



**Alianza
Latinoamericana
de Telecomunicaciones**

21 de julio de 2025

Comisión de Regulación de Comunicaciones

Cl 59 a bis # 5 – 53
Ed Link Siete Sesenta P9
Bogotá, Colombia.

Enviado por correo electrónico: medidasantifraude@crcom.gov.co

Ref: Consulta sobre “Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles”

Estimados Colegas,

Reciba un cordial saludo.

Me dirijo a usted en representación de la Alianza Latinoamericana de Telecomunicaciones¹ (ALT+), nuestra labor se centra en impulsar políticas públicas tecnológicamente neutrales, fomentar la innovación y asegurar que la regulación en el sector digital se fundamente en evidencia técnica y jurídica sólida.

En este marco, celebramos la iniciativa de la Comisión de Regulación de Comunicaciones (CRC) de Colombia, que reafirma su compromiso con la protección de los usuarios y la integridad de los servicios tradicionales de telecomunicaciones móviles mediante la publicación del documento de formulación del problema del proyecto: “Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles.”

Esta consulta pública representa un paso fundamental para construir, de manera conjunta con el sector y demás actores relevantes, soluciones regulatorias y no regulatorias que sean integrales, eficaces y sostenibles frente a una problemática creciente que afecta a miles de ciudadanos.

Desde ALT+ reconocemos el valor de este proceso abierto, participativo y técnico, y nos permitimos presentar nuestras observaciones y aportes con el ánimo de contribuir a una

¹ La Alianza Latinoamericana de Telecomunicaciones (ALT+) es una organización regional que agrupa asociaciones y colectivos de toda América Latina que representan a operadores locales y regionales independientes del sector de las telecomunicaciones. Su propósito es consolidar esfuerzos y compartir experiencias entre sus miembros para incidir de manera técnica, basada en evidencia y constructiva en políticas públicas, programas y legislación tanto a nivel nacional como internacional. ALT+ promueve una visión moderna de conectividad significativa, defiende el acceso equitativo al espectro, apoya incentivos fiscales para el desarrollo de infraestructura en comunidades desatendidas y fomenta una competencia justa entre tecnologías. La alianza también aboga por una regulación clara y transparente, y trabaja activamente para facilitar el intercambio de mejores prácticas entre operadores de la región.



**Alianza
Latinoamericana
de Telecomunicaciones**

regulación equilibrada, basada en la colaboración y orientada al fortalecimiento de la confianza y la seguridad en los servicios móviles.

Adecuación del Régimen de Recursos de Identificación

El régimen actual de numeración en Colombia presenta algunas vulnerabilidades que pueden ser aprovechadas con fines fraudulentos. Uno de los procesos donde se han identificado riesgos es la portabilidad numérica, un derecho que permite a los usuarios cambiar de operador conservando su número telefónico. Para mitigar posibles fraudes, como la duplicación de SIM (*SIM swapping* en inglés), la regulación vigente establece mecanismos de validación de identidad mediante datos personales y un Número de Identificación Personal (NIP) de confirmación.

Adicionalmente, la CRC ha explorado experiencias internacionales que incorporan tecnologías como la biometría y la autenticación multifactorial, con el objetivo de evaluar posibles mejoras en los esquemas de seguridad aplicables a este trámite. Si bien esta medida representa un avance significativo en la protección del usuario, su correcta implementación técnica y la uniformidad en su aplicación entre todos los operadores siguen siendo factores críticos. Además, persisten desafíos relacionados con falsos positivos, suplantación de biometría y brechas en zonas donde el acceso a mecanismos tecnológicos es limitado.

Por ello, se recomienda a la CRC continuar fortaleciendo los controles de portabilidad con auditorías periódicas, mecanismos de verificación complementarios y monitoreo de incidentes que permitan ajustar el esquema de autenticación en tiempo real. Esto con el objetivo de prevenir fraudes por suplantación, como la duplicación de SIM, en el que un atacante transfiere el número de una víctima a una nueva SIM para acceder a sus cuentas.

Adicionalmente, la trazabilidad de las llamadas de origen es limitada, especialmente cuando provienen de redes externas o servicios intermedios, dificultando la identificación del remitente real y el seguimiento de patrones de fraude. Otro factor crítico es el uso poco regulado de numeraciones cortas y líneas del tipo A2P (aplicación-a-persona), que son frecuentemente utilizadas en campañas de mensajería automatizada, pero que carecen de controles sobre autenticidad, propósito y destinatario final.

