

VPAC-100021-03-045

Bogotá D. C, 29 de diciembre de 2025

Doctora

CLAUDIA XIMENA BUSTAMANTE

Directora Ejecutiva

COMISIÓN DE REGULACIÓN DE COMUNICACIONES -CRC-

medidasantifraude@crcom.gov.co; atencioncliente@crcom.gov.co;

Calle 59A Bis N° 5-53 Edificio Link Siete Sesenta

Ciudad

Asunto: Comentarios al Documento de **Alternativas Regulatorias** del proyecto de *"Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles"* publicada por la CRC.

Apreciada Directora,

Reciba un cordial saludo. **Partners Telecom Colombia S.A.S.**, en adelante **"PTC"**, se dirige a usted, con el fin de presentar nuestros comentarios frente al proyecto señalado en el asunto, manifestando la relevancia y pertinencia del proyecto en el marco de un escenario complejo para la seguridad cibernética, especialmente por el uso inescrupuloso que la delincuencia realiza de los servicios móviles.

Desde PTC, manifestamos nuestra profunda preocupación en torno a la amenaza que el fraude cibernético representa para los usuarios, resaltando la importancia de este tipo de espacios para avanzar en la construcción e implementación de medidas que resulten adecuadas, no solo desde la óptica de los deberes antifraudes que se han impuesto a los PRST, sino también de los deberes y responsabilidades que deben asignarse a todos los actores que participan en la cadena de valor, como agregadores, PCA, plataformas, entre otros.

A continuación presentamos nuestros comentarios, abordando los diferentes puntos desarrollados en el documento de consulta pública de la Comisión.

1.1 Temáticas enfocadas en mitigar el contacto a usuarios mediante SMS.

1.1.1. Temática 1: Falta de identificación clara del remitente en SMS A2P.

Alternativa propuesta: Alternativa 2 – Asignación y uso de código alfanumérico (Sender ID).

PTC considera que la alternativa que introduce la obligatoriedad del uso de Sender ID alfanuméricos únicos para tráfico A2P constituye una medida efectiva y proporcional para mitigar el fraude por suplantación de identidad en SMS.

El uso de Sender ID permite una identificación clara y visible del remitente para el usuario final, reduciendo significativamente la probabilidad de engaño mediante mensajes que aparentan provenir de entidades legítimas. Técnicamente, esta solución es compatible con las plataformas actuales de mensajería A2P y con los mecanismos de control ya implementados por los operadores, lo que facilita su adopción sin requerir cambios disruptivos en la red.

Adicionalmente, la asignación controlada de Sender ID, asociada a procesos de validación previa de marca y contenido, fortalece la trazabilidad del tráfico A2P, permitiendo acciones de bloqueo oportunas ante comportamientos fraudulentos.

➤ Preguntas generales para esta alternativa:

Para esta alternativa, se tiene un tiempo estimado de implementación de un (1) año, contado a partir de la definición regulatoria y de los lineamientos técnicos asociados a la gestión de Sender ID. Este plazo contempla los ajustes necesarios en plataformas de mensajería, la adecuación de sistemas de enrutamiento y validación, así como la coordinación con agregadores y proveedores de contenido A2P.

Dentro de los retos técnicos, operativos y regulatorios, se identifican retos asociados al alto procesamiento en los ESME, derivado del incremento en los controles de validación de remitentes, así como a la correcta implementación del enrutamiento de códigos alfanuméricos en las redes de interconexión (ICX). En el ámbito operativo, la habilitación, eliminación y adición de nuevos códigos alfanuméricos requiere recursos especializados, procesos de gestión continua y capacidades de monitoreo reforzadas.

Adicional a lo anterior, es importante que se establezca un esquema claro para la organización y unicidad de los códigos, evitando duplicidades y posibles conflictos entre marcas o remitentes, así como implementar un esquema gradual, iniciando con un piloto controlado para remitentes de alto volumen y marcas críticas, complementado con campañas de socialización con agregadores, lo que permitiría obtener victorias tempranas en la reducción de mensajes fraudulentos.

1.1.2. Temática 2: Dificultad de trazabilidad en comunicaciones A2P.

Alternativa propuesta: Alternativa 4 - Identificación exclusiva mediante códigos cortos y numeración E.164.

PTC considera que la alternativa basada en la asignación de recursos exclusivos (códigos cortos o numeración E.164) para marcas constituye una solución integral que aborda tanto la trazabilidad como la prevención del fraude A2P.

Desde el punto de vista técnico, la exclusividad de los recursos de numeración facilita la identificación inequívoca del originador, permitiendo un monitoreo más preciso del tráfico y la aplicación de controles preventivos basados en patrones de uso. La incorporación de medidas complementarias como la categorización de contenido, el consentimiento del usuario y el KYC obligatorio para agregadores fortalece el control en toda la cadena de valor.

Asimismo, esta alternativa permite articular las medidas técnicas con registros existentes como el RNE, promoviendo coherencia normativa y evitando duplicidades. Si bien implica esfuerzos operativos para los actores del mercado, estos se justifican por el impacto positivo en la reducción del fraude y en la confianza del usuario en los servicios A2P.

➤ Preguntas generales para esta alternativa:

Para la implementación de esta alternativa, se estima un plazo de un (1) año, una vez sea asignado y habilitado el NDC 940, para la implementación completa de esta alternativa. Dicho plazo contempla la adecuación de plataformas, la reasignación de recursos de numeración y la formalización de procesos de validación con marcas y agregadores.

Dentro de los retos técnicos, operativos y regulatorios, esta alternativa mejora significativamente la trazabilidad, su implementación requiere una coordinación estrecha entre la CRC, los PRST y los agregadores, particularmente en la asignación y administración de los recursos de numeración exclusiva para su correcta configuración y gestión.

En caso de que se implemente, se sugiere una implementación por etapas, priorizando inicialmente a las marcas con mayor volumen de tráfico A2P, mientras se habilitan progresivamente los demás actores del ecosistema.

1.1.3. Temática 3: Falta de control en SMS P2P.

Alternativa propuesta: Alternativa 2 - Control de patrones de tráfico atípicos.

La implementación de mecanismos de detección de comportamientos anómalos en tráfico P2P, PTC considera que esta es la alternativa más adecuada al permitir un enfoque basado en análisis de red y gestión de riesgo.

Técnicamente, los PRST y demás actores tendrían que garantizar la capacidad de identificar patrones atípicos, como envíos masivos desde líneas individuales, tráfico intensivo hacia destinos no habituales o comportamientos incompatibles con el uso personal del servicio móvil. La aplicación de alertas automáticas y bloqueos temporales resulta una medida flexible y proporcional, que evita afectar

el uso legítimo del servicio por parte de los usuarios. Adicionalmente, esta alternativa evita restricciones generalizadas a planes con SMS ilimitados, preservando la libertad comercial, y se alinea con el principio de intervención mínima necesaria, enfocándose en el comportamiento fraudulento y no en el servicio en sí.

➤ Preguntas generales para esta alternativa:

Esta alternativa se encuentra asociada a procesos de aseguramiento continuo, pero según las disposiciones regulatorias se necesitaría un (1) año para su implementación dado que los mecanismos de detección y análisis de tráfico requieren ajustes en función de las disposiciones de fraude que sean indicadas.

Con relación a los retos técnicos, operativos y regulatorios, se resalta la necesidad de mantener modelos dinámicos de detección, evitando afectaciones al uso legítimo del servicio por parte de los usuarios. Para lo anterior, se propone fortalecer los controles existentes e incrementar gradualmente los umbrales de detección, permitiendo una adaptación progresiva y la obtención de resultados tempranos.

1.2. Temáticas enfocadas en mitigar el fraude mediante servicios de voz.

1.2.1. Temática 1: Enmascaramiento de la identidad de línea llamante (CLI).

Alternativa propuesta: Alternativa 2 - Prohibición total del enmascaramiento del CLI.

PTC considera que la prohibición del enmascaramiento en llamadas internacionales entrantes que presenten numeración nacional es una medida técnicamente efectiva, y necesaria, para reducir la suplantación de identidad. Desde el punto de vista de red, el bloqueo de este tipo de tráfico puede implementarse mediante reglas claras de enrutamiento y validación de señalización, con excepciones controladas para escenarios legítimos como el *roaming* internacional. Esta medida elimina una de las principales fuentes de fraude de voz, como el *vishing*.

➤ Preguntas generales para esta alternativa:

PTC estima un plazo de seis (6) meses para la implementación de esta alternativa, considerando que se trata de ajustes principalmente asociados a reglas de enrutamiento y validación de señalización.

Así mismo, se identifican retos relacionados con la generación de órdenes de trabajo, la coordinación entre áreas técnicas y la ejecución de cambios en ventanas programadas, con el fin de minimizar impactos en la red.

Adicionalmente, se sugiere iniciar con el bloqueo de rangos de alto riesgo previamente identificados, ampliando progresivamente la cobertura a otros rangos conforme se consoliden los controles.

1.2.2.Temática 2: Falta de aplicación coordinada de métodos preventivos.

Alternativa propuesta: Alternativa 2 - Prohibición total del enmascaramiento del CLI.

La creación de una plataforma nacional centralizada de intercambio de alertas es una alternativa que aporta valor desde una perspectiva sistémica del fraude.

El fraude de voz suele presentarse de manera distribuida y coordinada, por lo que la compartición de información en tiempo real entre operadores permite una respuesta más rápida y efectiva. Esta plataforma facilitaría la correlación de eventos, la identificación temprana de campañas fraudulentas y la mejora continua de los modelos de detección.

1.2.3.Temática 3: Ausencia de diferenciación en rangos de numeración.

Alternativa propuesta: Alternativa 2 - Rangos exclusivos para comunicaciones comerciales.

La definición de rangos de numeración específicos para comunicaciones comerciales y publicitarias aporta claridad tanto para el usuario como para los operadores. La diferenciación por NDC facilita la aplicación de filtros, políticas de gestión de tráfico y mecanismos de identificación automática del tipo de llamada. Esto mejora la capacidad del operador para implementar controles específicos sobre tráfico comercial.

Por lo anterior, es importante mencionar que esta medida fortalece la transparencia, facilita la supervisión y empodera al usuario para tomar decisiones informadas al recibir llamadas, contribuyendo a la reducción del fraude y de prácticas abusivas.

➤ Preguntas generales para esta alternativa:

PTC estima un plazo de un (1) año, una vez sean creados y definidos los rangos específicos de numeración E.164, para la implementación completa de esta alternativa.

La implementación requiere ajustes en sistemas de tarificación, enrutamiento y señalización, así como procesos de migración ordenada de los actores que actualmente utilizan numeración no diferenciada.

Con relación a los esquemas de transición o fases intermedias, se propone un esquema de migración gradual, iniciando con nuevos asignatarios y permitiendo un periodo de convivencia con la numeración actual.

1.2.4. Temática 4: Falta de estandarización de listas DNO.

Alternativa propuesta: Alternativa 2 - Registro DNO Nacional Único administrado por la CRC.

PTC sugiere esta alternativa ya que la creación de un registro DNO nacional único, administrado por la CRC, sería la alternativa más eficiente y coherente. Al contar con una fuente centralizada y actualizada en tiempo real permite una aplicación uniforme de bloqueos en todas las redes, reduciendo errores y asimetrías operativas. Además, simplifica la integración de los sistemas de los operadores con un único repositorio oficial, siendo una medida eficiente.

Adicionalmente, esta alternativa fortalece el rol coordinador de la CRC, elimina la fragmentación de criterios y garantiza condiciones homogéneas de cumplimiento, en beneficio de la eficacia de las medidas antifraude.

➤ Preguntas generales para esta alternativa:

PTC estima un plazo de un (1) año, una vez sea creado y puesto en operación el registro nacional de números DNO, para su integración completa con los sistemas de red.

Dentro de los principales retos se relacionan con la integración técnica del registro con los sistemas de los demás operadores y la definición de mecanismos de actualización en tiempo real.

Para esquemas de transición o fases intermedias, se sugiere que se contemple la posibilidad de iniciar con una versión mínima viable del registro, ampliando progresivamente su alcance y funcionalidades.

2. Respuesta a las preguntas formuladas por la CRC.

A continuación, se relacionan las respuestas de PTC a las preguntas formuladas por la CRC:

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

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

Como criterio mínimo, sugerimos que los integradores tecnológicos, se clasifiquen bajo un sistema de reputación establecido por la CRC, de manera que sea posible consultar el nivel de confiabilidad de cada agregador dependiendo de comportamiento y de su implementación, detección y gestión del fraude.

Dicho proceso debe ser digital, se debe realizar con soportes, por un determinado tiempo y debe extenderse tanto a integradores nacionales o internacionales.

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

Que permita conocer a los agregadores de manera pública y de conocimiento por parte de la CRC, de manera que se puede establecer confianza de cada agregador dependiendo de la medición del comportamiento en la detección del fraude.

Que sea un proceso digital, que solicite soportes, que sea por determinado tiempo y que no limite si es nacional o internacional.

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

El sistema debería tener la capacidad de procesar el total de los SMS enviados y recibidos en la red, que sea de manera automática y autónoma para evitar el filtrado de SMS de manera manual o búsquedas puntuales, debe ser masivo y el mismo software debe tener la capacidad de determinar la mayor probabilidad de

fraude, los bloqueos injustificados se darán y se deben desbloquear en el menor tiempo posible, estos deben ser analizados y aprobados o rechazados de manera manual.

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

El Código corto debe ser único para cada marca, este mecanismo ayudaría a los usuarios a identificar los originadores de manera clara.

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

Mecanismos de colaboración efectivos

- Plataforma de intercambio de información en tiempo real:
 - ✓ Base de datos compartida entre agregadores, operadores y autoridades para reportar fraudes detectados.
 - ✓ Alertas tempranas automatizadas.
 - ✓ Protocolos unificados de respuesta.
 - ✓ Procedimientos estandarizados para bloqueo de cuentas, suspensión de transacciones y notificación a usuarios.
 - ✓ Manuales operativos comunes.
 - ✓ Mesa técnica interinstitucional.
 - ✓ Reuniones periódicas para análisis de casos, tendencias y actualización normativa.
- Participación de entes judiciales y organismos de control: integración en tiempo real, mecanismos de comunicación clara y efectiva, apoyo entre las áreas de fraude de todas las compañías para mitigar este fraude

2.2. Frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz.

- En el servicio de llamadas de voz, los operadores pueden gestionar tanto tráfico originado por acuerdos directos con clientes nacionales (por ejemplo, bancos, comercios, entidades de salud, aerolíneas), como tráfico internacional que llega a través de cadenas de intermediarios, donde el originador de la llamada no siempre es certificado o plenamente identificable. ¿Qué diferencias, riesgos y oportunidades observa entre estos dos tipos de tráfico en relación con la prevención y mitigación del fraude?

¿Qué criterios, mecanismos o medidas considera relevantes para gestionar de manera diferenciada el tráfico directo y el tráfico en cadena, especialmente en lo relacionado con la trazabilidad, autenticación, control de llamadas sospechosas y judicialización?

El uso de llamadas desde bancos, comercio, entidades de salud, aerolíneas, deben tener una numeración única o mascarará que permita identificar el origen y así que se trata de una llamada legal, todo lo que este fuera de ese rango de líneas debe marcarse como spam o fraude, el cliente decide bloquear o no estas llamadas de origen

- ¿Qué mecanismos, herramientas o procedimientos tiene actualmente implementados su organización para detectar, prevenir y controlar el spoofing en llamadas de voz? ¿Qué nivel de efectividad han observado en estas medidas y qué retos técnicos y operativos han enfrentado en su aplicación?

Desde PTC, contamos con una estrategia de concientización dirigida a nuestros clientes. A través de mensajes de texto, compartimos recomendaciones de seguridad para prevenir posibles fraudes. Además, cuando se detecta una amenaza potencial, enviamos comunicados oportunos para alertar y proteger a nuestros usuarios.

PTC también tiene un programa de Alerta en línea que brinda recomendaciones de seguridad de la información a menores en los colegios

- ¿Qué efectos positivos y negativos prevé en la prohibición de llamadas internacionales con identidad de línea llamante CLI nacional? ¿Qué excepciones o consideraciones deberían contemplarse para no afectar la prestación de servicios legítimos?

Es positivo el control de dispersión de llamadas y llamadas cortas, se cuentan con controles automáticos que permiten bloquear la línea de manera unilateral en el momento donde se esté realizando llamadas automáticas a listas de clientes o numeraciones continuas, la efectividad es muy baja ya que las líneas detectadas tienen planes ilimitados de llamadas por lo cual no es viable el bloqueo al no tener una prueba

-¿Qué efectos positivos y negativos prevé en la prohibición de llamadas internacionales con identidad de línea llamante CLI nacional? ¿Qué excepciones o consideraciones deberían contemplarse para no afectar la prestación de servicios legítimos?

El uso de máscaras o prefijos que permita la identificación de las llamadas LDI entrantes con numeración local.

- ¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema que permita el enmascaramiento de la identidad de la línea llamante CLI en llamadas internacionales, siempre que estas sean etiquetadas en el dispositivo del usuario como “No verificada” o “Probable fraude”? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la prevención del fraude, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

El principal reto estaría relacionado con validar que se trata de una llamada no verificada o de potencial fraude y comprobar que efectivamente se trata de fraude, deben existir mecanismos que informen que no trata de fraude.

- ¿Qué ventajas y desafíos observa en la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias? ¿Considera que esta medida podría ser efectiva para facilitar la identificación y denuncia de fraudes por parte de los usuarios?

Desde PTC, consideramos que la medida propuesta resulta adecuada.

- ¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la transparencia en las comunicaciones, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

La implementación de prefijos a la numeración actual ayudaría a los operadores a identificar el origen, pero no a los usuarios, el operador tomaría acciones en caso de que cada prefijo sea para cada integrador y/o PCA y no contar con tráfico mezclado. La manera más efectiva debe ser que cada integrador y/o PCA tenga su numeración asignada.

2.3. Frente a las temáticas enfocadas en la educación de la ciudadanía

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

Desde PTC, sugerimos tener en cuenta los controles de seguridad de la información introducidos en la ISO27001.

Confiamos en que con estos comentarios podamos contribuir positivamente en el devenir de los proyectos regulatorios listados y que confiamos sean tenidos en cuenta por la Comisión, reiterando nuestra total disposición para contribuir de manera efectiva al proceso regulatorio en beneficio de los usuarios y en la prevención del fraude.

Cordialmente,



EMILIO SANTOFIMIO JARAMILLO

Director de Regulación

PARTNERS TELECOM COLOMBIA S.A.S. EN REORGANIZACIÓN