

Bogotá D.C., 28 de julio 2025

Señores

Comisión de Regulación de Comunicaciones (CRC)
Ciudad

Ref. Comentarios al Documento de Identificación del problema del proyecto Identificación de medidas regulatorias para mitigar el fraude cibernético por medio de servicios móviles.

El presente documento contiene los comentarios y recomendaciones al documento de Identificación del problema del proyecto 'Identificación de medidas regulatorias para mitigar el fraude cibernético por medio de servicios móviles' de conformidad con la publicación oficial y la invitación a la ciudadanía en general a participar en el proceso de consulta pública abierta por la CRC.

El proyecto que aborda una preocupación importante en el sector en los últimos años ha sido la proliferación de varias prácticas de fraude cibernético a través de los servicios de telecomunicaciones móviles. Lo cual ha afectado significativamente la confianza que los usuarios depositan en estos medios de comunicación digitales, generando considerables pérdidas en el mercado de esta industria y adicionalmente, ha comprometido la integridad y la privacidad de los usuarios.

Ante dicha problemática, resaltamos que la Comisión de Regulación de Comunicaciones incluyó en su Agenda Regulatoria 2025-2026 el proyecto denominado "Identificación de medidas regulatorias para mitigar el fraude cibernético por medio de servicios móviles", con el objetivo de analizar en detalle la situación, identificar y evaluar posibles medidas regulatorias y no regulatorias que permitan fortalecer la trazabilidad y el control sobre las comunicaciones que utilizan recursos de identificación en los servicios móviles, procurando que dichas medidas no afecten la innovación ni restrinjan el acceso de los actores legítimos al mercado, y contribuyendo así a consolidar un entorno de telecomunicaciones más seguro y confiable para todos los usuarios.

Fruto de los avances del proyecto, el pasado 4 de julio se publicó para comentarios el documento de formulación del problema y dentro del marco

de esta convocatoria, se llevó a cabo el foro “Identificación de medidas para mitigar fraude cibernético por medio de servicios móviles” en las instalaciones de la Universidad Externado de Colombia donde se dio espacio de socialización y conversación con los asistentes del evento, en el que estos compartieron sus apreciaciones sobre esta iniciativa.

No obstante que de los comentarios realizados en el foro se tomó nota directamente por la CRC, desde el Departamento de Derecho, Comunicaciones y Tecnologías de la Información de la Universidad Externado de Colombia, nos permitimos poner a su consideración los comentarios adicionales sobre el documento de formulación del problema del proyecto de referencia.

De acuerdo con la metodología de la consulta publicada por la CRC y el modelo de orientación a través de las preguntas formuladas, se procederá a dar respuesta a cada una de las preguntas propuestas, para finalmente, dar unas conclusiones generales.

I. Sobre el problema planteado:

a) ¿Por qué considera que el problema definido en este documento involucra todos los elementos que evidencian las dificultades generadas por la comisión de fraude cibernético mediante la provisión de los servicios tradicionales de llamadas de voz y SMS?

Dado el caso que considere que el problema definido no involucra todos los elementos necesarios, por favor justifique sus motivos, aporte evidencia al respecto y proponga un problema alternativo con sus respectivas causas y consecuencias.

R: Consideramos que el problema "Ausencia de herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto", tal como está formulado, efectivamente incorpora de manera pertinente los elementos relativos a las causas (por ejemplo, dificultad en la identificación y rastreo de ataques cibernéticos y ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto) y las consecuencias (como la pérdida de confianza de los usuarios y aumento de los casos de uso indebido de códigos cortos con fines fraudulentos). Estos elementos, en efecto permiten evidenciar las dificultades generadas por la

comisión de estos fraudes cibernéticos y abarcan los aspectos suficientes para un análisis completo que lleve a la formulación del problema cómo efectivamente se hizo.

b) Frente al problema planteado, ¿por qué considera que las causas presentadas en este documento son las que generan el problema definido?

En caso de considerar lo contrario, por favor indicar las razones por las cuales no está de acuerdo con la relación que se establece entre tales causas y el problema definido, y proponga las causas que considere pertinentes.

