

CONSULTA PÚBLICA

Proyecto regulatorio denominado Identificación de Medidas para Mitigar el Fraude Cibernético por Medio de Servicios Móviles.

CONTEXTO

La CRC, como autoridad regulatoria convergente del sector de las Tecnologías de la Información y las Comunicaciones (TIC), se encuentra facultada para, por un lado, expedir el régimen regulatorio para la maximización del bienestar social de los usuarios de los servicios de comunicaciones (en adelante, "*los usuarios*"; y por el otro, como ya se indicó, regular y administrar todos los recursos de identificación en Colombia, con excepción del nombre de dominio ".co" y la concesión y supervisión sobre el espectro electromagnético, entre otras funciones.

La CRC presentó un proyecto regulatorio para mitigar el fraude cibernético en servicios móviles, enfocándose en el uso indebido de recursos de identificación como llamadas y SMS, los cuales han sido explotados en modalidades de fraude como *smishing* y *vishing*. En el documento se hace un diagnóstico de las problemáticas para evaluar medidas regulatorias y fomentar la coordinación intersectorial.

Problema central:

Según el documento de la CRC el problema central es la ausencia de herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto.

Con el objetivo de orientar esta consulta, se solicitó a los agentes interesados, a más tardar el **28 de julio de 2025**, contestar las siguientes preguntas mediante el formulario de Forms que se encuentra en el siguiente enlace <https://forms.office.com/r/f0Qu3f3gHW> o mediante el correo electrónico medidasantifraude@crcom.gov.co:

PREGUNTAS

1. 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.**

La Superintendencia Financiera de Colombia (SFC), como autoridad encargada de la inspección, vigilancia y control del sistema financiero, bursátil y asegurador, considera que en efecto, "*la ausencia de herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios*

tradicionales de voz y mensajes de texto” definido por la CRC, permite el uso fraudulento de números telefónicos y códigos cortos para suplantar entidades legítimas, dado que no se cuenta con los mecanismos que faciliten a los usuarios verificar la autenticidad del remitente, lo que conlleva a la materialización de fraudes cibernéticos, bajo las modalidades del *vishing* y el *smishing*.

No obstante, para una respuesta integral desde la perspectiva de protección al consumidor financiero, se recomienda ampliar el enfoque incorporando los siguientes elementos a la definición del problema:

- Articulación efectiva entre operadores de servicios de telefonía móvil, entidades financieras, proveedores tecnológicos, Policía Nacional, los establecimientos de comercio y autoridades regulatorias para prevenir, mitigar y responder a estos fraudes de forma integral.
- Comunicación y protocolos conjuntos dirigidos a compartir alertas tempranas y reaccionar de manera sincronizada ante amenazas emergentes.
- Implementación de una herramienta única, digital, interoperable y de fácil acceso para que los usuarios reporten números telefónicos y códigos cortos desde los que se realicen intentos de fraude y se facilite la reacción de las entidades financieras, operadores móviles, proveedores tecnológicos, Policía Nacional y demás actores que puedan intervenir para la gestión efectiva de estos fraudes.

Ahora bien, proponemos el siguiente problema alternativo con sus respectivas causas y consecuencias:

Problema alternativo: Falta de herramientas regulatorias y de educación financiera, deficiencia en la articulación, canales y protocolos de comunicación entre los diferentes actores y ausencia de una herramienta única, digital, interoperable y de fácil acceso para los ciudadanos y entidades, que permitan prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto.

Causas que eventualmente se derivan en el problema alternativo propuesto:

- Vacíos regulatorios en la gestión y trazabilidad de numeración y autenticación de remitentes.
- Falta de integración de los actores y de sistemas de denuncia y trazabilidad de incidentes.
- Ausencia de campañas masivas y permanentes de educación para la protección de la información personal y prevención del fraude.
- Latencia en la respuesta judicial frente a delitos informáticos.

Consecuencias:

- Aumento del número de víctimas de fraude financiero.
- Pérdida de confianza en los canales digitales y los servicios móviles.

- Riesgo sistémico para la estabilidad del ecosistema financiero digital.

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.

La Superintendencia considera que las causas presentadas en el documento de la CRC guardan relación con el problema planteado y se alinean con los principales factores que han permitido la proliferación del fraude cibernético mediante servicios tradicionales como llamadas de voz y mensajes SMS; en particular, aquellas que inciden directamente sobre los usuarios del sistema financiero como:

- **Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso.** Coincidimos en la necesidad de que se establezcan reglas específicas a través de un marco regulatorio que permita mitigar el fraude, en modalidades tales como la suplantación de identidad o el uso indebido de la numeración, máxime cuando en la actualidad se evidencia un incremento en las operaciones digitales del sistema financiero colombiano, que cursan a través de Banca móvil.

Esas medidas regulatorias no contemplan elementos como la seguridad y trazabilidad de la numeración como aspectos relevantes para salvaguardar los intereses del consumidor financiero y responder de manera efectiva.

La ausencia de mecanismos robustos para validar la identidad del remitente y monitorear el uso indebido de la numeración deja al consumidor expuesto a esquemas de suplantación altamente sofisticados.

- **Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes.** La SFC comparte la opinión en torno a las medidas de control preventivas que deben ser adoptadas por los Proveedores de Redes y Servicios de Telecomunicaciones y los asignatarios de los recursos de identificación, con el propósito de mitigar la materialización de ventos asociados al fraude. Asimismo, es necesario el fortalecimiento de los procedimientos de monitoreo y de intercambio de alertas con proveedores de redes y servicios de telecomunicaciones móviles, para ayudar a contrarrestar los eventos de fraude bajo modalidades tales como *smishing* y *vishing*.

La SFC considera clave fortalecer los esquemas de coordinación entre entidades financieras, operadores de telecomunicaciones, autoridades judiciales, reguladores, comercios y demás actores, con el fin de

consolidar capacidades conjuntas de monitoreo, detección, prevención y respuesta frente al fraude cibernético.

Sin duda, estas dificultades en la identificación y rastreo de responsables dificultan las investigaciones que deben realizar las autoridades respectivas, por la falta de articulación de medidas técnicas y operativas que permitan generar una trazabilidad de toda la cadena de comunicación, así como a la ausencia de sistemas integrados de prevención y alerta temprana, lo cual impide una respuesta coordinada frente a estos delitos y debilita la capacidad institucional para proteger a los usuarios finales.

- **Desconocimiento de los usuarios sobre la privacidad de su información.** Se considera necesario fortalecer los esfuerzos de educación y sensibilización dirigidos al público en general, en materia de habeas data y seguridad de la información, y con ello exigir el cumplimiento de sus derechos como titulares de la información y de las obligaciones de los responsables y encargados de la información, y así mitigar el riesgo de fraude que se genera para los usuarios de servicios de telecomunicaciones móviles. De otra parte, estamos de acuerdo con lo planteado en el documento de la CRC, en cuanto a que un usuario no tiene cómo identificar los intentos de suplantación o solicitudes de datos engañosas, es decir, muchas personas no cuentan con la posibilidad de distinguir cuáles acciones estarían por fuera del marco de las obligaciones de los responsables de custodiar la información sujeta de protección.

En efecto, el bajo nivel de conocimiento del ciudadano sobre el tratamiento y protección de sus datos personales agrava el problema, al dificultar la identificación de intentos de fraude o suplantación.

Por eso, para garantizar la protección efectiva del consumidor financiero es indispensable avanzar hacia un esquema integral de prevención que combine un marco regulatorio orientado a la seguridad, medidas técnicas de monitoreo, programas de educación constante al usuario y canales idóneos de denuncia e intervención coordinada entre actores públicos y privados.

- **Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto.** Coincidimos con la CRC, en que es indispensable establecer protocolos de colaboración entre las autoridades, el sector privado, la sociedad civil y los operadores de telecomunicaciones, con el fin de generar estrategias, políticas, procedimientos y acciones, que permitan mitigar el fraude digital y la ingeniería social, que afectan a los usuarios en general.

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.

La SFC considera que las consecuencias expuestas en el documento guardan relación directa con la materialización del problema, teniendo en cuenta, que:

- La pérdida de confianza en los servicios de telecomunicaciones afecta a la confianza de los consumidores financieros en el canal banca móvil, cuyo instrumento generalmente es el celular. Lo anterior tiene la potencialidad de afectar la inclusión financiera y limitar el acceso a productos y/o servicios digitales seguros.
- La trasgresión de los derechos de los usuarios puede generar pérdida económica para el consumidor financiero por engaños que derivan en fraudes transaccionales en productos digitales. La inducción al error mediante el uso fraudulento de códigos cortos y numeración telefónica no solo pone en riesgo los recursos de los consumidores, sino que también incrementa los niveles de desinformación y desprotección, profundizando la asimetría entre los actores defraudadores y los usuarios.
- Afectaciones a empresas y organismos públicos, incremento en los costos operativos y reputacionales para las entidades vigiladas, por la atención de reclamos y la gestión de incidentes de fraude.
- El aumento en el uso indebido de códigos cortos con fines fraudulentos facilita la ejecución de fraudes como el *smishing* y el *vishing*, al inducir al usuario a entregar información sensible o realizar acciones que comprometen la seguridad de sus productos financieros.

2. 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.

Se sugiere incluir dentro del grupo de entidades gremiales a la Asociación Bancaria y de Entidades Financieras de Colombia – Asobancaria, así como a Fasecolda, Asofiduciarias, Asofondos y Asobolsa, que pueden aportar elementos técnicos, operativos y estratégicos para el desarrollo del proyecto regulatorio.

Adicionalmente, se recomienda incorporar a la Fiscalía General de la Nación, así como a la academia.

Además, pueden involucrarse los siguientes grupos que pueden aportar evidencia técnica, operativa y legal para diseñar soluciones más robustas:

- Empresas de ciberseguridad que aportan capacidades tecnológicas para detección temprana.
- Consumidores y asociaciones de usuarios: fuente clave para entender patrones de victimización.
- Establecimientos de comercio: sus intereses son relevantes para el entendimiento de las dificultades o retos que afrontan debido a este tipo de fraudes.

3. 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?

Se considera que la implementación de un registro de remitentes que utilice códigos alfanuméricos identificables y permita asociar cada mensaje a una campaña específica representa una medida positiva y necesaria que podría mitigar riesgos de fraude cibernético.

Además, representa un avance significativo en términos de seguridad, transparencia y confianza en los canales digitales.

Beneficios:

- Permitiría a los usuarios identificar de forma clara al remitente y asociarlo a una entidad o campaña legítima, reduciendo así la probabilidad de caer en fraudes como el *smishing* y facilitando la toma de decisiones informadas.
- Facilitaría la creación de filtros y alertas automatizadas en las herramientas de monitoreo de las entidades vigiladas, para identificar emisores no autorizados.

Desafíos:

- Costos y capacidades de implementación en los sistemas de monitoreo, principalmente para pequeñas empresas con infraestructuras limitadas que se encuentran eventualmente más expuestas.
- La disponibilidad y actualización en línea de la información sobre campañas activas, para que pueda ser consultada oportunamente por las entidades financieras, frente a lo cual surgiría la necesidad de asegurar interoperabilidad técnica entre operadores y sistemas financieros.
- La definición e implementación de una estrategia clara de campañas de educación dirigidas al usuario.

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?

Se considera pertinente la creación de un registro de remitentes que integre tanto la numeración de códigos cortos como la numeración no geográfica E.164 del NDC 940.

La inclusión de este tipo de numeración permitiría la interoperabilidad con bases de datos internacionales o multisectoriales, dada la estandarización de la numeración E.164.

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?

La prohibición de incluir enlaces en mensajes de texto puede contribuir de manera significativa a mitigar riesgos de fraude, en particular aquellos relacionados con técnicas de *phishing*. La prohibición del uso de enlaces en SMS eliminaría uno de los mecanismos más utilizados por los delincuentes para inducir al error y obtener información sensible de los usuarios.

En cuanto al mercado de envío de SMS, la medida podría impactar modelos de negocio basados en campañas digitales y comunicaciones transaccionales, por lo que se sugiere condicionar el uso de enlaces exclusivamente a remitentes previamente validados y registrados ante una base centralizada, bajo controles de trazabilidad y autenticación.

Desde la perspectiva de protección al consumidor financiero, al eliminar una de las vías más frecuentes mediante las cuales los delincuentes engañan a los usuarios para sustraer su información personal o acceder a sus productos financieros podría considerarse acertado para la disminución de estos casos de fraude; sin embargo, impactaría negativamente el acceso de los ciudadanos a los diversos productos o servicios ofrecidos legítimamente por entidades vigiladas, como notificaciones transaccionales o validaciones de seguridad.

Por ello, más que una prohibición absoluta, se propone un enfoque regulatorio diferenciado: permitir el uso de enlaces únicamente a remitentes registrados y autenticados en una base centralizada, con mecanismos de trazabilidad robustos y verificación de dominios seguros. Esta alternativa equilibra la necesidad de protección del consumidor con la continuidad operativa de servicios financieros digitales esenciales.

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 ¿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 prohibición de la intermediación o reventa de códigos cortos y la asignación exclusiva de éstos a un originador podría traer beneficios importantes en términos de trazabilidad, transparencia y control sobre el envío de mensajes, lo cual es relevante para mitigar fraudes por suplantación y phishing.

Respecto a la cantidad disponible de numeración de códigos cortos, sería necesario realizar un análisis técnico de las proyecciones de demanda, teniendo en cuenta que las entidades vigiladas utilizan un número distinto para cada uno de los tipos de operaciones como, por ejemplo: de alertas, campañas publicitarias o de seguridad, disponibilidad de canales, entre otros. Además, estos números cortos son utilizados por otros sectores económicos no vigilados por la SFC por lo pueden llegar a ser insuficientes.

Desde el punto de vista del consumidor financiero, la asignación exclusiva de códigos cortos a entidades específicas mejora la seguridad y confianza del usuario al permitir identificar claramente al remitente, lo que podría reducir el riesgo de suplantación y fraude. No obstante, debe garantizarse suficiente disponibilidad de numeración para no afectar la comunicación oportuna de servicios financieros esenciales.

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?

La migración hacia la numeración E.164 no geográfica, atribuida en el NDC 940, puede generar importantes beneficios en términos de seguridad, trazabilidad y confianza del usuario, esta medida fortalecería la identificación del remitente, lo cual resulta fundamental para garantizar la confianza del usuario y mitigar riesgos asociados a la suplantación de marca y la intermediación no autorizada, al permitir un mayor control sobre el origen de los mensajes.

Uno de los beneficios más relevantes es la posibilidad de asignar un número único y verificable a cada remitente o campaña, lo que optimiza la identificación del emisor y reduce significativamente el riesgo de fraudes como el smishing.

No obstante, esta transición implica desafíos importantes; entre ellos, la necesidad de adecuaciones tecnológicas por parte de operadores y proveedores

y para su implementación deberá contar con el acompañamiento técnico y campañas de pedagogía para los usuarios como para los actores del ecosistema.

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

Desde la SFC se recomienda considerar las siguientes alternativas regulatorias:

- Establecer la obligación de realizar bloqueos automáticos de códigos cortos, soportado en análisis de comportamiento inusual. Este bloqueo debe ser respaldado por sistemas de análisis predictivo, garantizando así una protección preventiva y efectiva del usuario frente a contactos fraudulentos.
- Creación de un canal único de reporte en tiempo real, con la información de los remitentes y campañas registradas.
- Mecanismo de validación visible para el usuario (icono de confianza en el remitente).

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 implementación de un registro de originadores de llamadas comerciales y publicitarias, que incluya identificación alfanumérica, uso exclusivo de rangos de numeración dedicados, bloqueo de numeración sospechosa y registro obligatorio de campañas de voz, constituye una medida eficaz para mitigar el fraude mediante técnicas como el vishing. