VPAC-100022-02-103 Bogotá D.C. 23 de junio de 2026

Doctor
FELIPE AUGUSTO DIAZ SUAZA
Director Ejecutivo
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
medidasantifraude@crcom.gov.co

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

Apreciado Director,
Reciba un cordial saludo por parte de **Partners Telecom Colombia S.A.S**. (En adelante "**PTC"**). Por medio de este escrito, PTC se permite presentar sus comentarios al proyecto de resolución "*Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones"* buscando aportar con nuestra experiencia y argumentos frente a las medidas que propone el regulador, buscando un loable e importante propósito de combatir el fraude.

I. COMENTARIOS GENERALES

El Proyecto de Resolución tiene como propósito principal fortalecer la prevención y mitigación del fraude cibernético, así como proteger a los usuarios frente a conductas como la suplantación de identidad, el phishing y el smishing. De igual manera, busca preservar y reforzar la confianza en el ecosistema digital, elemento esencial para el adecuado desarrollo de los servicios y transacciones realizadas a través de medios electrónicos.
En este contexto, resulta pertinente reconocer la importancia de dicha iniciativa y manifestar coincidencia con los objetivos que la inspiran. En particular, se destaca la necesidad de adoptar medidas regulatorias eficaces, proporcionales y técnicamente idóneas que permitan salvaguardar la seguridad, la integridad de las comunicaciones y el bienestar de los usuarios, frente a un entorno digital cada vez más complejo y expuesto a riesgos emergentes.
No obstante, se considera necesario advertir que algunas de las disposiciones contempladas en el Proyecto de Resolución podrían generar efectos contrarios a los fines que se pretende alcanzar. En particular, existe el riesgo de que determinadas medidas, en su implementación práctica, resulten desproporcionadas o generen cargas operativas que afecten el normal funcionamiento de los servicios, sin necesariamente traducirse en una reducción efectiva de las conductas fraudulentas.
En consecuencia, se estima oportuno que el Proyecto sea objeto de un análisis adicional, orientado a garantizar que las medidas propuestas no solo sean coherentes con el propósito de protección al usuario, sino también efectivas, razonables y alineadas con las dinámicas reales del ecosistema digital.

1.1. Sobre la simplificación regulatoria y la eliminación de cargas regulatorias innecesarias.

El artículo 19 de la Ley 1341 de 2009, modificado por el artículo 15 de la Ley 1978 de 2019, dispone que la regulación que adopte la CRC debe promover, entre otros principios, la simplificación regulatoria, en igual jerarquía que la promoción de la inversión y la protección de los usuarios. PTC comparte el propósito antifraude del Proyecto, pero advierte que, en su diseño actual, algunos puntos de la propuesta aplicable al ecosistema A2P y de voz móvil, suponen costos adicionales y excesivos para los PRST cuando no son los responsables de la generación del tráfico, nos referimos puntualmente a la creación del validador centralizado.

En igual sentido, si bien estamos de acuerdo con la generación de un nuevo recurso de identificación (SENDER ID), y dos instancias de coordinación con objeto parcialmente coincidente (CTLFSM y CTS), consideramos que dichas medidas no deben suponer un esquema que supone contratación de terceros, sino la asunción de dichas competencias y funciones por parte de la CRC.

1.2. Sobre la ausencia de un análisis de costo-beneficio respecto de las medidas más gravosas del Proyecto.

El propio documento soporte del Proyecto señala que la CRC aplicó las metodologías de Multicriterio, Costo-Beneficio, Costos Administrativos y Enfoque de Simplificación Normativa para evaluar las alternativas regulatorias, pero dicha aplicación se circunscribió a temáticas puntuales: la falta de identificación del remitente en SMS A2P y la falta de control en SMS P2P (Multicriterio); la comparación frente a la adopción de STIR/SHAKEN/RCD para el eje de voz (Costos Administrativos); y la revisión del Título VI bajo un enfoque de simplificación.

No se evidencia, en cambio, que se haya aplicado una metodología de costo-beneficio cuantificada, ni siquiera de manera aproximada, a las medidas individualmente más onerosas del Proyecto: la creación del recurso de identificación SENDER ID, la creación del Validador Centralizado y su esquema de financiamiento a cargo de los asignatarios de código corto A2P, y el régimen de debida diligencia KYC que se impone como obligación continua durante toda la relación contractual.
Esta omisión resulta particularmente relevante a la luz de los artículos 2.2.13.3.2. y 2.2.13.3.3. del Decreto 1078 de 2015, que exigen a la CRC sustentar la proporcionalidad y la eficiencia de las medidas regulatorias mediante un Análisis de Impacto Normativo (AIN) que vaya más allá de la descripción cualitativa de las alternativas evaluadas. Por ello, PTC solicita respetuosamente a la CRC que, antes de la expedición de la resolución definitiva, realice un análisis de costo-beneficio específico para la creación del SENDER ID, del Validador Centralizado y del régimen de KYC, que incluya, como mínimo, una estimación de la inversión

esperada, del impacto esperado en la reducción del fraude y de los agentes llamados a asumir cada costo.

1.3. Sobre la naturaleza regulada de los negocios mayoristas (DID y A2P) y su perspectiva de crecimiento de cara a la sostenibilidad del negocio regulado.

Los negocios mayoristas asociados al DID y al tráfico A2P no pueden ser entendidos como actividades puramente comerciales o de libre configuración entre las partes, en la medida en que su prestación se soporta en recursos de identificación, relaciones de acceso, capacidades de red, condiciones de interconexión y esquemas de remuneración previamente definidos por la regulación. En ese sentido, aunque las partes puedan pactar determinadas condiciones operativas o comerciales, el margen de gestión del PRST se encuentra condicionado por obligaciones regulatorias que limitan su capacidad de trasladar costos, diferenciar condiciones o ajustar unilateralmente la remuneración del servicio.

En el caso específico del tráfico A2P, esta naturaleza regulada resulta expresa, artículo 4.2.7.1 de la Resolución CRC 5050 de 2016, establece que todos los proveedores de redes y servicios de telecomunicaciones móviles deben ofrecer a los integradores tecnológicos y proveedores de contenidos y aplicaciones, para remunerar la utilización de su red en relación con la provisión de mensajes cortos de texto SMS de Aplicación a Persona –A2P–, tanto en sentido entrante como saliente del tráfico, un cargo de acceso máximo equivalente a $1,00 por SMS, expresado en pesos constantes de enero de 2022, actualizado conforme al Anexo 4.2 del Título de Anexos.

Lo anterior confirma que el negocio A2P se desarrolla dentro de un marco de remuneración regulada, en el cual el PRST no cuenta con plena libertad para definir el precio del uso de su red, aun cuando sobre dicha red recaen obligaciones técnicas, operativas, de seguridad, calidad, disponibilidad y gestión del tráfico. Por ello, cualquier análisis sobre la sostenibilidad de este negocio debe partir de una premisa básica: el crecimiento del tráfico A2P no necesariamente se traduce en una mayor rentabilidad proporcional para el operador de red, en tanto la remuneración por el uso de la infraestructura se encuentra sometida a un tope regulatorio que sí favorece a los PCA e IT.

Esta consideración adquiere especial relevancia frente a la evolución esperada del mercado. El tráfico A2P es cada vez más importante para sectores como banca, comercio electrónico, servicios digitales, autenticación, logística, salud, educación y relacionamiento con usuarios. Sin embargo, dicho crecimiento también implica mayores exigencias sobre las redes móviles, mayores riesgos de fraude, mayor necesidad de monitoreo y mayor exposición reputacional frente al usuario final. En consecuencia, el aumento en volumen no puede analizarse de manera aislada, sino en conjunto con las cargas asociadas a los PRST de garantizar trazabilidad, seguridad, disponibilidad y cumplimiento regulatorio. Cargas que se deben compartir con los demás actores del ecosistema A2P.