Encontramos que las causas identificadas en el documento son: enfoque limitado de las medidas técnicas y regulatorias sobre administración de recursos de identificación; insuficiencia de las medidas de gestión y control implementadas por los PRST y asignatarios; Dificultad en la identificación y rastreo de ataques cibernéticos; Desconocimiento de los usuarios sobre privacidad de la información facilita la obtención de datos personales con fines fraudulentos; Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto

Consideramos que las causas presentadas, son algunas de las que efectivamente generan el problema, no obstante, para ampliar la mirada, sería importante tener en cuenta otros puntos que también contribuyen a esta problemática, como los siguientes:

- Falta de interoperabilidad y estandarización de medidas de prevención entre operadores

Si bien una de las causas propuestas es la insuficiencia de las medidas implementadas por los PRST (Proveedor de Redes y Servicios de Telecomunicaciones) y los asignatarios, dichas medidas no sólo son insuficientes, sino que en la práctica se ve que cada operador puede tener controles internos para bloquear o detectar llamadas y SMS fraudulentos distintos, pero no existe un protocolo único, obligatorio y sectorial que los obligue a compartir en tiempo real información de amenazas o listas negras y gracias a esto, los defraudadores pueden aprovechar las diferencias, por ejemplo, si un operador bloquea un rango de números fraudulentos, esos mismos números pueden seguir operando en otra red que no los bloquee. Sin medidas coordinadas, el control es parcial y el fraude persiste.

Lo anterior se fundamenta en que de acuerdo con lo analizado en el estudio, *“solo el 34.9% de las empresas encuestadas reportó contar con procedimientos para el intercambio de alertas de fraude con PRST u otras entidades. Además, se encontró una alta heterogeneidad en las prácticas de los operadores, lo que “dificulta la detección temprana de patrones de fraude y limita la capacidad de respuesta coordinada ante incidentes”¹.*

Así pues, es importante que la causa en cuestión no sea sólo que las medidas son insuficientes sino que no hay una estandarización e interoperabilidad de estas, por lo cual, la causa en cuestión podría complementarse o agregarse de manera independiente al análisis.

- Limitada cooperación internacional y dificultad para perseguir responsables.

Teniendo en cuenta que muchos fraudes provienen de números extranjeros o de redes internacionales y que en el foro del pasado 24 de julio y en el documento de identificación del problema², se puso de manifiesto por entidades como la Fiscalía General de la Nación, la Policía Nacional y el ColCERT, las autoridades colombianas no siempre pueden pedir información o actuar sobre operadores en otros países. Lo anterior, evidencia que hace falta una coordinación internacional que permita una mayor efectividad en la persecución de los responsables, ya que el fraude cibernético es por definición transnacional. Y sin acuerdos o mecanismos ágiles de cooperación internacional, identificar a los responsables reales y cortar el fraude desde la fuente es casi imposible.

Como conclusión de esto, sería importante incluir esta situación como causa del problema, con miras a construir una mayor cooperación internacional que permita contar con medidas eficaces de persecución pues si bien en la exposición del documento se reconocen estas problemáticas, las mismas no se incluyeron directamente en las causas relacionadas previamente.

¹ Véase pág. 44 del documento.

² Véase nota de pie de página número 62 del documento, se señala que estas dificultades fueron puestas de presente en la mesa de trabajo llevada a cabo el 12 de febrero de 2025, en las instalaciones del MinTIC, en la que participaron la CRC, el ColCERT, el Cuerpo Técnico de Investigación (CTI) y el grupo de delitos informáticos de la Fiscalía General de la Nación y la Dirección de Investigación Criminal e Interpol (DIJIN) de la Policía Nacional.

c) Frente al problema planteado, ¿por qué considera que las consecuencias expuestas en el presente documento tienen relación directa con la materialización del problema?

(En caso de considerar lo contrario, indicar las razones por las cuales no está de acuerdo con la relación que se establece entre el problema definido y las consecuencias descritas, y proponga las consecuencias que considere pertinentes.)

Consecuencias identificadas: Pérdida de confianza en los servicios de telecomunicaciones, Afectaciones a empresas y organismos públicos, Transgresión de los derechos de los usuarios de los servicios de telecomunicaciones, **aumento de los casos de uso indebido de códigos cortos con fines fraudulentos.**

Consideramos que las consecuencias descritas en el documento que son la pérdida de confianza en los servicios de telecomunicaciones, las afectaciones a empresas y organismos públicos, la transgresión de los derechos de los usuarios y el aumento de casos de uso indebido de códigos cortos con fines fraudulentos están debidamente relacionadas con la materialización del problema identificado, pues reflejan impactos directos tanto en el funcionamiento del sector como en la experiencia y confianza de los usuarios.