Frente a este panorama, resulta necesario que la CRC avance en una revisión progresiva, dialogada y equilibrada del marco regulatorio de numeración, con el fin de fortalecer los mecanismos de control y trazabilidad, sin comprometer la sostenibilidad del ecosistema de telecomunicaciones ni imponer cargas desproporcionadas.

El proceso debe reconocer la diversidad de condiciones operativas en el país, en particular las de los pequeños operadores que prestan servicios en zonas rurales, apartadas o de difícil acceso, donde el número de usuarios puede ser inferior a 1000. Para estos actores, la implementación de



**Alianza
Latinoamericana
de Telecomunicaciones**

nuevas obligaciones técnicas podría representar desafíos económicos relevantes. Por ello, se propone que la CRC contemple esquemas de implementación escalonada, así como incentivos regulatorios o apoyos técnicos que faciliten la adopción de mejores prácticas sin afectar la continuidad del servicio.

Del mismo modo, se invita a los grandes operadores a participar activamente en el diseño de soluciones colaborativas, reconociendo que un entorno más seguro beneficia a toda la cadena de valor. Medidas como una supervisión más rigurosa en la cesión de bloques numéricos y procesos progresivos de identificación y autenticación pueden contribuir significativamente a reducir el fraude, siempre que se adopten de forma flexible y con el acompañamiento institucional adecuado. Así, se puede avanzar en un modelo de seguridad integral que respete la pluralidad del mercado y promueva la equidad entre operadores.

Herramientas Regulatorias Viables Técnica y Económicamente

Existen diversas herramientas regulatorias que presentan alta viabilidad técnica y económica y que pueden ser implementadas para mitigar significativamente el contacto fraudulento a través de voz y SMS. Entre estas destacan los filtros de origen de llamadas, que permiten bloquear o desviar automáticamente comunicaciones provenientes de numeraciones o patrones previamente identificados como fraudulentos.

Estas herramientas pueden complementarse con mecanismos de cooperación entre operadores, tales como bases de datos compartidas —previa autorización expresa de los titulares— que consoliden información sobre líneas o remitentes asociados a actividades sospechosas. Estas iniciativas, desarrolladas bajo los principios de legalidad, finalidad y seguridad previstos en las Leyes 1266 de 2008 y 1581 de 2012, permiten fortalecer la capacidad de respuesta del sector frente a conductas fraudulentas.

Otra medida de alta efectividad consiste en establecer mecanismos de autenticación reforzada, tanto para el aprovisionamiento de servicios como para el envío masivo de mensajes, lo que incluye verificación en dos pasos, validación biométrica o certificados digitales. Adicionalmente, el uso de alertas visuales o auditivas para llamadas catalogadas como de alto riesgo puede advertir al usuario final en tiempo real sobre una posible amenaza, aumentando la probabilidad de que interrumpa el contacto antes de que se materialice el fraude.

Muchas de estas herramientas ya han sido probadas con éxito en mercados como Estados Unidos, España y México, donde han contribuido a reducir el volumen de llamadas fraudulentas y aumentar la confianza del usuario en los servicios tradicionales. Su implementación progresiva en Colombia, bajo la supervisión técnica de la CRC y en articulación con los operadores, permitiría una mejora sustancial en la protección ciudadana frente al fraude digital.



**Alianza
Latinoamericana
de Telecomunicaciones**

Acciones Educativas para los Usuarios

Una parte fundamental de la estrategia contra el fraude en servicios de telecomunicaciones es la formación del usuario como primera línea de defensa. La concientización ciudadana no solo fortalece la seguridad individual, sino que también contribuye a la protección colectiva del ecosistema digital. Por ello, se requieren campañas educativas sostenidas, masivas y multicanal, que aborden tanto la prevención como la capacidad de respuesta frente a incidentes relacionados con suplantación de identidad, fraudes telefónicos, bancarios o cibernéticos.

Las campañas deben estar orientadas a informar y empoderar a los usuarios frente a los riesgos asociados a llamadas y mensajes fraudulentos, así como a prácticas de ingeniería social cada vez más sofisticadas. Es crucial que estas acciones educativas incluyan ejemplos claros y contextualizados sobre cómo identificar intentos de suplantación de identidad, fraudes bancarios vía SMS o correo electrónico (por ejemplo, phishing² y smishing³), y mensajes falsos que simulan provenir de entidades oficiales. Estos contenidos deben destacar patrones comunes utilizados por los delincuentes, como el uso de urgencia, amenazas o beneficios falsos para inducir al usuario a revelar información personal o financiera.

En este contexto, la CRC puede desempeñar un rol de liderazgo impulsando una estrategia nacional de comunicación en ciberseguridad. Dicha estrategia debe incluir la articulación de esfuerzos entre medios tradicionales (radio, televisión, prensa), plataformas digitales (redes sociales, sitios web institucionales) y alianzas con actores clave como operadores móviles, entidades financieras, organismos de seguridad digital, ministerios del sector TIC, y centros educativos. Esta coordinación interinstitucional permite maximizar el alcance de los mensajes y reforzar la confianza de los usuarios en las fuentes de información oficiales.

Además, es esencial que estas campañas consideren la diversidad del público objetivo, diseñando materiales pedagógicos adaptados a audiencias vulnerables o especialmente expuestas al fraude. Entre estos grupos se destacan los adultos mayores, que pueden tener menos familiaridad con las tecnologías digitales; la población rural, que enfrenta barreras de conectividad y menor acceso a información oportuna; y los usuarios con baja alfabetización digital, que requieren explicaciones visuales, sencillas y accesibles. Los formatos pueden incluir videos explicativos, infografías ilustradas, cápsulas radiales, y talleres presenciales o virtuales,

² La Fiscalía General de la Nación define phishing como: “una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas.” Ver: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf>

³ La Fiscalía también define smishing como “Modalidad consistente en el uso del phishing, métodos de engaño para obtener información personal confidencial o estafar a alguien, pero a través de SMS (mensajes cortos de celular) en lugar de correos electrónicos.” Ver: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf>



**Alianza
Latinoamericana
de Telecomunicaciones**

desarrollados en lenguajes claros, incluyentes e incluso en lenguas indígenas cuando corresponda.

Otro componente clave es la facilitación del reporte de fraudes, a través de canales simples y eficientes. Entre las opciones recomendables se encuentran las líneas cortas gratuitas de denuncia, botones integrados en aplicaciones móviles, formularios accesibles en portales web, y mecanismos de retroalimentación inmediata que confirmen al usuario que su reporte ha sido recibido y canalizado. Asimismo, se pueden implementar campañas de incentivo a la denuncia ciudadana, reconociendo la participación activa de los usuarios como parte de una red colaborativa de prevención.

Estas iniciativas, si se implementan de manera continua y transversal, permitirán aumentar la resiliencia digital de la ciudadanía, reducir la vulnerabilidad frente a tácticas delictivas y fortalecer la confianza en los servicios digitales y de telecomunicaciones del país. El enfoque debe ser preventivo, pero también reactivo, habilitando a los usuarios para identificar amenazas, tomar decisiones informadas y reportar incidentes de manera eficaz.

Desde el plano internacional, tanto la Organización para la Cooperación y el Desarrollo Económicos (OCDE) como la Unión Internacional de Telecomunicaciones (UIT) han resaltado la importancia de la educación al usuario como un componente esencial de la ciberseguridad nacional. La OCDE, en sus lineamientos sobre políticas digitales, subraya que los gobiernos deben promover competencias digitales básicas y avanzar hacia una ciudadanía informada, consciente de los riesgos en entornos conectados. Además, recomienda crear campañas nacionales alineadas con principios de inclusión, accesibilidad y enfoque diferencial para garantizar su efectividad.

Por su parte, la UIT ha señalado en sus informes sobre protección al consumidor que la concientización y la educación de los usuarios son herramientas críticas para combatir prácticas como el spam, el fraude por SMS, y la suplantación de SIM. También ha instado a los reguladores y operadores a desarrollar programas conjuntos de alfabetización digital y ciberseguridad, enfocados especialmente en las poblaciones con menor acceso a educación formal o tecnológica. Estos programas deben estar acompañados de indicadores de medición del impacto educativo, para evaluar su eficacia y ajustar las estrategias según los resultados obtenidos.

En conjunto, la adopción de una política pública robusta de educación digital, basada en las mejores prácticas internacionales y adaptada a las realidades locales, representa una inversión estratégica en la defensa del entorno digital. A medida que los delincuentes perfeccionan sus técnicas, la capacitación permanente del usuario se convierte en el eslabón más fuerte para prevenir el fraude y garantizar la seguridad del ecosistema digital colombiano.



