existe entre las obligaciones regulatorias impuestas a los agentes y los mecanismos de recuperación de costos necesarios para garantizar la sostenibilidad de dichas obligaciones. La ausencia de un análisis económico integral puede generar desincentivos a la inversión, barreras a la permanencia o participación eficiente de algunos actores, afectaciones a la competencia en mercados conexos y traslados de costos a usuarios finales o clientes empresariales.

Adicionalmente, al diferir nuevamente el análisis económico para una eventual fase posterior, se fragmenta la intervención regulatoria, se generan riesgos de inconsistencias normativas y se limita la posibilidad de evaluar de manera integral los impactos costo-beneficio de las medidas propuestas. En estas condiciones, no resulta posible determinar si las obligaciones planteadas son efectivamente proporcionales, eficientes y sostenibles.

Esta situación resulta particularmente contradictoria si se tiene en cuenta que la propia CRC reconoce en el documento soporte que aún requiere realizar un análisis sobre la prestación del servicio de

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

mensajería SMS A2P, sus condiciones operativas, económicas y comerciales, razón por la cual ha solicitado información adicional a algunos agentes del mercado. Si la Comisión considera que actualmente no cuenta con los elementos necesarios para comprender integralmente el funcionamiento de este segmento, resulta prematuro avanzar en la adopción de obligaciones regulatorias que impactan directamente dicho mercado.

En consecuencia, la expedición de una regulación definitiva debería estar acompañada de un análisis integral que incorpore simultáneamente los aspectos técnicos, operativos y económicos del ecosistema de mensajería empresarial. Solo de esta manera será posible verificar la proporcionalidad de las medidas propuestas, garantizar una adecuada asignación de incentivos entre los distintos actores de la cadena de valor y asegurar que las obligaciones regulatorias contribuyan efectivamente a la mitigación del fraude sin generar distorsiones competitivas o ineficiencias de mercado.

Finalmente, preocupa que la CRC tampoco haya realizado un análisis de fondo respecto de las observaciones formuladas por múltiples agentes frente a algunas de las medidas estructurales propuestas, particularmente aquellas relacionadas con la creación de un sistema centralizado de validación y la implementación de mecanismos de Sender ID.

En efecto, pese a que los distintos actores presentaron comentarios detallados sobre aspectos tales como riesgos de concentración, gobernanza del sistema, costos de implementación, responsabilidades operativas, seguridad de la información, riesgos competitivos y posibles afectaciones a la innovación, las respuestas contenidas en los documentos publicados por la CRC se limitan esencialmente a resumir las posiciones expuestas por los participantes y a señalar que los aportes recibidos constituyen insumos para evaluar la proporcionalidad de las alternativas regulatorias y los riesgos competitivos y operativos asociados a su implementación. No obstante, no se evidencia una valoración técnica individual de las observaciones formuladas ni una explicación concreta sobre las razones que justificarían la adopción, modificación o descarte de cada una de las alternativas planteadas por la industria.

Lo anterior cobra especial relevancia si se tiene en cuenta que el esquema de validación centralizada y los mecanismos de Sender ID constituyen pilares fundamentales de la propuesta regulatoria actual. Por tanto, antes de avanzar hacia la imposición de obligaciones concretas, resulta indispensable que la Comisión responda de manera sustantiva los cuestionamientos formulados por los agentes y publique un análisis detallado de los impactos técnicos, operativos, económicos y competitivos asociados a dichas medidas.

La principal preocupación radica en que el documento soporte no demuestra que la implementación de un esquema centralizado de validación y autenticación constituya la alternativa regulatoria más eficiente para mitigar el fraude cibernético asociado a servicios móviles.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Si bien la CRC identifica potenciales beneficios derivados de mecanismos de validación ex ante, el documento no incorpora una comparación rigurosa entre dicha alternativa y otras herramientas regulatorias ya existentes o susceptibles de fortalecimiento, las cuales podrían generar resultados equivalentes o incluso superiores con menores costos de implementación y menores riesgos operativos.

Particularmente, llama la atención que la Comisión **no haya evaluado de manera detallada la efectividad de mecanismos actualmente disponibles, tales como los procedimientos de suspensión provisional de códigos cortos, las medidas de bloqueo de tráfico irregular, los sistemas de monitoreo y detección temprana de patrones fraudulentos, ni las actuaciones coordinadas entre operadores y autoridades competentes.**

Tampoco se evidencia un análisis cuantitativo que compare los costos y beneficios asociados a cada alternativa regulatoria. Si bien es cierto que la CRC reconoce que algunas medidas son costosas, no analiza en detalle que son medidas que van a garantizar que no se envíen más mensajes o se hagan más llamadas con fines fraudulentos.

La implementación de un esquema centralizado implicaría la creación de nuevas infraestructuras tecnológicas, mecanismos de gobernanza, procedimientos de validación, procesos de auditoría, esquemas de administración de información y responsabilidades operativas adicionales para todos los actores involucrados.

En consecuencia, la Comisión no ha acreditado que la alternativa seleccionada corresponda efectivamente a la medida menos gravosa ni a la más eficiente para alcanzar los objetivos perseguidos. Por el contrario, la información disponible permite considerar que el fortalecimiento de mecanismos regulatorios ya existentes —particularmente aquellos asociados a monitoreo, detección temprana, suspensión provisional y acciones coordinadas de control— podría generar beneficios comparables con menores costos regulatorios y menores riesgos para la competencia, la innovación y la operación del mercado.

Por lo anterior, antes de avanzar hacia la implementación de mecanismos centralizados de validación o autenticación obligatoria, la CRC debería realizar una evaluación exhaustiva de la efectividad de las medidas actualmente vigentes, identificar eventuales oportunidades de mejora y demostrar, 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, y permitir en un tiempo razonable que los diferentes agentes del sector analicen dicho estudio.

Así las cosas, Comcel considera que la adopción de obligaciones relacionadas con validación de remitentes, autenticación de mensajes y nuevas exigencias operativas no puede analizarse de manera aislada de la estructura económica que soportará el funcionamiento del esquema.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

En particular, no resulta posible determinar la viabilidad y proporcionalidad de las medidas propuestas mientras no exista claridad respecto de:

- 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.

La ausencia de esta información impide que los agentes puedan valorar adecuadamente el impacto económico del proyecto y limita la capacidad de la CRC para demostrar que la regulación propuesta resulta eficiente y proporcionada.

1.2. La propuesta no demuestra la necesidad de crear un tercero centralizado para la validación de remitentes y desconoce las competencias que actualmente ejerce la CRC como administradora de los recursos de identificación

Comcel observa que la propuesta regulatoria parte de la premisa según la cual 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 asociada a los remitentes habilitados para el envío de mensajes.

No obstante, el documento soporte no demuestra por qué dichas funciones no podrían ser desarrolladas directamente por la propia CRC en ejercicio de las competencias que actualmente le han sido atribuidas por la Ley y por el marco regulatorio vigente.