Desde esta perspectiva, la sostenibilidad del negocio regulado exige que las nuevas medidas reconozcan el equilibrio económico de la relación mayorista. Si el precio está regulado y el margen del PRST se encuentra limitado por un cargo máximo, las cargas adicionales que se impongan sobre la red deben ser proporcionales, técnicamente viables y económicamente razonables. De lo contrario, se corre el riesgo de trasladar al PRST responsabilidades crecientes sobre un negocio cuya remuneración no refleja necesariamente la totalidad de los costos operativos, tecnológicos, administrativos y de prevención del fraude que demanda su prestación.
En consecuencia, PTC considera que el fortalecimiento del ecosistema A2P debe acompañarse de un análisis integral de sostenibilidad. La regulación puede promover mayor trazabilidad, control y seguridad en el tráfico, pero no debería desconocer que el PRST actúa dentro de un negocio mayorista regulado, con cargos máximos definidos por la CRC y con obligaciones que deben guardar correspondencia con la remuneración reconocida por el uso efectivo de la red.

1.4. Sobre la incorporación de medidas y cargas adicionales para los PRST.

Acorde con lo expuesto, la incorporación de nuevas medidas orientadas a prevenir el fraude en servicios móviles es necesaria y responde una problemática real del sector. No obstante, dichas medidas deben diseñarse bajo criterios de proporcionalidad, razonabilidad, neutralidad tecnológica y adecuada distribución de responsabilidades entre todos los agentes que intervienen en la cadena de valor. En particular, debe evitarse que el PRST termine asumiendo, de manera principal o residual, cargas que corresponden a otros actores del ecosistema, tales como integradores tecnológicos, proveedores de contenidos y aplicaciones, asignatarios de recursos de identificación, generadores de contenido o validadores centralizados.

En el caso del tráfico A2P, esta precisión resulta indispensable porque los PRST ya operan dentro de un esquema de acceso regulado. La Resolución 5050 de 2016 les impone obligaciones asociadas a permitir el acceso a sus redes, habilitar códigos cortos, aplicar reglas de remuneración, gestionar capacidades, garantizar niveles de calidad y abstenerse de imponer condiciones discriminatorias. A ello se suma que la remuneración por la utilización de la red para SMS A2P se encuentra limitada por un cargo máximo regulado. Por tanto, cualquier nueva obligación técnica, administrativa o de monitoreo debe evaluarse teniendo en cuenta que el operador no cuenta con libertad plena para recuperar, vía precio, los costos adicionales que se deriven de su implementación.

Bajo este contexto, medidas como la validación centralizada, el fortalecimiento de procesos KYC, la administración de plantillas de contenido, la trazabilidad del Sender ID, la gestión de listas DNO, el monitoreo de tráfico, el etiquetado de

llamadas, la participación en comités técnicos y la implementación de mecanismos adicionales de prevención generan impactos operativos concretos. Estas obligaciones requieren inversión en plataformas, procesos internos, personal especializado, ajustes de red, desarrollos tecnológicos, coordinación interinstitucional y gestión permanente de información. En consecuencia, no pueden ser tratadas como simples cargas de cumplimiento sin impacto económico.

PTC considera que la regulación debe evitar una asimetría en la asignación de cargas. El fraude en SMS y voz no se origina en la red móvil, sino que tiene su origen en los PCA e involucra a múltiples agentes que participan en la generación, agregación, validación, originación, transporte y entrega del tráfico. Por ello, las obligaciones deben ubicarse en cabeza del agente que tenga control efectivo sobre el riesgo que se pretende mitigar. Así, por ejemplo, la verificación del cliente, la legitimidad de la campaña, la consistencia del contenido y el uso adecuado de plantillas deben recaer principalmente sobre quienes originan, agregan o intermedian el tráfico A2P, sin trasladar a los PRST una función de auditoría integral sobre contenidos, campañas o relaciones comerciales respecto de las cuales no tiene control directo ni acceso efectivo a la información necesaria para su verificación. Lo anterior resulta especialmente relevante considerando que, en múltiples casos, las relaciones entre los PCA y los demás agentes que participan en el ecosistema A2P se encuentran sujetas a acuerdos de confidencialidad que limitan el acceso de los PRSTM a información sobre el originador real del tráfico, lo que dificulta o incluso imposibilita el cumplimiento de obligaciones de verificación exhaustiva sobre dichos contenidos o actores.

En esa misma línea, cualquier carga adicional impuesta a los PRST debe estar acompañada de reglas claras sobre alcance, responsabilidad, costos, tiempos de implementación y efectos frente a terceros. De lo contrario, se podría generar un incentivo contrario al objetivo regulatorio: aumentar las obligaciones sobre los operadores que soportan la infraestructura, mientras que los agentes que tienen mayor cercanía con el origen del tráfico no tienen o tienen menores cargas y consecuencias frente al uso indebido de los recursos de identificación.

Por lo anterior, PTC considera que las medidas propuestas deben preservar el equilibrio entre prevención del fraude y sostenibilidad del negocio regulado. La lucha contra el fraude exige trazabilidad y corresponsabilidad, pero no puede traducirse en la imposición de cargas ilimitadas a los PRST dentro de un mercado en el que la remuneración por el uso de red, particularmente para SMS A2P, está sometida a un cargo máximo regulado de $1,00 por SMS conforme al artículo 4.2.7.1 de la Resolución CRC 5050 de 2016. En consecuencia, toda nueva obligación debe ser técnicamente viable, económicamente eficiente y asignada al agente que se encuentre en mejor posición para prevenir, controlar o corregir el riesgo correspondiente.

Esta preocupación adquiere especial relevancia frente a la decisión que la propia CRC adoptó mediante la Resolución CRC 8183 de 2026, en la que se mantuvo el cargo de acceso de $1,00 por SMS A2P (en pesos constantes de 2022) precisamente en espera de la revisión integral que se adelantaría en el marco del presente proyecto regulatorio sobre mitigación del fraude cibernético. En otras palabras, la CRC condicionó la actualización del cargo de acceso a los resultados de este mismo Proyecto, el cual, sin embargo, en su Fase I, se limita a imponer un extenso conjunto de obligaciones técnicas y operativas nuevas (monitoreo de tráfico, integración con el Validador Centralizado, KYC, gestión de plantillas, validación anual del SENDER ID, participación en el CTLFSM y en el CTS) sin que su costo haya sido incorporado a la base de costos que sustenta dicho cargo, el cual solo será revisado en la Fase II. El resultado práctico es que los PRST deben financiar, desde la entrada en vigor de esta resolución, inversiones que las propias medidas regulatorias les imponen, sin que exista certeza de que la remuneración regulada las reconozca ni de cuándo ocurrirá dicho reconocimiento.

Por lo expuesto, PTC solicita a la CRC que, en el texto definitivo de la resolución, se incluya una manifestación expresa en el sentido de que los costos generados por las obligaciones adoptadas en esta Fase I, incluyendo la tarifa que los asignatarios de código corto A2P deberán pagar al Validador Centralizado conforme al artículo 6.13.1.2. del Proyecto, en la medida en que dicha tarifa pueda trasladarse a los PRST que actúen como integradores tecnológicos, serán considerados de manera expresa dentro de la base de costos que se evalúe en la Fase II de revisión de la remuneración del ecosistema A2P.

De manera subsidiaria, y mientras se define dicha actualización, se solicita a la CRC valorar la procedencia de un mecanismo transitorio de reconocimiento de costos para los PRST, en línea con el principio de causalidad de costos que debe orientar la regulación de cargos mayoristas.

A su vez, y como se desarrollará más adelante, resulta pertinente reafirmar que los Proveedores de Contenidos y Aplicaciones (PCA) y los Integradores Tecnológicos (IT) que ostentan la calidad de asignatarios de numeración en Colombia sí se encuentran sometidos al cumplimiento de obligaciones legales y regulatorias derivadas de la asignación y uso de códigos cortos y de la gestión de tráfico A2P. En efecto, la Resolución CRC 5050 de 2016 establece expresamente una serie de obligaciones y condiciones asociadas al uso adecuado de los recursos de numeración, las cuales son exigibles a todos los asignatarios. En consecuencia, no resulta jurídicamente procedente que dichos agentes pretendan sustraerse del cumplimiento de tales deberes bajo el argumento de que no son sujetos regulados de manera integral por la CRC, pues las obligaciones derivan precisamente de su condición de asignatarios de recursos escasos y limitados administrados por el Estado a través de la CRC.

De esta manera, los PCA e IT que reciben asignaciones de códigos cortos asumen responsabilidades propias respecto del uso adecuado de dichos recursos, así como frente a la prevención de prácticas fraudulentas, abusivas o contrarias a la regulación vigente. Por tanto, la asignación de numeración no puede entenderse únicamente como una habilitación para el uso del recurso, sino también como una fuente de obligaciones regulatorias cuyo incumplimiento puede generar consecuencias administrativas y regulatorias.