No obstante, estimamos pertinente incluir, como consecuencia adicional, la afectación de la reputación del país como destino digital. Esta consecuencia, aunque indirecta, resulta relevante porque la persistencia de prácticas de fraude cibernético no controladas puede generar percepciones negativas en inversionistas, empresas tecnológicas y plataformas internacionales, afectando el posicionamiento del país como un entorno seguro y confiable para el desarrollo de servicios digitales e innovaciones basadas en telecomunicaciones móviles. Esta consecuencia podría ser parte de la primera mencionada en el documento, no obstante, debe aclararse que se puede dar esa desconfianza no sólo por parte de los usuarios de los servicios sino también en extranjeros respecto a lo que ofrece el país ante una posible inversión local.

Incluir esta dimensión contribuiría a una caracterización más completa del problema, evidenciando que sus impactos trascienden el ámbito estrictamente económico o individual de los usuarios, y pueden incidir en la competitividad y proyección internacional del ecosistema digital colombiano.

II. Respetto de los grupos de valor

a) ¿Por qué considera que existen otros grupos de valor que deben tenerse en cuenta en el desarrollo del presente proyecto regulatorio?

Por favor indíquelos, justificando la razón que tendría para incluirlos. En caso de considerar que se encuentran incluidos todos los grupos de valor, justifique también su respuesta.

Aunque el documento menciona usuarios, operadores y reguladores, podría incluirse a: Las plataformas tecnológicas integradoras (proveedores de soluciones SMS/ USSD); empresas de ciberseguridad que pueden ofrecer herramientas de detección y respuesta ante fraudes; organismos judiciales y de control; por último, la academia y sociedad civil.

III. Sobre posibles alternativas de solución a la problemática identificada

a) En relación con el uso indebido de la numeración de códigos cortos:

a.1. ¿Cuáles beneficios o desafíos cree que podría tener la implementación de un registro de remitentes de mensajes cortos de texto, que haga uso de códigos alfanuméricos para su identificación por parte de los usuarios, así como de la identificación de la campaña de comercialización o publicidad que se va a adelantar por parte del remitente?

Beneficios: mejora la identificación del remitente por parte del usuario, disminuye la posibilidad de suplantación y facilita trazabilidad regulatoria.

Desafíos: implementación técnica para todos los operadores y posible impacto en plataformas pequeñas que no puedan adoptar alfanuméricos.

a.2. ¿Cómo valora la creación de un registro de remitentes que utilice tanto numeración de códigos cortos como numeración no geográfica de servicios (Numeración E.164 del NDC 940), teniendo en cuenta la actualización de las categorías de atribución como requisito para su asignación? ¿Considera viable esta alternativa? ¿Qué pros y contras podría identificar?

Pro: Aumenta la capacidad numérica, mejora categorización por tipo de servicio.

Contra: Posible confusión en usuarios y requiere fuerte campaña de pedagogía y control.

a.3. ¿Qué efectos cree que tendría una medida regulatoria que prohíba la inclusión de enlaces o URL de cualquier tipo en el contenido de los mensajes cortos de texto? ¿Esta restricción podría mitigar riesgos de fraude? ¿Qué efectos tendría sobre el mercado de envío de SMS?

Algunos efectos positivos, pueden ser que reduce riesgo de phishing y fraudes instantáneos. Por otro lado, los efectos negativos: afecta servicios legítimos que usan URLs seguras y pueden incentivarse uso de canales no regulados.

a.4. ¿Qué implicaciones considera que tendría la prohibición de la intermediación o reventa del uso de numeración de códigos cortos por parte de los asignatarios, estableciendo la identificación exclusiva de remitentes de mensajes de texto (SMS) a través de un único código corto atribuido a una modalidad y rango numérico exclusivo? Es decir, un código corto como canal dedicado de comunicación entre un originador de mensajes de texto y sus destinatarios, atribuido en la modalidad de servicios financieros. Ejemplo: código corto: 86000; modalidad: servicios financieros; uso: para uso exclusivo por parte de la entidad financiera: Banco X

Implica entonces que aumenta la trazabilidad y responsabilidad directa, al tiempo en que mejora el control sobre el remitente de la información.

¿Considera que la cantidad disponible de numeración de códigos cortos sería suficiente para atender la demanda de estos servicios, o sería necesario migrar a otro tipo de numeración con mayor disponibilidad de números?

La disponibilidad numérica puede agotarse rápidamente, por lo cual sería una expansión de la numeración disponible o migración parcial a E.164 no geográfica.

a.5. ¿Qué beneficios o desafíos considera que podría tener la migración del uso de la numeración de códigos cortos a numeración E.164 no geográfica de servicios atribuida en el NDC

940 para acceder a contenidos y aplicaciones soportados en SMS y USSD, con reglas estrictas sobre exclusividad de uso y prohibición de compartición o tercerización del recurso?

Beneficios: Mayor disponibilidad numérica; mejores controles por categoría y Facilidad de seguimiento por parte de reguladores

Desafíos: Alta inversión en cambios técnicos; coordinación regional e internacional para compatibilidad, y Riesgo de disrupción a servicios ya operativos.

a.6. Por favor describa de manera detallada cualquier otra alternativa regulatoria que considere podría contribuir a prevenir el uso indebido de la numeración de códigos cortos y el contacto a usuarios con fines presuntamente fraudulentos mediante el envío de mensajes cortos de texto.

Implementar un sistema nacional de alertas sobre campañas activas de fraude, con colaboración entre operadores, regulador y policía cibernética.

Incentivar el uso de protocolos de autenticación (ej. STIR/SHAKEN) para llamadas de voz. Campañas masivas de educación digital ciudadana, para enseñar a detectar y reportar fraudes.

b) Respecto del uso inadecuado de la numeración E.164:

b.1. ¿Qué beneficios y retos identifica en la implementación de un registro de originadores de llamadas comerciales y publicitarias, que permita su identificación por parte del usuario final mediante códigos alfanuméricos, y que se complemente con medidas como el uso exclusivo de rangos de numeración dedicadas, bloqueo de numeración no válida o extranjera sospechosa y el registro de campañas que se van a realizar por medio de llamadas de voz?

La adopción de técnicas de filtrado automatizado o screening es una estrategia altamente recomendable y necesaria para mitigar el contacto fraudulento con usuarios. Estas tecnologías, basadas en aprendizaje automático o reglas predefinidas, permiten identificar patrones de tráfico anómalos (como mensajes masivos con links maliciosos o llamadas de suplantación) y detener su propagación en tiempo real.

No obstante, este tipo de soluciones debe ir acompañada de medidas regulatorias, particularmente sobre:

- ✓ El uso, cesión o alquiler de numeración sin trazabilidad.

- ✓ La responsabilidad solidaria de quien facilita el uso de recursos numéricos a terceros.
- ✓ Reglas sobre frecuencia de envíos y validación de campañas autorizadas

b.2. ¿Qué percepción tiene sobre la adopción de técnicas tecnológicas de filtrado (screening) para identificar y bloquear llamadas o mensajes sospechosos? ¿Considera que esta medida debe ser complementada con acciones regulatorias sobre el uso de numeración?

Una alternativa adicional útil sería la creación de un sistema obligatorio de "verificación de identidad del originador de la llamada" (call validation system) para numeración E.164. Esto incluiría:

- ✓ Validación previa del uso del número por parte del operador.
- ✓ Registro unificado de uso autorizado de numeración por tipo de campaña o servicio.
- ✓ Protocolos tipo STIR/SHAKEN, adaptados al entorno colombiano.
- ✓ Estas medidas permitirían frenar el uso fraudulento de números válidos y mejorar la trazabilidad en casos de fraude.

c) En relación con el desconocimiento de los usuarios sobre privacidad de la información técnicas de ingeniería social:

c.1. ¿Cuál es su opinión sobre establecer obligaciones de divulgación pedagógica y de prevención en cabeza de los operadores móviles, PCA e integradores tecnológicos, complementadas con un portal de la CRC con información sobre remitentes denunciados?

Establecer obligaciones de divulgación pedagógica es altamente recomendable. Los operadores y PCA (Proveedores de Contenidos y Aplicaciones) están en una posición privilegiada para educar al usuario desde el primer contacto con el servicio. Una medida conjunta con la CRC, como un portal actualizado de remitentes y campañas denunciadas, aumentaría la capacidad de defensa del usuario frente a engaños.

c.2. ¿Qué efectos cree que tendría la creación de un portal que incluya una lista negra con los recursos de identificación más denunciados ante la CRC, e identificados de oficio por esta autoridad, que sean utilizados para contactar usuarios con fines presuntamente fraudulentos?

Una lista negra pública y actualizada de números y remitentes sospechosos o denunciados, administrada por la CRC, tendría un efecto disuasivo y permitiría a los usuarios filtrar o reportar más eficientemente. No obstante, requeriría:

- ✓ Procesos de verificación para evitar falsos positivos.
- ✓ Reglas claras de exclusión o rectificación de números.

c.3. ¿Cómo valoraría la creación de un sistema intersectorial de trazabilidad de recursos de identificación, administrado por la CRC, que centralice las PQRDs presentadas por los usuarios y se complemente con campañas educativas conjuntas?

Un sistema intersectorial de trazabilidad de recursos de identificación sería una medida robusta. Centralizaría las PQRD (Peticiones, Quejas, Reclamos y Denuncias), conectaría operadores, CRC y autoridades judiciales, y permitiría:

- ✓ Analítica de datos en tiempo real para detectar patrones de fraude.
- ✓ Rápida suspensión del recurso numérico comprometido.
- ✓ Coordinación para sancionar prácticas reincidentes.
- ✓ Debería incluir herramientas para que el usuario reciba retroalimentación y actualizaciones sobre su reporte.

c.4. Por favor describa de manera detallada cualquier otra alternativa que considere útil para aumentar el conocimiento y empoderamiento de los usuarios frente a los riesgos del fraude cibernético por medio de servicios móviles.

La implementación de una campaña nacional de alfabetización digital en seguridad móvil, bajo tres frentes:

- ✓ Contenido audiovisual simplificado sobre fraudes comunes y buenas prácticas.
- ✓ Inclusión de material obligatorio en procesos de contratación de servicios móviles.
- ✓ Iniciativas en colegios y universidades sobre “ciudadanía digital segura”.

d) Sobre la revisión integral del Régimen de Recursos de Identificación

d.1. ¿tiene alguna propuesta o recomendación para optimizar los procedimientos de asignación y recuperación de los recursos de identificación?

Las propuestas que proponemos para optimizar los procedimientos de asignación y recuperación de los recursos de identificación son la Digitalización y automatización del sistema de asignación y recuperación, con trazabilidad desde la solicitud hasta el uso final; el Establecimiento de plazos máximos de respuesta y obligación de reportar cambios de uso del número asignado; la aplicación de un modelo de categorización inteligente que limite el uso de ciertos rangos numéricos a sectores como salud, finanzas, seguridad; la inclusión de criterios de historial de cumplimiento como condición para nuevas asignaciones y por último, auditorías periódicas para verificar el uso legítimo de los recursos numéricos entregados.

I. CONCLUSIONES

La confianza del usuario es el activo más valioso en los servicios móviles. Cada llamada engañosa, cada mensaje fraudulento, mina la relación de confianza entre las personas y sus operadores. Los servicios móviles deben volver a ser un entorno seguro, confiable y transparente. La regulación y la tecnología deben trabajar al servicio de esa confianza.

En ese sentido, no hay solución mágica: se necesita un enfoque múltiple y colaborativo. La complejidad del fraude cibernético exige acciones coordinadas entre operadores, reguladores, proveedores de tecnología, autoridades judiciales y los propios usuarios. Solo un esfuerzo colectivo, sostenido en el tiempo, podrá hacer frente a estas amenazas de forma efectiva.

El usuario no puede seguir siendo el eslabón más débil. Muchas víctimas caen en fraudes por falta de información o educación digital básica. La regulación debe reconocer esto y promover mecanismos pedagógicos obligatorios y accesibles, que acompañen al usuario desde su primer contacto con los servicios móviles.

La numeración es poder: hay que protegerla como un bien público. El uso indebido de códigos cortos, numeración E.164 o recursos sin trazabilidad permite que los delincuentes operen con impunidad. Es fundamental una

gestión ética, transparente y responsable de estos recursos, reconociendo su impacto directo en la seguridad digital.

Por tanto, la tecnología puede ser aliada si se usa con responsabilidad. Herramientas de filtrado inteligente, identificación alfanumérica, trazabilidad automatizada o portales de denuncia pueden empoderar al usuario y anticipar fraudes. Pero su éxito depende de una implementación técnica rigurosa y una supervisión regulatoria comprometida.

Regulación no es sinónimo de rigidez, sino de oportunidad para evolucionar. El ecosistema digital cambia cada día. La regulación debe ser dinámica, basada en datos, y abierta a la innovación, sin perder de vista su objetivo superior: proteger los derechos de las personas y garantizar un entorno digital sano.

Cordialmente,

Departamento de Derecho, Comunicaciones y Tecnologías de la Información

Facultad de Derecho – Universidad Externado de Colombia