De conformidad con el artículo 22 de la Ley 1341 de 2009, la CRC tiene a su cargo la administración de los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones. En desarrollo de dicha competencia, mediante la Resolución CRC 5968 de 2020 se consolidó el Régimen de Administración de Recursos de Identificación contenido en el Título VI de la Resolución CRC 5050 de 2016, dentro del cual se encuentran incluidos los códigos cortos para SMS y USSD.

En particular, la regulación vigente establece que la CRC administra la asignación de códigos cortos, verifica el cumplimiento de los requisitos para su otorgamiento, mantiene información sobre los asignatarios, controla el uso eficiente del recurso, adelanta procesos de recuperación cuando se presentan incumplimientos y ejerce funciones permanentes de administración sobre este recurso público escaso.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Lo anterior implica que la Comisión ya dispone de una parte sustancial de la información requerida para identificar a los titulares de los códigos cortos, conocer las condiciones bajo las cuales fueron asignados, verificar los servicios asociados a dichos recursos e incluso adelantar actuaciones administrativas cuando detecta usos presuntamente irregulares.

Sin embargo, el documento soporte no explica por qué estas capacidades institucionales resultarían insuficientes para soportar mecanismos de validación y autenticación de remitentes, ni presenta evidencia que permita concluir que la creación de un tercero centralizado generaría beneficios superiores a los que podrían obtenerse mediante el fortalecimiento de las herramientas regulatorias e institucionales actualmente existentes.

Adicionalmente, la propuesta no contiene un análisis detallado sobre aspectos esenciales para la creación de dicho tercero, tales como mecanismos de supervisión, régimen de responsabilidad, tratamiento de información sensible, estándares de ciberseguridad, manejo de incidentes, conflictos de interés y mecanismos de resolución de controversias.

La ausencia de este análisis resulta especialmente relevante si se considera que la creación de un nuevo intermediario incorporaría costos adicionales para todos los actores del ecosistema, generaría nuevas dependencias operativas y tecnológicas y podría introducir riesgos de concentración en un mercado que actualmente opera bajo esquemas descentralizados.

Desde la perspectiva del Análisis de Impacto Normativo, la carga de la prueba recae sobre la CRC para demostrar que la creación de un nuevo actor constituye la alternativa más eficiente, proporcional y menos gravosa para alcanzar los objetivos perseguidos. No obstante, el documento soporte no presenta una evaluación comparativa entre esta alternativa y otras opciones regulatorias menos intrusivas, tales como el fortalecimiento de los mecanismos de administración actualmente ejercidos por la propia CRC sobre los recursos de identificación.

En consecuencia, antes de imponer la creación de un esquema centralizado de validación, la Comisión debería demostrar por qué las funciones asociadas a la verificación de remitentes no pueden ser desarrolladas dentro del marco institucional existente y por qué resulta necesario trasladar dichas actividades a un tercero, considerando los costos, riesgos e impactos competitivos que ello supone, máxime cuando el mercado fue recientemente intervenido con una tarifa de terminación de $0,03 por SMS.

1.3. Validación de la relación directa entre la propuesta y una reducción efectiva del fraude cibernético.

Si bien compartimos 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

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

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, 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, 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 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 que las actividades fraudulentas migren hacia otros canales que presenten menores restricciones regulatorias o menores costos de operación, luego de realizar estas cuantiosas inversiones.

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, el documento soporte no contiene un análisis de sustitución o desplazamiento del fraude entre canales de comunicación.

En consecuencia, es necesario que antes de adoptar nuevas obligaciones, se debe complementar 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 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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Asimismo, 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.

Más aún, 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.

2. MEDIDAS PROPUESTAS QUE APORTAN POSITIVAMENTE A LA MITIGACIÓN DEL FRAUDE

Es importante reconocer el esfuerzo realizado por la CRC para identificar mecanismos orientados a fortalecer la protección de los usuarios frente a las diferentes modalidades de fraude que afectan los servicios móviles. En particular, considera que algunas de las medidas incluidas en la propuesta regulatoria constituyen herramientas razonables, proporcionales y potencialmente efectivas para contribuir a la mitigación de conductas fraudulentas.

2.1. Estrategias de educación y concientización a usuarios

Se resalta la importancia de fortalecer las estrategias de educación digital dirigidas a los usuarios finales, especialmente aquellas orientadas a incrementar el conocimiento sobre las modalidades de fraude más frecuentes, los mecanismos de suplantación de identidad y las recomendaciones para la protección de la información personal y financiera.

El fraude cibernético es un fenómeno que, en gran medida, explota factores asociados al comportamiento humano y a la ingeniería social. Por esta razón, las acciones de prevención y concientización constituyen herramientas complementarias fundamentales dentro de cualquier estrategia integral de mitigación del fraude.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

En este sentido, es positiva la incorporación de medidas que promuevan campañas educativas, mecanismos de divulgación y acciones de sensibilización dirigidas a los usuarios.

2.2. Facultades para la suspensión preventiva de servicios asociados a posibles actividades fraudulentas

Es acertado que la propuesta fortalezca las herramientas disponibles para que los PRST puedan adoptar medidas oportunas frente a situaciones en las cuales existan indicios razonables de utilización indebida de los servicios o de desarrollo de actividades potencialmente fraudulentas.

La posibilidad de suspender temporalmente la prestación de servicios asociados a campañas o actividades respecto de las cuales existan elementos objetivos que permitan inferir riesgos para los usuarios constituye una medida que puede generar efectos inmediatos en la contención del fraude y en la reducción de su impacto.

Adicionalmente, esta herramienta permite una actuación rápida frente a situaciones de riesgo, evitando que la materialización de los daños continúe mientras se realizan las verificaciones correspondientes.

Esta medida, sumada con la suspensión provisional implementada por la CRC dentro del desarrollo de una actuación administrativa, y bajo una actuación expedita de la misma, logra mejores beneficios a favor de los usuarios.

2.3. Terminación de relaciones contractuales

Desde las diferentes intervenciones realizadas por COMCEL, siempre manifestó la necesidad de incorporar mecanismos que permitan la terminación de relaciones contractuales cuando se acrediten incumplimientos graves asociados a actividades fraudulentas o al uso indebido de los servicios.

La posibilidad de excluir del ecosistema a actores que reiteradamente incumplen las condiciones regulatorias o contractuales constituye un incentivo importante para el cumplimiento y contribuye a preservar la confianza en los servicios de mensajería empresarial.

Este tipo de medidas tienen la ventaja de actuar directamente sobre los agentes responsables de las conductas indebidas, sin imponer cargas indiscriminadas sobre la totalidad de los participantes del mercado.

2.4. Necesidad de privilegiar mecanismos focalizados sobre actores de riesgo

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Las medidas anteriormente descritas comparten una característica especialmente relevante: se encuentran dirigidas a atender situaciones concretas de riesgo o incumplimiento y recaen principalmente sobre los agentes respecto de los cuales existen indicios objetivos de conductas potencialmente fraudulentas.