Bajo esta perspectiva, resulta razonable que estos agentes asuman responsabilidades directas, e incluso solidarias cuando corresponda de acuerdo con el marco normativo aplicable, respecto de las obligaciones asociadas al uso de la numeración y a la mitigación de riesgos de fraude y uso indebido de los servicios A2P, sin que dichas cargas recaigan exclusivamente sobre los PRST.

En esa misma línea, PTC considera pertinente recordar que los PRST ya se encuentran sometidos a un régimen integral de prevención del fraude conforme al artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, vigente desde antes de este Proyecto, el cual les exige implementar herramientas tecnológicas de prevención, investigar las PQR asociadas a presuntos fraudes y abstenerse de cobrar los consumos cuando el usuario haya actuado diligentemente. Sobre esa base regulatoria ya existente, el Proyecto adiciona un nuevo y extenso catálogo de obligaciones en cabeza de los PRST (monitoreo de patrones P2P, esquema de respuesta escalonado, bloqueo de CLI, listas DNO, etiquetado de llamadas, participación en el CTLFSM y en el CTS, integración técnica con el Validador Centralizado), mientras que las obligaciones equivalentes en cabeza de los PCA y de los Integradores Tecnológicos se concentran, en gran medida, en el proceso de KYC y en el uso correcto de las plantillas A2P.

Dado que el PRST carece de visibilidad sobre el contenido, la campaña, la relación comercial subyacente y el originador real del tráfico, elementos que sí conoce y controla directamente el PCA, y de manera derivada el IT, , PTC solicita respetuosamente a la CRC que, en el artículo 6.13.4.4. del Proyecto (atribución de responsabilidad por mal uso de plantillas), se incorpore una presunción expresa según la cual, salvo prueba en contrario, la responsabilidad primaria por el contenido fraudulento, engañoso o no autorizado de un mensaje A2P recae en el asignatario del SENDER ID, en su calidad de responsable directo de la producción del contenido, y de manera subsidiaria en el asignatario del código corto A2P cuando se acredite que este último facilitó o permitió el envío del tráfico irregular con conocimiento de dicha irregularidad.

Esta precisión es consistente con el régimen de causales de recuperación que el propio Proyecto ya diferencia entre el SENDER ID (artículo 6.12.3.2.) y el código corto A2P (artículo 6.4.3.2.), y evita que la indeterminación actual de la regla

derive, en la práctica, en el traslado de cargas de verificación hacia el PRST, quien no tiene ni el control ni el acceso a la información necesaria para asumirlas.

II. COMENTARIOS ESPECIFICOS III.

Sobre los cambios que el proyecto incorporaría en la Resolución CRC 5050 de 2016, PTC se permite formular los comentarios que se relacionan a continuación y que abordan de manera específica las normas citadas para comentarios:

3.1. Sobre las obligaciones contenidas en el Articulo 2.1.10.7.2.1. y las *Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.*

Respecto al Artículo 2.1.10.7.2.2.1. norma que establece que Los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número que haga parte del Plan Nacional de Numeración (PNN) colombiano; por lo tanto, PTC se permite manifestar que es importante que la CRC incorpore expresamente en la resolución, el formato y la numeración que debe bloquearse "+5760X", "5760X", "60X", "+573X", "573X", "3X" por las rutas LDI, razón por la cual, se sugiere la siguiente redacción:

> *2.1.10.7.2.2.1.* norma que establece que *Los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano,* y con numeración "+5760X", "5760X", "60X", "+573X", "573X", "3X" por las rutas destinada a Larga Distancia Internacional (LDI).

3.2. Respecto a las obligaciones contenidas en el Artículo 2.1.10.7.2.2.2.1. Etiquetado de llamadas con fines publicitarios, y el artículo 2.1.10.7.2.2.2.2. Procedimiento de revisión del etiquetado de llamada sospechosa.

Respecto a los ajustes propuestos en estos artículos, PTC se permite reiterar que estas obligaciones representan erogaciones económicas considerables para los PRST, quienes, en línea con lo expuesto con el apartado de comentarios generales del presente escrito, han visto como el modelo de negocio de LDI ha venido perdiendo participación en el mercado. En todo caso, vale la pena mencionar que la CRC debe establecer un plazo de al menos seis (6) meses para la implementación de dichas medidas, por cuanto su implementación no solo representa un esfuerzo económico, sino una coordinación interna administrativa de aprobación presupuestal y de desarrollo que puede involucrar a proveedores y terceros ajenos a PTC.

3.3. RESPECTO A LA *SECCIÓN 4. RÉGIMEN DE PLANTILLAS DE CONTENIDO A2P Y OBLIGACIONES DE LOS ACTORES.*

PTC se permite manifestar respetuosamente que, dado que los servicios A2P pueden incorporar información de naturaleza comercial, estratégica o incluso confidencial de los generadores de contenido, la obligación de registrar y reportar las plantillas de mensajería propuesta en el proyecto regulatorio podría generar riesgos asociados a la protección de información sensible y a la preservación de secretos empresariales, especialmente si no se establecen mecanismos regulatorios expresos que garanticen su adecuado tratamiento, custodia y confidencialidad.

En este sentido, resulta necesario que la CRC precise las condiciones bajo las cuales dicha información será administrada, así como las medidas destinadas a evitar accesos no autorizados, filtraciones o cualquier situación que pueda derivar en una afectación a la competencia o a los intereses comerciales legítimos de los agentes involucrados.

No obstante, PTC considera que el objetivo perseguido por la Comisión podría alcanzarse mediante mecanismos alternativos menos intrusivos. En particular, se estima que una certificación emitida por el Integrador Tecnológico respecto del cumplimiento de las condiciones regulatorias aplicables a las plantillas registradas permitiría gestionar adecuadamente los riesgos asociados al uso indebido de la mensajería A2P, sin requerir la revelación detallada del contenido de las comunicaciones.

Lo anterior resulta razonable en la medida en que los Integradores Tecnológicos, en su calidad de actores directamente involucrados en la cadena de valor del servicio, pueden asumir un deber de gestión y mitigación del riesgo de fraude, suplantación o uso indebido de la mensajería, quedando sujetos a las consecuencias regulatorias y sancionatorias previstas en la regulación en caso de incumplimiento. De esta forma, se logra un equilibrio entre los objetivos de supervisión y control perseguidos por la CRC y la protección de la información comercial sensible de los distintos agentes del ecosistema.

Aunado a lo anterior, solicitamos que la Comisión determine de manera clara y expresa la periodicidad con la que deberán actualizarse las plantillas registradas, con el fin de brindar certeza regulatoria a los agentes obligados y evitar interpretaciones divergentes respecto de esta obligación.

En particular, consideramos necesario que el plazo de actualización responda a criterios de razonabilidad y proporcionalidad, de forma tal que no genere cargas operativas excesivas derivadas de actualizaciones recurrentes e innecesarias, pero que tampoco permita que la información registrada permanezca

desactualizada por periodos prolongados que puedan afectar los objetivos de trazabilidad y control perseguidos por la medida regulatoria.

3.4. RESPECTO A LOS MENSAJES DE AUTENTICACIÓN Y SEGURIDAD

El artículo 6.12.1.3.1 establece que los mensajes de autenticación y seguridad, tales como códigos de un solo uso u OTP, 2AF, alertas de inicio de sesión, confirmaciones de operaciones, validaciones transaccionales y mecanismos similares, se generan a solicitud del usuario y, en consecuencia, no requieren consentimiento adicional. Esta disposición reconoce que dichos mensajes tienen una naturaleza funcional y de seguridad, distinta de la mensajería comercial, promocional o publicitaria, en la medida en que son necesarios para permitir el acceso seguro a servicios digitales, confirmar la identidad del usuario o proteger sus cuentas frente a accesos no autorizados.

No obstante, los artículos 6.13.4.1 y 6.13.4.7.2 disponen que todo mensaje A2P, incluidos los mensajes de autenticación, debe contar con una plantilla aprobada y vigente. Así mismo, prevén que, en ausencia de dicha aprobación, el PRST pueda bloquear el mensaje o marcarlo como "sin verificar". Esta exigencia implica que los mensajes de autenticación quedarían sujetos a un esquema de validación previa y control operativo similar al previsto para otros tipos de mensajería A2P, **sin diferenciar adecuadamente su finalidad, criticidad y sensibilidad temporal.**

En este contexto, se considera que el Proyecto presenta una contradicción interna, en la medida en que, por una parte, reconoce la naturaleza especial de los mensajes de autenticación y seguridad, pero, por otra, los somete al mismo régimen de control previo de contenido y a la misma posibilidad de bloqueo aplicable a la mensajería comercial o publicitaria. Esta equiparación resulta problemática, pues desconoce que los mensajes de autenticación son generados a partir de una acción activa, específica e inmediata del usuario, como iniciar sesión, recuperar una contraseña, confirmar una transacción, validar un dispositivo o autorizar una operación. Por tanto, no se trata de comunicaciones imprevistas, masivas o no deseadas, ni de mensajes que, por su sola naturaleza, puedan asimilarse a campañas comerciales o publicitarias.

Adicionalmente, los mensajes de autenticación cumplen una función esencial dentro de los ecosistemas digitales, financieros, comerciales, gubernamentales y de servicios en línea. Su finalidad no es promover productos o servicios, sino permitir que el usuario acceda de manera segura a plataformas, confirme su identidad o complete procesos que él mismo ha iniciado. En ese sentido, imponerles controles previos de contenido, vigencias periódicas y validaciones operativas en tiempo real puede afectar negativamente la continuidad de servicios que dependen de una entrega inmediata y confiable de estos mensajes.

Las características técnicas propias de este tipo de comunicaciones hacen que algunas de las medidas propuestas sean de difícil implementación práctica. En particular, los OTP y 2FA mensajes de autenticación incorporan variables dinámicas, códigos únicos, datos transaccionales, referencias temporales, nombres de servicios, montos, identificadores parciales o instrucciones específicas que cambian en función de cada operación. Además, son altamente sensibles al tiempo, pues su utilidad depende de que sean entregados dentro de ventanas muy cortas. Un retraso de pocos segundos puede hacer que el código pierda vigencia, que el usuario abandone la operación o que se genere una experiencia fallida de autenticación.

Si bien el Proyecto no necesariamente exige la aprobación de la configuración exacta de cada OTP, sí somete la plantilla, el contenido estático, la lógica o sentido del contenido dinámico y el enrutamiento del mensaje a un esquema de validación previa y consulta operativa. Esta aproximación puede generar incertidumbre sobre el alcance de la validación requerida, especialmente en escenarios en los que los mensajes deben adaptarse a múltiples casos de uso, distintos canales, idiomas, marcas, servicios, niveles de riesgo o necesidades de seguridad. En la práctica, ello puede traducirse en una carga operativa significativa para los originadores, integradores, agregadores y PRST involucrados en la cadena de envío.

Los servicios de autenticación normalmente operan bajo exigencias de continuidad cercanas al tiempo real, por lo que cualquier demora, indisponibilidad del sistema validador, inconsistencia en la información de la plantilla, falla de sincronización o error de clasificación puede impedir la entrega oportuna del mensaje.

En particular, se identifican los siguientes riesgos operativos asociados a la aplicación del esquema propuesto a mensajes de autenticación y seguridad:

1. **Riesgo de latencia en la entrega del mensaje:** La consulta previa al validador antes del enrutamiento puede aumentar el tiempo total de entrega. En mensajes comerciales, un retraso puede ser tolerable; en un OTP, un retraso puede impedir que el usuario complete la operación dentro del tiempo previsto.
2. **Riesgo de falsos bloqueos:** Diferencias menores entre la plantilla aprobada y el mensaje generado dinámicamente podrían dar lugar a bloqueos indebidos o a marcaciones como “sin verificar”, aun cuando se trate de comunicaciones legítimas solicitadas por el usuario.
3. **Riesgo de indisponibilidad por fallas del validador:** Si el sistema de validación presenta caídas, demoras, errores de procesamiento o indisponibilidad temporal, los mensajes de autenticación podrían no ser

cursados oportunamente, afectando servicios críticos que dependen de ellos.

4. **Riesgo de afectación a procesos esenciales del usuario:** La no entrega de un OTP puede impedir el inicio de sesión, la recuperación de cuentas, la confirmación de pagos, la activación de servicios, la validación de dispositivos o la autorización de operaciones sensibles.
5. **Riesgo de degradación de la experiencia del usuario:** Retrasos o fallas en la entrega pueden generar múltiples solicitudes de reenvío, abandono de transacciones, llamadas a canales de soporte, pérdida de confianza en el servicio y percepción de inseguridad o ineficiencia.
6. **Riesgo de congestión operativa:** En eventos de alto tráfico, por ejemplo, jornadas de pago, campañas masivas de acceso, cierres contables, eventos comerciales o incidentes de seguridad– la necesidad de validar grandes volúmenes de mensajes en tiempo real puede generar cuellos de botella.
7. **Riesgo de incremento de cargas administrativas y técnicas:** La gestión, actualización, renovación y control de plantillas para múltiples servicios, casos de uso, marcas, entidades o flujos de autenticación puede exigir desarrollos adicionales, recursos humanos especializados y ajustes continuos en los sistemas de mensajería.
8. **Riesgo de afectación a la seguridad del usuario:** Paradójicamente, si los mensajes de autenticación no se entregan oportunamente, los usuarios podrían recurrir a mecanismos menos seguros, reutilizar contraseñas, mantener sesiones abiertas o buscar canales alternativos que aumenten su exposición a riesgos de fraude.
9. **Riesgo de interrupción de servicios digitales críticos:** La autenticación vía OTP es utilizada en sectores como banca, comercio electrónico, salud, servicios públicos, gobierno digital, transporte, educación y plataformas empresariales. Una falla generalizada en la entrega de estos mensajes podría afectar no solo a un proveedor específico, sino a múltiples servicios esenciales para los usuarios.
10. **Riesgo de responsabilidad y conflictos entre actores de la cadena:** En caso de bloqueo o retraso, podría generarse incertidumbre sobre la responsabilidad entre originadores, agregadores, integradores, validadores y PRST, especialmente si el mensaje fue solicitado legítimamente por el usuario, pero no fue entregado por razones asociadas al sistema de control.

En ese sentido, el costo asociado a un falso bloqueo o retraso de un mensaje de autenticación es considerablemente superior al de un mensaje comercial no entregado. Mientras que la no entrega de un mensaje publicitario puede implicar la pérdida de una oportunidad comercial, la no entrega de un OTP puede impedir el acceso del usuario a su cuenta, bloquear una operación financiera, frustrar una recuperación de contraseña, afectar la continuidad de un servicio o incluso generar riesgos adicionales de seguridad y vulnerar derechos de los usuarios

Por lo anterior, la regulación debería reconocer una categoría diferenciada para los mensajes de autenticación y seguridad, estableciendo reglas proporcionales a su naturaleza funcional, transaccional y crítica. En particular, resultaría conveniente que estos mensajes no estén sujetos al mismo régimen de bloqueo previo aplicable a la mensajería comercial, o que, al menos, se prevean mecanismos especiales que garanticen su continuidad, tales como tratamientos prioritarios, reglas de excepción, validaciones ex post, esquemas de certificación de originadores confiables o controles orientados a patrones de abuso y no a la validación individual previa de cada mensaje.

En consecuencia, el efecto práctico de la propuesta, en los términos planteados, podría ser contrario al objetivo del propio Proyecto de Resolución. En lugar de fortalecer la seguridad y prevenir el fraude, la medida podría afectar el funcionamiento de una de las herramientas más eficaces para proteger a los usuarios frente a accesos indebidos, suplantaciones y operaciones no autorizadas. Por ello, se recomienda revisar el tratamiento regulatorio aplicable a los mensajes de autenticación y seguridad, de manera que se preserve su disponibilidad, oportunidad y confiabilidad, sin perjuicio de que se adopten medidas razonables y proporcionadas para prevenir su uso indebido.

3.5. SOBRE EL SENDER ID Y MARCO DE IMPLEMENTACIÓN

PTC considera indispensable esta medida, encontrando que la finalidad del SENDER ID es el recurso de identificación administrado por la CRC, que identifica de manera única e inequívoca a la persona natural o jurídica responsable directa por la producción y generación de contenidos o aplicaciones enviados a través de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD).