**Alianza
Latinoamericana
de Telecomunicaciones**

Líneas de Acción y Recomendaciones Institucionales

La CRC debe establecer un conjunto claro de líneas de acción que refuercen su papel coordinador dentro de una estrategia nacional de lucha contra el fraude por medios tradicionales. Esto incluye la actualización urgente del régimen de numeración, la definición de estándares técnicos mínimos para identificación de llamadas y mensajes, y el desarrollo de normativas que obliguen a operadores a reportar eventos sospechosos y colaborar con las autoridades competentes.

Igualmente, se recomienda la creación de un observatorio interinstitucional sobre fraude en telecomunicaciones, donde confluyan la CRC, la Superintendencia de Industria y Comercio, la Policía Nacional, la Fiscalía, el sector financiero y las asociaciones de consumidores. Este espacio debe servir para compartir datos, generar inteligencia preventiva y diseñar respuestas rápidas ante incidentes masivos.

Finalmente, la CRC puede liderar la expedición de un protocolo unificado que estandarice los procesos de atención al usuario víctima de fraude, asegurando una respuesta eficiente, coherente y coordinada entre todos los actores del ecosistema.

Colaboración entre la CRC y la Policía Nacional

Dado que la Policía Nacional es la entidad constitucionalmente encargada de prevenir, investigar y combatir los delitos informáticos en Colombia, y considerando que la CRC posee el conocimiento técnico, normativo y operativo sobre el funcionamiento de las redes, servicios móviles y el comportamiento del ecosistema digital, se propone establecer un marco de colaboración interinstitucional entre ambas entidades.

Esta alianza permitiría combinar las capacidades legales de la Policía con la experiencia sectorial de la CRC para fortalecer los esfuerzos en materia de capacitación, prevención, respuesta oportuna y educación ciudadana frente al creciente fenómeno del fraude digital. En este sentido, se sugiere desarrollar de forma conjunta las acciones detalladas a continuación, orientadas a mitigar los delitos informáticos más frecuentes, tales como el hurto por medios informáticos, la violación de datos personales y la suplantación de sitios web. Entre las sugerencias para fortalecer la cooperación CRC – Policía Nacional en la lucha contra el fraude digital se identifican:

- Diseñar un programa conjunto de capacitación para operadores móviles y funcionarios públicos sobre los principales delitos informáticos, con base en los tipos penales más frecuentes (artículos 269 del Código Penal), sus características, modus operandi y medidas preventivas.
- Establecer un convenio institucional entre la CRC y la Policía Nacional, que permita: Compartir datos estadísticos y patrones de fraude digital, articular campañas de



**Alianza
Latinoamericana
de Telecomunicaciones**

prevención conjuntas y generar alertas tempranas de nuevos métodos delictivos que involucren el uso de servicios móviles.

- Crear un protocolo técnico y legal para que los operadores móviles puedan colaborar de forma ágil y segura con las autoridades en investigaciones penales, respetando la ley de habeas data y los derechos de los usuarios, pero permitiendo respuestas eficaces ante delitos como suplantación, hurto o transferencia no consentida de activos.
- Liderar, junto a la Policía, jornadas de alfabetización digital comunitaria, enfocadas en los delitos más comunes, entre los que se encuentran: Hurto por medios informáticos, violación de datos personales y suplantación de sitios web (phishing).

Estas acciones pueden implementarse prioritariamente en zonas con alta incidencia de delitos informáticos, mediante la coordinación entre autoridades locales y operadores móviles. Se sugiere, además, promover una línea de reporte unificada, como un número corto nacional o un botón integrado en aplicaciones móviles, que facilite a los ciudadanos informar intentos de fraude directamente a la Policía, con respaldo técnico por parte de los operadores y acompañamiento de la CRC. Asimismo, es recomendable que la CRC incorpore contenidos de prevención de fraude digital en sus programas de educación cívica digital, alineados con la clasificación legal de delitos informáticos y las directrices técnicas de las autoridades competentes.

Conclusiones

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

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



**Alianza
Latinoamericana
de Telecomunicaciones**

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

Agradezco su atención y ALT+ queda a su disposición para colaborar en el diseño de soluciones de política digital coherentes con los retos actuales de Colombia.

Atentamente,

A handwritten signature in dark ink, featuring a long horizontal stroke followed by a stylized, looped flourish.

José F. Otero
Director Ejecutivo
Alianza Latinoamericana de Telecomunicaciones
Tel: +1 202 766 5840