Por esta razón, estas herramientas merecen una valoración prioritaria dentro del análisis regulatorio, particularmente cuando se comparan con otras alternativas de carácter estructural que implican cargas significativas para la totalidad de los actores del ecosistema sin que se haya demostrado plenamente su efectividad.

En consecuencia, el fortalecimiento de mecanismos de educación, prevención, suspensión temporal y terminación de relaciones contractuales constituye una aproximación regulatoria que resulta consistente con los principios de necesidad, proporcionalidad y eficiencia que deben orientar la intervención regulatoria.

3. COMENTARIOS PUNTUALES SOBRE LA PROPUESTA DE CREACIÓN DE UN VALIDADOR CENTRALIZADO:

La propuesta pretende crear una persona jurídica *"validador centralizado"* que tiene a su cargo la administración, gestión e integridad del proceso de validación de los agentes, marcas y plantillas de contenido que participan en el ecosistema de tráfico A2P. Sus funciones comprenden la verificación del proceso de KYC adelantado por los asignatarios del código corto A2P respecto de los potenciales asignatarios del SENDER ID, la aprobación de las plantillas de contenido A2P, y la emisión de las certificaciones requeridas en el proceso de asignación de los recursos de identificación código corto A2P y SENDER ID. La actuación del validador centralizado se enmarca en los lineamientos regulatorios que para el efecto expida la CRC y bajo la supervisión permanente del Administrador de los Recursos de Identificación.

- Al respecto, es pertinente aclarar que dicha propuesta actualmente es técnicamente incompatible con la arquitectura, la capacidad de procesamiento y los niveles de servicio actuales.

- La integración de sincronizar en tiempo real con el Validador Centralizado, tal como la exige la resolución, introduciría una **latencia adicional mínima de 200ms** por mensaje sobre una plataforma GW PCA que hoy opera con latencias de 50-150ms.

- A un throughput pico de 2.000-3.000 msg/seg, esto representa la generación de 2.000-3.000 llamadas API externas síncronas por segundo — volumen para el cual el GW PCA actual de COMCEL no fue diseñado ni tiene capacidad nativa.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- El cumplimiento literal de la norma, sin rediseño arquitectural profundo, degradaría el servicio de mensajería A2P hasta hacerlo inoperativo en horas pico.

- La latencia actual del GW PCA (50-150ms) es compatible con los SLA de entrega de mensajes **A2P transaccionales (OTP, alertas bancarias),** que típicamente exigen entrega en < 500ms.

- Con la integración síncrona al Validador, la latencia mínima sería de 290-495ms en condiciones normales — antes de llegar al SMSC, que añade su propio tiempo de procesamiento.

- En condiciones de alta demanda del Validador (500ms permitidos por la norma), la latencia total superaría los 610-890ms por mensaje, violando los SLA de mensajería transaccional.

- Los mensajes OTP bancarios y alertas de seguridad, que son los más críticos para el usuario final, serían los más afectados por esta degradación.

- La obligación de consultar al Validador Centralizado en cada mensaje A2P genera una demanda de llamadas API externas síncronas proporcional al throughput del GW PCA, para la cual ni el GW PCA ni el Validador están dimensionados. El GW PCA actual procesa 2.000-3.000 msg/seg en hora pico.

- Con la integración síncrona al Validador (latencia adicional mínima de 240ms en condiciones normales), el throughput efectivo se reduciría a aproximadamente 340-510 msg/seg. Esto representa una pérdida del 83% de la capacidad de procesamiento del GW PCA en hora pico.

- Los mensajes que no puedan ser procesados en tiempo real se acumularán en cola, generando timeouts SMPP, rechazos de mensajes, y degradación progresiva hasta el colapso total 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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- 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 definió mecanismos de caché local, TTL de validaciones, o validaciones optimizadas por SENDER ID + Template ID para reducir el número de consultas.

- El argumento de inviabilidad técnica no aplica solo al GW PCA: también aplica al Validador Centralizado, que deberá procesar la demanda de consultas de todos los PRST del país simultáneamente.

- 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.

- Un único Validador Centralizado debe atender 6.000 a 12.000 consultas API por segundo provenientes de todos los PRSTM.

- Si el Validador tiene cualquier degradación de rendimiento (respuestas superiores a 200ms), todos los GW PCA de los operadores se degradarán simultáneamente.

- Una falla del Validador (incluso dentro del SLA del 99.5% mensual que permite hasta 3.6 horas de caída al mes) impacta la mensajería A2P de todo el ecosistema.

- 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 anteriormente expuesto, se sugiere tener en consideración las siguientes adecuaciones técnicas:

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Transformación requerida	Descripción técnica	Plazo mínimo realista	Por qué no en 6 meses
Rediseño del núcleo de procesamiento del GW PCA: de modelo SMPP síncrono a modelo asíncrono no bloqueante (async/event-driven)	Refactorización del motor de mensajería para soportar llamadas I/O no bloqueantes. Implica cambio de paradigma de programación del sistema completo. En hardware físico dedicado, esto puede requerir reemplazo o actualización del sistema operativo y runtime.	**14 – 20 meses**	Rediseño de la arquitectura central del sistema. No es un módulo adicional, es el corazón del GW PCA.
Implementación de connection pooling y caché de validaciones con TTL	Pool de conexiones HTTP persistentes hacia el Validador para evitar overhead de TLS handshake por mensaje. Caché local en memoria con TTL corto (e.g., 60 segundos) para evitar N consultas redundantes del mismo SENDER ID + Template ID.	**5 – 6 meses**	Requiere que las especificaciones del Validador (API, TTL aceptado) estén definidas. Aún no lo están.
Módulo de sincronización offline y failover automático	Sistema de sincronización periódica de la lista completa de agentes, SENDER IDs y plantillas vigentes desde el Validador hacia el GW PCA, para operación offline durante contingencias. Activación automática y reconexión transparente.	**7 –9 meses**	Depende de la existencia y estabilidad del Validador para diseñar el protocolo de sincronización.
Actualización o reemplazo de hardware (scale-up/out)	El hardware dedicado actual no puede escalar horizontalmente. Para mantener el throughput de 2.000-3.000 msg/seg con la latencia adicional de la API, se requeriría multiplicar la capacidad de cómputo por un factor de ~6x.	**8 – 14 meses**	Adquisición, instalación, configuración y pruebas de hardware en datacenter. No es inmediato.
Pruebas de carga, integración y certificación	Pruebas de carga a throughput pico (3.000 msg/seg) con el Validador real. Pruebas de failover, contingencia y reconexión. Certificación de seguridad de la API. Pruebas en ambiente de staging antes de producción.	**5 – 7 meses**	Requiere que el Validador tenga ambiente de pruebas disponible. Hoy no existe.

En virtud de lo anterior, COMCEL presenta la siguiente propuesta, la cual 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 COMCEL A IMPLEMENTAR:

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. Se proponen 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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- 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.