En este sentido, el usuario podrá identificar de manera clara e inmediata al originador del contenido, lo que le permitirá adoptar decisiones informadas respecto del tratamiento de sus datos personales y valorar con mayor certeza la legitimidad de las comunicaciones recibidas. Adicionalmente, la medida se encuentra alineada con tendencias regulatorias internacionales orientadas a fortalecer la transparencia y la trazabilidad de las comunicaciones electrónicas. Tal es el caso de España, donde la implementación del Registro de Alias ha mostrado resultados preliminares positivos en materia de identificación de remitentes, reducción de riesgos de fraude y fortalecimiento de la confianza de los usuarios en los servicios de mensajería[1].

[1] El Registro de alias, gestionado por la CNMC, recogerá todos los identificadores alfanuméricos (letras, números y letras combinados u otros caracteres) que pueden utilizarse como remitente en mensajes enviados a números españoles.

Ahora bien, este caso de referencia se pone en consideración de la CRC, ya que estipuló una serie de medidas técnicas previas a la generación obligatoria de bloqueo de mensajes y llamadas.

En este sentido, se reconoció por parte de la Comisión Nacional de los Mercados y la Competencia (CNMC) los retos técnicos que implicaban el desarrollo, la implementación y el funcionamiento escalonado de las medidas de bloqueo, disponiendo en el texto modificatorio a la orden TDF/149/2025, un periodo de aproximadamente un (1) año para el bloqueo de mensajes enviados con alias no registrados.

Es importante considerar un periodo de transición entre la adecuación técnica e implementación de las medidas sujetas a cumplimiento más amplio al previsto en el actual proyecto. Ello teniendo en cuenta que los artículos 2.1.10.7.2.1.5.[2] , 2.1.10.7.2.2.4.[3] estipularon que obligaciones como las de: implementar los

Permitirá identificar y gestionar los alias utilizados en servicios de mensajería, contribuyendo a reforzar la seguridad y a combatir el fraude mediante su bloqueo, cuando se detecte un uso indebido. A partir del 15 de septiembre de 2026, entrarán plenamente en vigor las obligaciones de bloqueo de mensajes enviados con alias no registrados o que, estando inscritos, no provengan de proveedores habilitados en el Registro de alias. Además, la CNMC habilitará en su página web un portal público que permitirá consultar qué alias están registrados y quién es su titular, lo que contribuirá a aumentar la transparencia y la confianza de los usuarios finales en las comunicaciones electrónicas.

[2] **2.1.10.7.2.1.5**. Los PRST deberán implementar los sistemas de monitoreo previstos en el presente artículo y acreditar su puesta en operación ante la CRC dentro de los tres (3) meses siguientes a la publicación en el Diario Oficial de la resolución que los adoptó. La acreditación se realizará mediante la presentación ante la CRC de un informe técnico que describa la arquitectura del sistema implementado, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas. Dentro de los seis (6) meses siguientes a la presentación de ese primer informe, los PRST remitirán un segundo informe a la CRC que contendrá lo siguiente: a. El número de eventos de detección de patrones de tráfico P2P atípico registrados en el período transcurrido desde la implementación de las medidas, discriminado por tipo de patrón detectado. b. El número de casos en que el sistema descartó el evento como falso positivo en la primera etapa del esquema de respuesta, con indicación de los factores de contexto que motivaron esa determinación. c. El número de casos en que el usuario manifestó una causa legítima en la segunda etapa y el PRST aceptó dicha justificación, con indicación agregada del tipo de causa alegada. d. El número de restricciones temporales del servicio de mensajería aplicadas en la cuarta etapa, discriminado por duración de la restricción. e. El número de casos reportados a la CRC en la quinta etapa y el número de terminaciones contractuales derivadas de la aplicación del presente artículo. f. Los umbrales y criterios aplicados por el PRST para la detección de cada uno de los patrones, con indicación de las actualizaciones realizadas a dichos criterios durante el período reportado. g. Las PQR recibidas en relación con la aplicación del presente artículo, con indicación de su resultado

[3] **2.1.10.7.2.2.4**. Plazo de implementación y reporte. Los PRST deberán implementar las medidas previstas en los numerales 2.1.10.7.2.2.1., 2.1.10.7.2.2.2. y 2.1.10.7.2.2.3 del presente artículo dentro de los tres (3) meses siguientes a la publicación en el Diario Oficial de la resolución que las adoptó, y acreditarán su puesta en operación ante la CRC mediante informe técnico que describa los sistemas implementados, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas, los cuales serán presentados a más tardar dentro del mes

sistemas de monitoreo previstos para SMS, así como acreditar su puesta en operación ante la CRC, bloqueo de llamadas internacionales entrantes con identificador de línea llamante (CLI), etiquetado de llamadas con fines publicitarios, implementación de sistemas de monitoreo en tiempo real del tráfico, Crear e implementar en las redes una lista de no originación (DNO) están sujetas a cumplimiento y validación **en tres (3) meses posteriores** a la publicación en el diario oficial de la resolución.

El término previsto resulta corto frente al cumulo de actividades que de ello se deriva. Teniendo en cuenta que las medidas no son menores y comprenden gestiones internas administrativas y de consecución y aprobación presupuestal y la posterior actuación incluso de terceras personas, lo cual, conlleva a que sea necesario reconsiderar un lapso tan corto al establecido en el proyecto, contrario a ello, la imposibilidad de generar los desarrollos de manera adecuada puede dar lugar a una posible implementación irregular y/o defectuosa.

Por lo anterior expuesto, solicitamos a la Comisión considerar que no todos los PRST presentan equivalencia en desarrollo tecnológico. Asimismo, debe valorarse que los desarrollos conllevan una inversión la cual, debe ser considerada conforme al tamaño de cada PRST, sumado a las cargas administrativas que de cada una de las obligaciones se derivan.

3.6. VALIDADOR CENTRALIZADO

En relación con los artículos 6.13.1.1 a 6.13.1.6 y 18 del Proyecto, mediante los cuales se establece la figura de un **validador centralizado**, entendido como una persona jurídica única, seleccionada por los PRST móviles y financiada por los asignatarios de códigos cortos A2P, a la cual se le atribuyen funciones tales como la verificación de requisitos de conocimiento del cliente (KYC), la aprobación de plantillas de mensajería y la emisión de certificaciones indispensables para el acceso a los recursos y el curso de tráfico, se formulan las siguientes consideraciones:

Resulta especialmente preocupante que el Proyecto concentre en un **actor privado** un conjunto de funciones que, en la práctica, **condicionan el acceso al mercado, la asignación de recursos escasos y el flujo de comunicaciones electrónicas**. Esta configuración regulatoria podría generar riesgos significativos desde la perspectiva de delegación de competencias, al conferir a dicho actor una posición determinante en la cadena de valor del servicio A2P.

---

siguiente al vencimiento del plazo otorgado para su implementación. Los PRST deberán reportar, previo requerimiento de la CRC, los eventos de detección, las medidas de etiquetado aplicadas, las revisiones solicitadas por usuarios y las actualizaciones realizadas a sus listas DNO, conforme al requerimiento que expida la Comisión.

Si bien el Proyecto contempla instancias de supervisión por parte de la CRC o del Administrador de Recursos de Identificación, se observa que **no se establecen salvaguardas suficientes** que garanticen:

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

Más allá de las consideraciones de política regulatoria expuestas, PTC considera necesario poner de presente que la creación del Validador Centralizado plantea un reparo de legalidad que antecede cualquier discusión sobre su diseño institucional.
La administración de los recursos de identificación, dentro de los cuales se incluyen el código corto A2P y el SENDER ID que el propio Proyecto crea, es una función pública atribuida de manera expresa y exclusiva a la CRC por el numeral 12 del artículo 22 de la Ley 1341 de 2009, modificado por el artículo 19 de la Ley 1978 de 2019.
Dicha atribución comprende no solo la asignación y recuperación de los recursos, sino también las actividades de verificación, validación y certificación que condicionan su otorgamiento, en la medida en que estas últimas constituyen presupuesto necesario e inescindible del ejercicio de dicha competencia legal.