A título de conclusión, se acepta la obligación de validar el SENDER ID, el código corto A2P y la plantilla de contenido antes de cursar tráfico A2P. Sin embargo, se solicita que la CRC reconozca la inviabilidad técnica de la consulta síncrona por mensaje individual y permita implementaciones alternativas equivalentes (por sesión + push de cambios, o caché con TTL regulado).

Se propone que los mensajes de autenticación y seguridad (OTP) sean excluidos de la validación síncrona por mensaje, dado su criticidad para el usuario final y el riesgo de afectación por latencia adicional.

4. SOBRE LA PROPUESTA REGULATORIA ESTABLECIDA EN LA RESOLUCIÓN *"POR MEDIO DE LA CUAL SE ESTABLECEN MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES Y SE DICTAN OTRAS DISPOSICIONES"*

4.1. Sobre la definición de CONOCIMIENTO DEL CLIENTE – KYC (KNOW YOUR CUSTOMER).

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. Se ha observado que estas empresas que están en estos estados envían tráfico presuntamente fraudulento.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Adicionalmente, se pone sobre la mesa un Onboarding más lento (KYC + validación + plantillas) y dependencia de un tercero (validador). La activación de un código o el proceso de venta se puede ralentizar por estas dependencias.

4.2. Sobre la definición de LISTA DNO (DO NOT ORIGINATE):

COMENTARIO COMCEL: Se respalda la estrategia integral propuesta por la CRC al abordar el fraude desde múltiples frentes (bloqueo, monitoreo, gobernanza y etiquetado). No obstante, 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, es necesario que se definan mecanismos de validación progresiva como attestation frameworks (equivalente a STIR/SHAKEN) antes de una prohibición absoluta.

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, se solicita a la CRC que incluya este aspecto en la definición de LISTA DNO (DO NOT ORIGINATE).

4.3. Sobre la definición de PLANTILLA DE CONTENIDO A2P (TEMPLATE ID):

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, 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

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

carga operativa que asumirían los PRST. Lo anterior, en atención a los principios de transparencia, participación y análisis de impacto normativo.

Finalmente, se 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, 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.

4.4. Sobre la definición de SENDER ID y los requisitos para su asignación:

COMENTARIO COMCEL: El SENDER ID tiene viabilidad Técnica limitada, toda vez que el estándar de señalización telefónica internacional (GSM/3GPP) soporta nativamente remitentes alfanuméricos de hasta 11 caracteres. (lo anterior incluido el SENDER ID + el CODIGO CORTO).

Además de la señalización celular (GSM/3GPP), el SENDER ID alfanumérico es soportado nativamente por el protocolo SMPP (Short Message Peer-to-Peer), que es el estándar industrial utilizado para conectar a los Integradores Tecnológicos (IT) con los centros de mensajería (SMSC) de los operadores (PRST).

Compatibilidad Universal de Terminales (Agnóstico al Dispositivo): A diferencia de otras tecnologías de seguridad digital, el SENDER ID alfanumérico no requiere que el usuario final tenga un teléfono inteligente (Smartphone) de última generación ni planes de datos móviles. Funciona e impacta visualmente con el nombre de la marca tanto en un teléfono básico (2G) como en terminales 4G/5G, garantizando una cobertura del 100% de la población de manera inmediata. Estos sistemas son los que soportan nativamente remitentes alfanuméricos de hasta 11 caracteres.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

El SENDER ID presenta una viabilidad técnica inmediata debido a que el estándar GSM/3GPP y el protocolo SMPP soportan nativamente remitentes alfanuméricos de hasta 11 caracteres en formato ASCII de manera universal en los terminales.

La resolución establece que el PCA debe solicitar a la CRC la asignación del SENDER ID a nombre del creador del contenido. Al respecto, se sugiere considerar que esta obligación recaiga directamente sobre el creador o responsable del contenido. Lo anterior, en la medida en que el SENDER ID constituye un identificador asociado a la identidad, actividad y responsabilidad del remitente final de las comunicaciones, quien es el sujeto que conoce, controla y responde por el contenido de los mensajes enviados.

Cuando la solicitud y administración del SENDER ID es realizada directamente por el creador o responsable del contenido, se fortalece la trazabilidad, se garantiza una correspondencia directa entre el identificador y el sujeto responsable de las comunicaciones, se facilita la supervisión por parte de las autoridades y se reduce el riesgo de suplantación o uso indebido de identificadores asociados a terceros.

Adicionalmente, este modelo promueve una distribución más eficiente de responsabilidades dentro del ecosistema de mensajería, en la medida en que cada agente asume las obligaciones relacionadas con la información y actividades que efectivamente controla.

Respecto a la limitante de "Un único SENDER ID por Empresa": Esto genera un error operativo grave para grandes corporaciones. Un banco grande (persona jurídica única) necesita múltiples Sender IDs para segmentar sus servicios por seguridad (ej. "BANCO_OTP" para contraseñas, "BANCO_AVISO" para alertas, y "BANCO_PROMO" para publicidad). Si se les limita a uno solo, el usuario no podrá priorizar los mensajes de seguridad sobre los comerciales, y las empresas no podrán gestionar sus marcas de forma independiente.

Adicionalmente, si no hay un filtro de validación cruzada inmediato, un ciberdelincuente con una empresa legalmente constituida podría solicitar a la CRC el SENDER ID "AMAZ0N" o "DIAN_COL" antes de que las entidades reales lo hagan. Se debe ligar la asignación del SENDER ID a la validación de marcas ante la SIC o al nombre comercial registrado en el RUES.

Finalmente, se deben excluir caracteres especiales y homoglifos: los defraudadores usan caracteres visualmente idénticos para engañar al usuario (ataques de homoglifos). Por ejemplo, reemplazar una letra "O" por el número cero "0", o usar caracteres del alfabeto cirílico. La norma debe exigir que el SENDER ID use exclusivamente caracteres alfanuméricos estándar en formato ASCII para evitar estas trampas visuales.

4.5. Sobre el VALIDADOR CENTRALIZADO:

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Adicional a lo señalado en el capítulo en el cual se presenta la propuesta de COMCEL para poder implementar el validador centralizado, se incluyen las siguientes observaciones:

Validador como "Punto Único de Falla" (Single Point of Failure - SPoF): En la arquitectura tecnológica actual, si el nodo SMS de un operador falla, el tráfico se puede desviar por otro. Con un Validador Centralizado, toda la mensajería del país depende de un solo actor. El Riesgo: Un apagón tecnológico, un error de software en la plataforma del Validador o una falla en su proveedor de nube dejaría a toda Colombia sin capacidad de recibir OTPs bancarias, alertas de pánico, coordenadas de georreferenciación de vehículos de transporte de valores o confirmaciones de alarmas residenciales. Impacto: Parálisis financiera y vulnerabilidad crítica en la seguridad física de los ciudadanos y empresas.

El "Efecto Atractivo" para Ciberataques (Honeypot): El Validador Centralizado concentrará el inventario completo de marcas, códigos cortos, plantillas y metadatos de las transacciones de todo el país. El Riesgo: Se convierte en el objetivo número uno de los grupos de ransomware y actores estado a nivel mundial. Un hackeo exitoso a esta entidad podría permitir a los criminales modificar plantillas de seguridad para inyectar smishing masivo directamente desde los servidores aprobados del banco, evadiendo todos los firewalls 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, el validador tiene la función de desactivar la plantilla si detecta mal uso de la misma. Esta función debe ser complementada indicando que informa inmediatamente al PRSTM para que suspenda el envío de estos SMS.

4.6. Sobre la definición de CODIGO CORTO A2P:

Falta de Exclusividad para Sectores de Alto Riesgo: El texto no discrimina sectores. La industria bancaria, el gobierno y los servicios de salud (tráfico crítico) deberían exigir códigos cortos A2P exclusivos y dedicados, prohibiendo normativamente que sus mensajes compartan el mismo canal (código corto) con tráfico de marketing o entretenimiento.

4.7. Sobre la definición de INTEGRADOR TECNOLÓGICO:

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

En el mercado de telecomunicaciones internacional es muy común que un Integrador Tecnológico colombiano le revenda capacidad a un integrador extranjero, y este a su vez a otro. Si el IT asignatario del código corto A2P en Colombia le permite a sub-agregadores usar su conexión sin que el Validador Centralizado les haga KYC individual, se rompe por completo la trazabilidad del fraude. La norma debe prohibir expresamente la sub-agregación ciega o exigir que el IT responda solidariamente por cualquier tercero intermedio.

Adicionalmente, el artículo presenta una inconsistencia al establecer: *"(...) soporte técnico entre los PRST y los PCA (...) sin conexión directa con los PRST, a través de una relación contractual de acceso directo con al menos un PRST."*

Técnicamente, un Integrador Tecnológico SÍ tiene conexión directa con las redes de los operadores móviles (PRSTM) para poder inyectar el tráfico. Si se deja el texto diciendo que "no tiene conexión directa", se confunde la figura del IT con la de un "Sub-agregador" o revendedor informal (que son los que suelen originar el tráfico de smishing internacional sin control contractual). El texto debe ser modificado aclarando que el IT es el que conecta de forma directa al PRSTM con los PCA, quienes estos últimos sí carecen de enlace directo con el operador.

4.8. Sobre la definición de PROVEEDOR DE CONTENIDOS Y APLICACIONES (PCA):

El artículo propuesto señala que el PCA es el responsable directo de los contenidos y aplicaciones. Sin embargo, no menciona explícitamente que la condición de PCA está sujeta a la aprobación previa del procedimiento obligatorio de KYC ante el Validador Centralizado. Si un ciberdelincuente crea una aplicación móvil maliciosa y se autodenomina "PCA", la definición genérica podría ampararlo para reclamar un SENDER ID. Se debe condicionar la calidad de PCA a la validación formal de su identidad jurídica.

El peligro del tráfico transfronterizo o "Offshore PCA": Muchas aplicaciones globales de origen extranjero (redes sociales, plataformas de streaming, billeteras digitales globales) actúan como PCA pero no tienen presencia legal o física en Colombia. El artículo deja en el aire cómo se regulará a estos actores internacionales para obtener el SENDER ID. Si no se les exige un representante legal local o un mecanismo de homologación internacional estricto para el KYC, los estafadores transfronterizos se harán pasar por PCA internacionales legítimos utilizando plataformas extranjeras para inyectar smishing hacia Colombia.

4.9. Sobre las obligaciones generales y particulares relacionadas con la prevención de fraudes:

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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

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.

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”, se 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.

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.

Este proceso garantiza la protección del usuario y está alineado con el objetivo del proyecto regulatorio.

4.10. Sobre el plazo para la implementación de sistemas de monitoreo establecido en el artículo 2.1.10.7.2.1.5.

El artículo 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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- 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.

Respecto del plazo de tres (3) meses previstos en el artículo 2.1.10.7.2.1.5 para la implementación de sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P), consideramos que dicho término 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. 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.

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 no incorpora evidencia que demuestre que un plazo de tres meses sea técnica y operativamente suficiente para implementar las capacidades exigidas por todos los PRSTM, 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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

En consecuencia, se 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.

4.11. Sobre el reporte a entregar para SMS en el cual se debe incluir 1) 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 2) 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.

COMCEL solicita se eliminen estos aspectos a reportar por ser técnicamente es inviable. Las redes móviles tranzan millones de eventos de SMS al día. Un Firewall de SMS o un sistema FMS (Fraud Management System) funciona mediante reglas de descarte perimetral inmediato. Si el sistema tuviera que guardar en una base de datos (logs) cada evento analizado que NO coincidió exactamente con el patrón de fraude, el volumen de datos e indexación crecería de forma exponencial (varios Terabytes por día). Esto saturaría los repositorios, elevaría los costos de almacenamiento en la nube (OpEx) y degradaría el rendimiento del procesamiento de la red.

Frente a la identificación de los "factores de contexto que motivaron esa determinación". Si un proceso es automatizado, la única "motivación" es que el algoritmo no sumó el puntaje (score) suficiente para activar la alerta. Pedir factores de contexto contextuales o cualitativos de millones de descartes por segundo es un requerimiento imposible de automatizar.

4.12. **Sobre el reporte a entregar sobre SMS A2P en el cual se debe incluir 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.**

Se propone ELIMINAR este requisito. Esta exigencia representa un riesgo crítico para la seguridad del ecosistema de telecomunicaciones y viola el principio de confidencialidad comercial.

En el ámbito de la ciberseguridad, esta información se clasifica como Secreto Industrial, y su divulgación, pone en peligro la efectividad de los sistemas y la seguridad nacional.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Amparo Legal Nacional e Internacional del Secreto Industrial: Los criterios, fórmulas lógicas y umbrales de configuración desarrollados por los equipos de ingeniería de un PRST (o adquiridos bajo costosas licencias a proveedores globales de ciberseguridad) constituyen un Secreto Empresarial protegido por la Decisión 486 de la Comunidad Andina de Naciones (Régimen Común sobre Propiedad Industrial). Dicha normativa prohíbe la divulgación de información no divulgada que tenga valor comercial y esté sujeta a medidas razonables de protección.

Asimetría Competitiva: Las herramientas de detección de fraude son un factor de diferenciación competitiva entre operadores. Un PRST que invierte millones de dólares en algoritmos avanzados de Inteligencia Artificial para proteger a sus usuarios no puede ser obligado a plasmar sus metodologías en un documento regulatorio que, por dinámicas del derecho administrativo, podría terminar expuesto a la competencia.

4.13. Sobre la obligación de los PRST de bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano, salvo cuando se trate de tráfico de roaming internacional debidamente identificado como tal por el carrier de origen. Los carriers internacionales interconectados con operadores colombianos para la terminación de tráfico en la red móvil nacional deberán cumplir con los formatos y longitudes de numeración establecidos en la Recomendación UIT-T E.164, respetando el código de país correspondiente al origen real de la llamada.

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, 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

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

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".

4.14. Sobre 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.

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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- 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.

4.15. Frente a la obligación de los PRSTM de etiquetar llamadas con fines publicitarios:

Los PRSTM deberán implementar un registro en el que sus clientes corporativos inscriban previamente los números, rangos de numeración o identificadores de llamada que utilizarán para realizar llamadas con fines publicitarios. Con base en este registro, los PRSTM administrarán una lista dinámica de números publicitarios y deberán etiquetar las llamadas originadas desde dichos números con la leyenda “Llamada con fines publicitarios”, visible para el usuario receptor. Asimismo, los PRSTM deberán mantener actualizado este registro y podrán modificarlo a solicitud de sus clientes o por decisión propia. Finalmente, cuando identifiquen que un cliente corporativo está realizando llamadas publicitarias a usuarios inscritos en el Registro de Números Excluidos (RNE), deberán bloquear dichas llamadas en lugar de etiquetarlas.

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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- 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.

4.16. 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:

Esta obligación 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.

4.17. Sobre el procedimiento de revisión del etiquetado de llamada sospechosa:

Por los argumentos indicados en los numerales anteriores, no es viable el etiquetado, motivo por el cual, tampoco es viable el procedimiento.

4.18. Sobre la obligatoriedad de los PRSTM de implementar una lista de no originación (LDN)

Se considera inviable que cada PRSTM tenga su propia lista de no originación.

A título de ejemplo, 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.**

4.19. 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 (LDN)

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

De acuerdo con que la lista en el SIGRI sea administrada por la CRC. No obstante, 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. 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.

4.20. Sobre la creación del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles.

Sobre las funciones del Comité: El artículo 2.1.10.7.3 crea el Comité Técnico de Lucha contra el Fraude y establece el carácter obligatorio de las decisiones que allí se adopten. No obstante, la propuesta regulatoria no define aspectos esenciales relacionados con su funcionamiento, administración, alcance de competencias, mecanismos de adopción de decisiones ni procedimientos aplicables.

Esta ausencia genera incertidumbre jurídica y operativa para los agentes obligados a cumplir las decisiones del Comité, en la medida en que no resulta posible determinar con claridad el alcance de sus facultades, los asuntos sobre los cuales podrá pronunciarse, los requisitos para la adopción de decisiones, los mecanismos de participación de los integrantes ni los procedimientos para documentar y comunicar sus determinaciones.

Adicionalmente, la propuesta podría generar una delegación excesivamente amplia de aspectos regulatorios hacia el Comité, permitiendo que se establezcan obligaciones, procedimientos o criterios técnicos sin que estos hayan sido objeto de los análisis de impacto, publicidad y participación propios del proceso regulatorio adelantado por la CRC.

Por lo anterior, se considera necesario que la CRC incorpore directamente en la regulación las reglas de funcionamiento y administración del Comité Técnico de Lucha contra el Fraude, definiendo de manera expresa sus competencias, procedimientos, límites de actuación y mecanismos de adopción de decisiones. Alternativamente, cualquier decisión del Comité que implique la creación de obligaciones, cargas operativas o requerimientos técnicos para los agentes del sector debería ser sometida previamente a los procesos de consulta y participación correspondientes, garantizando los principios de transparencia, seguridad jurídica y debido proceso regulatorio.

Así las cosas, si las decisiones del comité son obligatorias, el comité no puede convertirse en un mecanismo de regulación paralela. Es decir, la CRC no debería permitir que obligaciones, plazos, especificaciones técnicas o criterios de cumplimiento sean definidos posteriormente por un órgano técnico sin surtir el procedimiento regulatorio de publicidad, participación y análisis de impacto previsto

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

para la expedición de normas regulatorias. Este argumento suele tener bastante peso frente a la CRC porque se relaciona directamente con los principios de transparencia y legalidad regulatoria.

Frente a la Vinculatoriedad: El comité obliga a la asistencia de los PRST y de los asignatarios de códigos cortos (los IT), pero omite incluir como miembro obligatorio a la persona jurídica que operará el Validador Centralizado de SMS. Dado que este validador custodia la base de datos de marcas, contratos KYC y plantillas, es técnicamente absurdo dejarlo fuera del comité principal de fraude.

Cualquier cambio regulatorio u obligación técnica que genere costos o impactos técnicos debe pasar obligatoriamente por un proceso de consulta pública y un Análisis de Impacto Normativo (AIN), y no ser impuesto por la votación simple de un comité donde los operadores son minoría.

Frente al Quórum y votación: En Colombia existen pocos PRSTM pero existen decenas de asignatarios de códigos cortos (IT y agregadores pequeños). Bajo este esquema de mayoría simple, los integradores pequeños podrían unirse para votar y aprobar obligaciones técnicas u operativas que afecten directamente el núcleo de la red de los operadores, o bloquear medidas de seguridad estrictas que afecten sus volúmenes de tráfico comercial. Los PRSTM perderían el control técnico de sus propias redes.

En virtud de lo anterior, se 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"

4.21. Frente a la Oposición a la Interconexión:

Se solicita adicionar como complemento un numeral 4.1.2.6.6 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.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

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".

4.22. Sobre la asignación de SMS A2P y SENDER ID, cuando el A2P es internacional:

En cuanto a los A2P internacionales, 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 shortcode, este lo usa para el envío de todos los clientes que tenga. Si para internacionales 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. Se requiere que la CRC indique cómo se va a asignar 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 para nosotros no es posible.

La lista DNO también exigirá integración con sistemas de voz y numeración para bloquear CLI no válidos. Y se deberá tener en cuenta el desarrollo de procesos internos, ajustes de sistemas, validaciones documentales, también pueden aumentar los tiempos de activación de servicios y los costos de cumplimiento asociados a revisiones KYC y trazabilidad. El nuevo modelo puede exigir ajustes contractuales y operativos con integradores y clientes que actualmente utilizan códigos cortos bajo esquemas comerciales existentes.

Implementar la prevención del fraude sobre las plataformas existentes, generará un sobrecosto e incremento de actividades al interior de la compañía por lo que es inminente que se revise el mercado de A2P, previo a cualquier modificación.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

4.23. Comentarios sobre la limitación a un único código corto y un único Sender ID por titular

El proyecto de resolución establece que cada titular únicamente podrá contar con un código corto y, de manera similar, limita a un único SENDER ID por asignatario. Consideramos que esta restricción resulta excesiva y no refleja la realidad operativa de los modelos de negocio que utilizan servicios de mensajería para interactuar con sus usuarios.

En la práctica, una misma empresa puede gestionar múltiples líneas de negocio, marcas, productos, servicios o procesos de comunicación diferenciados, cada uno de los cuales requiere mecanismos propios de identificación frente a los usuarios. De igual forma, muchas organizaciones utilizan identificadores distintos según la naturaleza de la comunicación, diferenciando, por ejemplo, mensajes transaccionales, códigos de autenticación, notificaciones operativas, campañas informativas, comunicaciones de servicio al cliente o actividades comerciales.