Conforme al artículo 210 de la Constitución Política y a los artículos 110 a 114 de la Ley 489 de 1998, la atribución de funciones administrativas a particulares requiere de autorización legal expresa, otorgada por el Congreso de la República o, cuando la ley así lo habilite, mediante acto administrativo que desarrolle un marco legal preexistente que contemple dicha posibilidad. Ninguna de las leyes que confieren a la CRC la competencia de administración de los recursos de identificación, ni la Ley 1341 de 2009, ni la Ley 1978 de 2019, habilita a la Comisión para delegar, encargar o trasladar a un tercero particular el ejercicio de las funciones de verificación, validación y certificación que son inherentes a dicha competencia. En consecuencia, la creación del Validador Centralizado por la vía de una resolución de carácter general excede la potestad reglamentaria de la CRC y no satisface la reserva de ley que la Constitución y la Ley 489 de 1998 exigen para la atribución de funciones públicas a particulares.

Por lo anterior, PTC reitera su solicitud de que las funciones actualmente previstas para el Validador Centralizado sean ejercidas directamente por la CRC, en su calidad de Administrador de los Recursos de Identificación, sin perjuicio de que esta pueda apoyarse en terceros para la prestación de servicios técnicos u operativos puramente instrumentales –tales como infraestructura tecnológica o soporte operativo–, siempre que las decisiones de verificación, validación, certificación, aprobación o rechazo que tengan incidencia directa sobre el acceso a los recursos de identificación permanezcan radicadas en cabeza de la Comisión. En consecuencia, y conforme a la naturaleza de funcionamiento e importancia de la materia, **debería ser la CRC quien ejerza este tipo de funciones de Validador Centralizado,** y junto a ello, incorporar medidas regulatorias adicionales que mitiguen estos riesgos, garanticen condiciones equitativas de acceso al mercado y eviten la posible generación de barreras de entrada o restricciones indebidas a la competencia.

Adicionalmente, el Proyecto debería **precisar de manera expresa y detallada la gobernanza** aplicable a los registros, bases de datos, listas y mecanismos de clasificación que sirven de insumo para validar, bloquear, etiquetar o restringir comunicaciones en el ecosistema A2P.

En particular, resulta indispensable definir con claridad:

- La **titularidad, administración y supervisión** de dichos registros, incluyendo las responsabilidades específicas de cada actor involucrado;
- Los **criterios técnicos, objetivos y verificables** que deben aplicarse para la inclusión, exclusión, suspensión o reclasificación de originadores, SENDER ID, códigos cortos y plantillas;
- Los estándares mínimos de **soporte probatorio** requeridos para adoptar decisiones que generen efectos restrictivos; y
- Los **plazos máximos y perentorios** para la atención y resolución de solicitudes de revisión, actualización o corrección de la información contenida en dichos sistemas.

La ausencia de estas definiciones genera un margen de discrecionalidad que puede derivar en **decisiones arbitrarias o inconsistentes**, incrementar la ocurrencia de falsos positivos y afectar de manera desproporcionada a los agentes del mercado.

En este sentido, dichas precisiones no solo son necesarias para dotar de seguridad jurídica y operativa al esquema propuesto, sino también para garantizar que los actores potencialmente afectados cuenten con **mecanismos efectivos de contradicción, defensa y debido proceso**, en línea con los principios de transparencia, trato no discriminatorio y promoción de la competencia previamente señalados.

Teniendo en cuenta lo anterior, y considerando las contingencias que se derivan del proyecto, se solicita a la CRC mapear los efectos que de las medidas se derivan, con relación al Análisis de Impacto Normativo (AIN), comprender en tal sentido, indicadores mínimos de desempeño y efectividad, falsos positivos en el bloqueo o etiquetado de mensajes, niveles de disponibilidad del validador, tiempo de respuestas a consultas, entrega de comunicaciones críticas, número de solicitudes de corrección o reclasificación y evolución de eventos de fraude asociados a SMS o llamadas.

Tal trazabilidad en asunción del AIN, permitirá a la CRC verificar los ajustes oportunos y necesarios, evaluando la proporcionalidad de las obligaciones impuestas y evitaría que medidas concebidas para proteger al usuario terminen afectando servicios legítimos esenciales.

Por otra parte, si bien el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles, es un canal de interacción que prevé el proyecto, resulta importante y conveniente que el Proyecto incorpore la **habilitación de canales seguros y estandarizados de intercambio de información entre los PRST, asignatarios de códigos cortos A2P**, proveedores de contenido y aplicaciones (PCA), integradores tecnológicos de **manera independiente a la CRC.** Estos mecanismos deben estructurarse bajo principios claros de gobernanza de datos, que garanticen el uso adecuado y controlado de la información compartida.

Asimismo, es fundamental que dicho intercambio se rija por criterios estrictos de necesidad, finalidad y proporcionalidad, limitando el tratamiento de la información exclusivamente a los fines legítimos de prevención, detección y mitigación de fraudes y abusos. Igualmente, deberán contemplarse salvaguardas robustas en materia de reserva de la información y protección de datos personales, en cumplimiento del marco normativo aplicable.

La implementación de estos canales contribuirá a fortalecer la coordinación interinstitucional, mejorar la eficacia de las medidas preventivas y reducir riesgos sistémicos, sin afectar indebidamente los derechos de los actores involucrados. En definitiva, su adecuada regulación permitirá alcanzar un equilibrio entre la seguridad del ecosistema y la promoción de condiciones de competencia leal y transparente.

3.7. COMITÉ TÉCNICO DE LUCHA CONTRA EL FRAUDE EN REDES DE SERVICIOS MÓVILES

PTC está de acuerdo con la creación del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles (En adelante CTLFSM) como instancia de intercambio de alertas, identificación de patrones de fraude y espacio de revisión técnica de medidas frente al fraude cibernético a través de servicios de voz móvil

y mensajes cortos de texto (SMS). No obstante, se consideran algunos aspectos a precisar del proyecto los cuales se enuncian en los siguientes términos:

- ✓ Artículo 2.1.10.7.3.2. – Periodicidad y convocatoria: El proyecto establece que la CRC podrá convocar de manera extraordinaria cuando se presenten incidentes de fraude en servicios móviles que requieran **atención urgente** o cuando las circunstancias del ecosistema así lo demanden. Ahora bien, no se evidencia dentro del resto del proyecto de resolución que se puede llegar a entender por "atención urgente", dado que en materia de incidentes de fraude todos deben ser atendidos en una ventana temporal y con un procedimiento de urgencia conforme se estandarizó en el mismo proyecto en las medidas asociadas a SMS y Telefonía móvil.

  En este sentido, se solicita a la CRC respetuosamente aclarar la expresión "Atención urgente" con el fin de tener expresas estas circunstancias que darían cabida a la convocatoria. Asimismo, es menester que se aclare si la convocatoria pudiera ser promovida ante la CRC a solicitud de parte, por uno de los agentes del CTLFSM (PRST y Asignatarios de recursos de identificación A2P) o el mismo únicamente resulta ser ex oficio por parte de la Comisión.

- ✓ Artículo 2.1.10.7.3.4. – Vinculatoriedad: el proyecto de resolución establece que las decisiones del CTLFSM sobre los parámetros técnicos serán de cumplimiento obligatorio para los PRST en los términos y plazos establecidos en la respectiva acta de sesión y, **de identificarse necesario, en la resolución por medio de la cual se incorporen actualizaciones a la regulación general**, la cual será expedida por el Director Ejecutivo de la Comisión, previa aprobación del Comité de Comisionados de Comunicaciones de la CRC.

  Lo cual, resulta preocupante al ser analizado desde el Análisis de Impacto Normativo, puesto que el artículo 16 del mismo proyecto regulatorio **incluye dentro de los casos de proyectos de regulación que no son sujetos de publicación la expedición de las resoluciones de las que trata el artículo 2.1.10.7.3.4. relacionadas con las decisiones que adopte el CTLFSM en los términos allí contenidos, en los Casos de proyectos de regulación no sujeta a publicación.**

  Esta situación puede resultar particularmente gravosa para los PRST, en la medida en que la expedición de actos administrativos de carácter general que habiliten la introducción de modificaciones técnicas por decisión de la Comisión, sin surtir previamente un proceso de discusión sectorial ni un análisis de impacto normativo que permita evaluar su necesidad,

proporcionalidad y efectos, podría generar cargas operativas y económicas significativas para los agentes obligados.