La limitación a un único código corto o un único Sender ID dificulta la adecuada identificación del origen de las comunicaciones por parte de los usuarios, reduciendo la trazabilidad y generando potenciales confusiones respecto de la entidad, área o servicio que origina el mensaje. Paradójicamente, esta restricción podría afectar uno de los objetivos perseguidos por el propio proyecto regulatorio, consistente en fortalecer la transparencia y la confianza de los usuarios frente a las comunicaciones electrónicas.

Asimismo, la medida desconoce que muchas compañías operan estructuras corporativas complejas, con diferentes unidades de negocio, filiales, marcas comerciales o plataformas tecnológicas que requieren identificadores independientes para garantizar una gestión eficiente de sus comunicaciones y una adecuada segmentación de riesgos.

Desde una perspectiva de prevención del fraude, la utilización de múltiples identificadores debidamente registrados y asociados a un mismo responsable no genera un riesgo adicional. Por el contrario, permite una mejor trazabilidad de las comunicaciones, facilita la identificación de su origen y contribuye a la gestión diferenciada de incidentes, reportes y controles de seguridad.

Adicionalmente, el proyecto regulatorio no presenta evidencia que demuestre que limitar a un único código corto o Sender ID por titular contribuya de manera efectiva a la mitigación del fraude, ni analiza los impactos operativos, comerciales y tecnológicos que esta restricción generaría para los agentes que actualmente utilizan múltiples identificadores de manera legítima.

Por lo anterior, se solicita eliminar la restricción propuesta y permitir que un mismo titular pueda contar con varios códigos cortos y Sender ID, siempre que estos se encuentren debidamente registrados, asociados a un responsable identificable y sujetos a las medidas de control y trazabilidad que establezca la regulación.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

A título de ejemplo, un banco, una aseguradora, una plataforma de comercio electrónico o una entidad gubernamental pueden requerir identificadores distintos para separar mensajes de autenticación (OTP), alertas de seguridad, notificaciones transaccionales y comunicaciones informativas. Obligar a concentrar todas las comunicaciones en un único identificador dificulta que el usuario reconozca el propósito del mensaje y puede incluso aumentar el riesgo de fraude por confusión del destinatario. Esto conecta directamente con los objetivos de seguridad del proyecto regulatorio.

Adicionalmente, la restricción propuesta desconoce la diversidad de roles que pueden desempeñar los agentes dentro del ecosistema de mensajería. En particular, las empresas de telecomunicaciones pueden actuar simultáneamente como Proveedores de Redes y Servicios de Telecomunicaciones (PRST), Proveedores de Contenidos y Aplicaciones (PCA) o Integradores Tecnológicos (IT), dependiendo del servicio específico que estén prestando y de la naturaleza de las comunicaciones que cursan.

En estos escenarios, una misma organización puede requerir identificadores diferenciados para las comunicaciones asociadas a sus propios servicios, así como para aquellas que gestiona en calidad de PCA o IT para terceros. La limitación a un único código corto o un único SENDER ID genera incertidumbre respecto de la posibilidad de utilizar identificadores propios para sus comunicaciones corporativas y, al mismo tiempo, administrar identificadores destinados a los servicios que presta a sus clientes.

La restricción también dificulta la adecuada separación entre comunicaciones de diferentes naturalezas, afectando la trazabilidad, la gestión operativa y la identificación clara de los responsables de cada mensaje. Por ejemplo, una empresa de telecomunicaciones podría requerir códigos cortos o Sender ID distintos para sus propias comunicaciones transaccionales, de autenticación o atención al cliente, y otros identificadores asociados a los servicios de mensajería que provee como PCA o IT a entidades financieras, comercios, plataformas digitales u otros clientes corporativos.

Por lo anterior, resulta necesario que la regulación reconozca expresamente estas situaciones y permita la asignación de múltiples códigos cortos y Sender ID cuando exista una justificación operativa, comercial o funcional, garantizando en todo caso la plena identificación del responsable de las comunicaciones y la trazabilidad de los mensajes cursados. De lo contrario, la medida podría limitar injustificadamente modelos de negocio legítimos y generar barreras para la prestación eficiente de servicios de mensajería y comunicaciones electrónicas.

En virtud de lo anterior, se solicita eliminar el artículo 6.4.2.2.2. que establece: "*6.4.2.2.2. Se verificará que el solicitante no tenga un código corto A2P previamente asignado en el SIGRI. Si existe uno previo asignado, se negará la asignación salvo solicitud simultánea de devolución del anterior*".

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

Adicionalmente, no se justifica la creación de un ente validador centralizado, si tan solo tiene que administrar un código corto, con un SENDER ID por empresa.

4.24. Sobre las obligaciones de debida diligencia de los asignatarios de códigos cortos, y el proceso de KYC establecido:

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.

4.25. Sobre las obligaciones especiales de los PRSTM:

No queda clara la necesidad del establecimiento de un validador centralizado, si el PRSTM debe cumplir las mismas obligaciones de validación de: código corto, Sender ID, plantilla, etc, y si la red del PRSTM se conecta a través de API al validador central.

El validador central no debe ser un simple administrador de información, debe ser también un validador de la misma, y debe advertir las anomalías que se presentan con los envíos de los SMS. Si el PRSTM va a seguir teniendo la responsabilidad de validar dicha información, no queda clara la necesidad de un validador centralizado, fortaleciendo aun mas la premisa de que la CRC sin la necesidad de conformar este validador es suficiente para administrar la información que se relaciona en el proceso.

Tampoco queda claro para que se debe realizar el reporte de los mensajes bloqueados por ausencia o invalidez de identificadores de plantilla, si el validador centralizado va a tener acceso a la red, a través de la API y puede obtener la información.

4.26. Sobre la creación del Comité de seguimiento y coordinación operativa.

Se considera innecesario, toda vez que la CRC tiene la obligación de hacer este seguimiento, sin que sea requisito la creación de este. No queda claro por que los asignatarios de códigos cortos deben ser miembros de este comité; deben ser invitados. De la misma manera, **no debe haber un sistema de votación para tomar decisiones, toda vez que no se puede establecer una nueva instancia regulatoria**.

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, lo establecido en el artículo 6.13.5.1.11 sobre Naturaleza y vinculatoriedad de las determinaciones del CTS, en donde se indica que “las determinaciones que establezcan parámetros técnicos de operación entre los participantes del ecosistema, tales como especificaciones de las API de integración, formatos de reporte de incidentes, protocolos de comunicación entre sistemas, umbrales de monitoreo de tráfico y procedimientos de gestión de contingencias***, SERÁN DE***

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

CUMPLIMIENTO OBLIGATORIO PARA LOS ASIGNATARIOS DE CÓDIGO CORTO A2P, LOS PRST Y EL VALIDADOR CENTRALIZADO EN LOS TÉRMINOS Y PLAZOS ESTABLECIDOS EN LA RESPECTIVA ACTA DE SESIÓN. Debe ser eliminado.

El regulador no puede imponer implementaciones técnicas, sin la realización de un análisis de impacto normativo.

4.27. Sobre la obligatoriedad de modificar los contratos con actores del sector financiero:

La resolución pone en cabeza de los PRSTM la obligación de modificar los contratos con entidades del sector financiero, obligándolos a inscribirse en el portal de la CRC que utilicen para hacer llamadas de voz.

Se considera improcedente que la regulación pretenda trasladar a los PRSTM la obligación de modificar sus contratos con entidades financieras para incorporar deberes derivados de la regulación, particularmente en cabeza de entidades del sector financiero.

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, no resulta razonable ni jurídicamente adecuado exigir a los PRSTM que gestionen modificaciones contractuales con terceros para asegurar el cumplimiento de obligaciones que no les corresponden.

Desde una perspectiva de eficiencia regulatoria, resulta más adecuado que cualquier obligación de inscripción o actualización de información ante la CRC sea exigida directamente a las entidades financieras responsables, evitando la creación de cargas administrativas innecesarias y la introducción de intermediarios regulatorios que no participan en la relación jurídica que da origen a la obligación. Lo contrario podría generar complejidades operativas, costos adicionales y riesgos de incumplimiento atribuibles a factores ajenos a los PRSTM, sin que ello contribuya efectivamente al logro de los objetivos perseguidos por la regulación.

4.28. Sobre los tiempos establecidos para seleccionar el Validador centralizado:

Dada la complejidad del tema, los tiempos establecidos son muy cortos y se requiere la participación de diferentes empresas que cumplan con los parámetros técnicos establecidos. En virtud de lo anterior, como mínimo los cambios deben ser:

- Los días no deben ser calendario, deben ser hábiles.
- El plazo para elaborar los documentos del proceso de selección deben ser mínimo 15 días hábiles.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- El proceso de selección del validador debe ser de un mes, prorrogable por otro mes, en caso de que ninguno de los oferentes cumpla los requisitos.

4.29. Sobre el periodo de transición establecido en el artículo 19.

No es claro el periodo de transición establecido, pues las obligaciones incluidas a lo largo de la resolución establecen que aplican desde la publicación en el Diario Oficial. Teniendo en cuenta lo anterior, nuevamente se insiste en que se expida un solo acto administrativo que comprenda los aspectos aquí comentados y los aspectos de remuneración de un SMS A2P.

De todas maneras, el plazo que se incorpora para la realización del periodo de transición (de 6 meses) es imposible de cumplir por los argumentos ampliamente expuestos a lo largo de este documento. Al respecto, teniendo en cuenta las adecuaciones que se deben realizar sobre la red, las mismas se podrían implementar en DIECIOCHO (18) MESES, desde la publicación en el Diario Oficial.

5. NECESIDAD DE FORTALECER LA ACTUALIZACIÓN DE LA INFORMACIÓN DE PORTABILIDAD NUMÉRICA PARA GARANTIZAR LA ENTREGA EFECTIVA DE MENSAJES ASOCIADOS A PROCESOS DE AUTENTICACIÓN Y SEGURIDAD

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.

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

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

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.

6. **CONCLUSIONES:**

- Falta de integralidad en el análisis regulatorio. La CRC propone nuevas obligaciones técnicas y operativas sin un análisis económico completo, especialmente sobre SMS A2P, lo cual impide evaluar la proporcionalidad, sostenibilidad e impacto competitivo de las medidas.

- Insuficiente evaluación de alternativas existentes. No se demuestra que el esquema propuesto (validador centralizado, Sender ID) sea superior a mecanismos actuales. Herramientas como la suspensión provisional de códigos cortos, el monitoreo y bloqueo de tráfico, y la coordinación entre operadores ya generan resultados y no han sido evaluadas ex post.

- No se acredita la necesidad de un validador centralizado. La CRC no justifica por qué sus propias capacidades (administración de numeración) no son suficientes. La creación del

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

tercero duplica funciones, introduce costos adicionales y genera riesgos de concentración y dependencia.

- Riesgo sistémico del modelo centralizado. El validador se convierte en un Single Point of Failure (SPOF) y en objetivo crítico de ciberataques. Una falla impactaría todo el ecosistema nacional de mensajería, incluyendo OTP y servicios críticos.

- Inviabilidad técnica de la validación síncrona por mensaje. La consulta en tiempo real por cada SMS reduce hasta el 83% la capacidad de red incrementa la latencia y rompe los SLA de servicios críticos. Esto puede llevar a la degradación o colapso del servicio en horas pico.

- Falta de evidencia de reducción real del fraude. La propuesta no demuestra disminución del fraude, sino solo una posible migración a canales OTT, aplicaciones y otros canales digitales. No se analiza el efecto de sustitución entre canales.

- Sobrecarga regulatoria sin claridad de costos. No se define el esquema de remuneración, la recuperación de inversiones ni la asignación de costos. Esto genera riesgos de desincentivo a la inversión, aumento de costos a usuarios y afectación a la competencia.

- Medidas positivas identificadas por COMCEL. Se destacan como adecuadas las estrategias de educación y concientización a usuarios, la suspensión preventiva de servicios y la terminación contractual a infractores.

- Problemas de diseño regulatorio y gobernanza. Se evidencia falta de análisis técnico de viabilidad, respuesta sustantiva a comentarios y definición clara de roles y responsabilidades. Existe el riesgo de crear regulación paralela vía comités técnicos y decisiones obligatorias sin Análisis de Impacto Normativo (AIN).

- Restricciones operativas inconvenientes. Limitar a un único Sender ID y un único código corto afecta la trazabilidad y la operación empresarial.

- Problemas de implementación y plazos. Los plazos establecidos (por ejemplo, 3 meses) son insuficientes técnicamente. Los requerimientos de reporte son técnicamente inviables y generan cargas excesivas por el manejo de datos masivos y la protección de secretos industriales.

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co

- Inconsistencias técnicas en medidas de voz y etiquetado. El etiquetado de llamadas y bloqueo de CLI no es viable en redes actuales (2G/3G) y depende de sistemas operativos, no del operador.

- Riesgos de seguridad y competencia. La divulgación de criterios antifraude compromete la seguridad y afecta el secreto industrial.

En virtud de lo anterior, solicitamos que con ocasión de los aspectos nuevos que se incluyeron, y los comentarios presentados por COMCEL, se responda de manera puntual a cada uno de los comentarios presentados por los diferentes actores, y se ajuste la propuesta de regulación a lo que es viable, teniendo en cuenta los tiempos de implementación.

Respetuosamente,

Firmado por:
Santiago Pardo Fajardo
C8E4C986876A45F...

Inicial
MTCG

SANTIAGO PARDO FAJARDO
DIRECTOR CORPORATIVO JURIDICO Y SOSTENIBILIDAD

Carrera 68 A No. 24 B – 10
Teléfonos: 57 - 1 – 7429797 – 7500 300
Bogotá, D.C., Colombia
www.claro.com.co