Lo anterior resulta especialmente relevante cuando dichas modificaciones implican desarrollos tecnológicos, ajustes en sistemas, cambios operativos o inversiones adicionales cuya implementación demanda recursos y tiempos de ejecución que deben ser debidamente valorados. En consecuencia, la adopción de este tipo de medidas sin una evaluación previa de sus impactos y de su eficiencia en costos podría afectar los principios de transparencia, participación y regulación eficiente que orientan la actuación regulatoria.

Por lo anterior, PTC considera que cualquier modificación técnica que genere nuevas obligaciones para los agentes del sector debe ser objeto de un proceso previo de consulta pública y de un análisis de impacto normativo que permita valorar adecuadamente sus efectos técnicos, operativos y económicos, garantizando la participación efectiva de los sujetos obligados y la adopción de medidas regulatorias proporcionales y razonables.

Por lo anterior, se solicita a la CRC modificar la redacción prevista en el referido articulo 2.1.10.7.3.4. en los siguientes términos:

"2.1.10.7.3.4. Vinculatoriedad. En el marco del CTLFSM los participantes podrán proponer y acordar mejoras en la implementación de las medidas mínimas establecidas en el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, cuando la evolución de las modalidades de fraude así lo requieran. En caso de que no haya propuestas o acuerdos de mejoras, aplicarán los estándares mínimos establecidos en el mencionado artículo. Las decisiones del CTLFSM sobre tales parámetros serán de cumplimiento obligatorio para los PRST en los términos y plazos establecidos en la respectiva acta de sesión ~~y, de identificarse necesario, en la resolución por medio de la cual se incorporen actualizaciones a la regulación general, la cual será expedida por el Director Ejecutivo de la Comisión de Regulación de Comunicaciones, previa aprobación del Comité de Comisionados de Comunicaciones de la CRC~~. La vinculatoriedad de estas decisiones deriva de la obligación regulatoria de participar en el CTLFSM. Las decisiones del CTLFSM no podrán, en ningún caso, desmejorar, degradar, modificar o derogar los parámetros técnicos mínimos establecidos en el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016."

Esto, guarda coherencia dado que como se dispuso en el artículo 2.1.10.7.3.6. del proyecto en comento, se establece que los resultados y actas del CTLFSM servirán a la CRC como insumo técnico para la

actualización de cualquier medida contenida en la resolución CRC 5050 de 2016, protegiendo de tal formal el derecho de participación que le asisten al sujeto pasivo de la obligación.

- ✓ 2.1.10.7.3.16. Vigencia de CTLFSM. En relación con lo establecido en el parágrafo del proyecto en comento en el que se indica "Cualquier incumplimiento a las disposiciones establecidas en el artículo 2.1.10.7. dará lugar a que la CRC realice el respectivo traslado a la SIC o al MinTIC para el ejercicio de sus funciones de vigilancia y control de conformidad con sus respectivas competencias" PTC considera que tal atribución si bien es competencia de la Comisión en el marco de sus funciones, para que dicha remisión oficiosa deba darse, resulta necesario incorporar dentro del proyecto en comento, reglas asociadas sobre **incumplimiento injustificado o atribuible exclusivamente al obligado.** Ya que de advertirse alguna causal legal que le justifique o le impida dar cumplimiento, la remisión oficiosa a autoridades de control como la SIC o el MinTIC puede saturar innecesariamente a las autoridades de control y agravar la carga administrativa al obligado.

3.8. BLOQUEO O ETIQUETADO DE MENSAJES

El artículo 6.13.4.7.2 del Proyecto establece que, antes de enrutar cada mensaje A2P, el Proveedor de Redes y Servicios de Telecomunicaciones –PRST– deberá verificar en el sistema validador la existencia del código corto A2P, del *Sender ID* y de la plantilla vigente. En caso de que alguno de estos elementos no se encuentre registrado o validado, el PRST deberá bloquear el mensaje e impedir su entrega al usuario final o, **alternativamente, marcarlo con una etiqueta de "no verificado".**

Desde el punto de vista de política regulatoria, la medida puede generar efectos adversos sobre la confianza del usuario. Si un mensaje legítimo de autenticación, seguridad o prevención de fraude es marcado como "no verificado", el usuario puede interpretar que se trata de una comunicación fraudulenta, aun cuando provenga de un remitente legítimo. Esto puede debilitar la confianza en los canales formales utilizados por entidades financieras, plataformas digitales, comercios, prestadores de servicios esenciales y remitentes globales.

Más aún, una señalización inconsistente o errónea podría ser aprovechada por actores maliciosos mediante esquemas de ***ingeniería social***. Los defraudadores podrían explotar la confusión generada por mensajes legítimos etiquetados como "**no verificados" para inducir al usuario a abandonar los canales oficiales y dirigirlo hacia canales alternativos menos seguros**. Así, una herramienta concebida para fortalecer la confianza podría terminar generando incertidumbre y ampliando las superficies de riesgo. En términos de

proporcionalidad, la Comisión debería ponderar no solo el beneficio esperado de la medida, sino también el costo potencial de falsos negativos, fallas de sincronización, indisponibilidad del sistema o etiquetados erróneos. Por ello, una exigencia procedimental no debería convertirse en una barrera operativa que comprometa la seguridad, la experiencia del usuario o la continuidad de servicios esenciales.

En consecuencia, se recomienda ajustar la redacción del artículo 6.13.4.7.2 para incorporar salvaguardas que permitan equilibrar los objetivos de seguridad con la necesidad de garantizar la entrega oportuna de comunicaciones críticas. Finalmente, el PRST no debe asumir la responsabilidad de marcar la etiqueta como "No verificado" es un riesgo bastante critico que no puede recaer en discusión mediante regulación.

3.9. PROCESO DE CONOCIMIENTO DEL CLIENTE (KYC)

Frente a las disposiciones contenidas en el artículo 6.13.3.1. por el cual se dispone el proceso de debida diligencia que deben surtir los asignatarios del código corto A2P respecto de cada agente con quien celebren contratos para cursar tráfico A2P, con carácter previo al inicio de la relación contractual y de manera continua durante su vigencia, PTC considera esta medida indispensable en la reducción de eventos de fraude.

Es necesario que **el responsable de la emisión de los contenidos realice un procedimiento de conocimiento del cliente**, la identificación de tal persona es la única herramienta posible para determinar en grado de responsabilidad e investigación penal la persecución de aquellos delitos asociados con el fraude.

Doctrina especializada ha documentado que en los casos de estafas bajo modalidad de delito informático en su mayoría terminan con orden de archivo por parte de la Fiscalía General de la Nación, Carrizosa señala que: *"la Fiscalía General de la Nación afronta sus propios desafíos técnicos y de personal para investigar los delitos informáticos frente a la alta demanda investigativa cuyo resultado es que cerca del 95% de las denuncias de delitos informáticos hoy estén en la impunidad."*[4] En este sentido identificar un posible responsable es objetivamente la forma de determinar la cadena final del presunto autor de conductas delictivas.

3.10. ACCESO AL REGISTRO DE NÚMEROS EXCLUIDOS

En validación del parágrafo del artículo 2.1.18.1. del proyecto de resolución, establece que "*La Superintendencia de Industria y Comercio (SIC), en el marco de*

[4] CARRIZOSA, Xiomara. Los retos de la investigación y sanción penal del delito de estafa en espacios digitales. Universidad Cooperativa de Colombia. 2024.

sus competencias y, en especial, en virtud de la facultad prevista en el artículo 9[5] *de la Ley 2300 de 2023, podrá solicitar a la CRC cualquier tipo de información relacionada con los trámites administrativos de recuperación de recursos de identificación establecidos en el TÍTULO VI de la Resolución CRC 5050 de 2016, con la finalidad de que sirvan de insumo para las investigaciones que la SIC adelanta relacionadas con el RNE**. La SIC podrá solicitar información al validador centralizado, una vez esté, con la finalidad de recabar insumos y pruebas que sirvan para las investigaciones que la SIC adelanta relacionada con el RNE***»"

PTC pone de presente que, si bien la CRC expresamente por mandato de Ley tiene la obligación de remitir información de insumo para las investigaciones que adelanta la SIC relacionado con el RNE, no por ello, puede pretender extender tal competencia sin disposición legal de por medio frente al Validador Centralizado. Ello conlleva a desconocer por mandato de ley los límites que ostenta tal prerrogativa, esto confirma que el deber ser indica que las facultades que se pretenden atribuir al Validador Centralizado, sean asumidas directamente por la Comisión, ratificando lo expuesto líneas atrás.

En este sentido, el artículo 5 de la Ley 2300 de 2023 estipuló que el gobierno nacional a través del MINTIC coordinará con la Comisión la implementación de **las medidas técnicas necesarias para adoptar el registro de Números Excluidos** conforme a lo establecido en la ley.

Con lo anterior, se evidencia un limitante material, referido sobre la implementación de medidas técnicas asociadas con el RNE, más ello, no derivo en una competencia reglamentaria para que la Comisión disponga como obligación del Validador Centralizado suministrar información a la SIC.

Para tal efecto, debe precisarse que quien dispone y administra el RNE es la Comisión, por lo cual, es la CRC quien cuenta con información actualizada sobre el registro y consulta de este y, corresponderá a la SIC vigilar entorno a las competencias legalmente definidas solicitar la información correspondiente a la entidad estipulada en la Ley.

En atención a lo anterior, se solicita respetuosamente a la CRC eliminar el apartado en el que pretende habilitar un requerimiento directo por parte de la SIC ante el Validador Centralizado.

[5] **ARTÍCULO 9.** El incumplimiento de las medidas de protección de que trata la presente ley, se sancionará por la Superintendencia Financiera de Colombia y la Superintendencia de Industria y Comercio, de acuerdo con el marco de competencias previsto en la Ley Estatutaria 1266 de 2008 o las normas que lo modifiquen, adicionen o sustituyan.

3.11. CAMPAÑAS PEDAGÓGICAS DE LOS ASIGNATARIOS Y OPERADORES

Entorno a la obligación de realizar al menos cuatro (4) campañas pedagógicas a cargo de los PRST difundidas en redes sociales y páginas web, teniendo en cuenta el nivel de detalle que estas requieren, consideramos que, puede resultar subjetiva y no estratégica la forma en la que se tendría por cumplida esta obligación.

En este sentido, el artículo 6.14.1.3 del proyecto establece una carga de detalle que debe ser divulgada a la ciudadanía en relación con los "*derechos de los usuarios respecto de sus datos personales, las modalidades de fraude existentes a través de mensajes de texto y llamadas de voz, las técnicas de ingeniería social utilizadas por los ciberdelincuentes para obtener información confidencial, y las acciones que los usuarios pueden tomar para prevenirlas o mitigarlas*", prueba que debe ser enviada a la CRC, quince (15) días siguientes a la finalización de cada trimestre.

Considerando lo anterior, PTC sugiere respetuosamente que la CRC fije un modelo estándar de contenido a ser publicado por los PRST que contenga la información y detalle que la Comisión estima necesaria para conocimiento del usuario[6], a efectos de que en el futuro se entienda cumplida la obligación con la publicación de esta. Lo anterior, deja de lado, cualquier interpretación subjetiva que pudiera llegar a generarse por la ausencia de algún componente o información que el funcionario de la Comisión en el momento de la verificación considere.

Asimismo, considérese que para que las medidas pedagógicas resulten ser efectivas, es importante que desde entidades como el MinTic, se adelante asistencia especial para aquellos grupos con índices bajos de alfabetización digital, con el fin de que los usuarios conozcan la importancia de protección de sus datos personales. Lo anterior, se ve alineado con lo dispuesto en el artículo 12 de la Ley 2573 de 2026, por el cual se autorizó al MinTIC a incorporar los recursos necesarios para que se financien productos audiovisuales cortos con perfil multiplataforma que informe a las personas la importancia del manejo de sus datos personales y del correcto uso de las redes sociales y la ruta que deben seguir en caso de ser afectadas por la utilización de sus datos personales de forma fraudulenta ante un operador de telecomunicaciones, entidad financiera y crediticia y demás establecimientos comerciales con esta competencia.

[6] La CRC ya ha fijado contenidos unificados, ejemplo de ello, es el contrato único convergente el cual se estandarizó para aplicación y modificación puntual en ciertos campos por parte de los PRST.

3.12. FORMACIÓN INTERNA EN MATERIA DE PREVENCIÓN DEL FRAUDE

PTC estima razonable la obligación asociada con los programas de formación interna en materia de prevención del fraude cibernético dirigidos a los equipos de trabajo, con una periodicidad mínima de cuatro (4) sesiones al año, una por cada trimestre calendario.

Ahora bien, en relación con la acreditación de cumplimiento de esta obligación, en la cual, se espera que dentro de los quince (15) días hábiles siguientes a la finalización de cada trimestre, el agente obligado remita a la CRC un reporte que acredite "el cumplimiento del programa de formación del período, con indicación del número de empleados capacitados, los contenidos cubiertos, la metodología utilizada y la **cobertura por área funcional"**, PTC sobre este último aspecto, solicita a la Comisión aclarar a que hace referencia con cobertura por área funcional, con el fin de evitar interpretaciones subjetivas.

Asimismo, es menester que la CRC indique si para efectos de esta acreditación se creara un formato de cumplimiento, un canal especial al cual se deberá remitir tal reporte (correo electrónico general de la CRC o especial del CTLFSM) determinando de manera clara y expresa la contactabilidad para tal fin.

Por último, en relación con la fecha de vigencia que prevé el proyecto para esta obligación (Artículo 6.14.1.5.)[7] PTC considera que en vista de las gestiones administrativas que comprende al interior de las compañías el efectuar un contenido propicio para las diversas áreas, se considera que esta obligación debería ser exigible a corte del siguiente trimestre en el que entre a regir la norma. Lo anterior, permitirá en primera medida adoptar un plan de trabajo que tenga en cuenta no solo el impartir y difundir el contenido, si no también, evidenciar en esta primera fase, aspectos de mejora que pudieran pulirse conforme a la entrada en vigor de la norma, así como de las obligaciones especiales que de estas se derivan.

En conclusión, PTC considera que la lucha contra el fraude cibernético exige una aproximación regulatoria integral que reconozca la participación y responsabilidad de todos los actores que intervienen en la cadena de generación, agregación, validación, transporte y entrega de las comunicaciones, especialmente de los PCA e Integradores, que son quienes menor responsabilidad e impacto reputacional tienen de cara al usuario.

No resulta eficiente ni proporcional que las obligaciones continúen concentrándose principalmente en los PRST, cuando muchos de los riesgos que

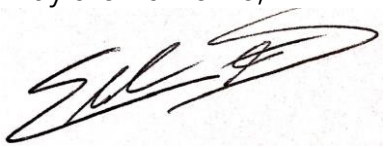
[7] Al momento de la publicación de esta resolución en el Diario Oficial: El artículo 15 de esta resolución, por medio del cual se adicionó el Capítulo 14 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016.

se pretenden mitigar se originan en etapas previas del ecosistema y son controlados por otros agentes.

En consecuencia, la CRC debe propender por un esquema de corresponsabilidad regulatoria en el que los PCA, los Integradores Tecnológicos, los asignatarios de recursos de identificación y los demás actores involucrados asuman obligaciones efectivas de debida diligencia, trazabilidad, verificación y prevención del fraude, acordes con el grado de control que ejercen sobre dichas actividades. Combatir el fraude requiere intervenir sus causas y no únicamente sus efectos; por ello, la efectividad de las medidas regulatorias dependerá de que las responsabilidades se distribuyan de manera equilibrada entre todos los participantes del ecosistema, evitando trasladar a los PRST funciones de control que material y jurídicamente corresponden a terceros. Solo bajo un modelo de responsabilidades compartidas será posible fortalecer la confianza de los usuarios, reducir de manera efectiva los incentivos al fraude y garantizar la sostenibilidad de las medidas regulatorias en el largo plazo.

Así las cosas, manifestamos nuestro apoyo a la finalidad perseguida por la CRC, y esperamos que los comentarios contenidos en el presente escrito resulten constructivos y sean acogidos por la CRC, a efectos de fortalecer el presente proyecto, así como la estrategia liderada por el regulador y demás autoridades sectoriales en torno a la lucha contra el fraude cibernético a través de servicios móviles.

Muy atentamente,



EMILIO SANTOFIMIO JARAMILLO
Director de Regulación
Partners Telecom Colombia S.A.S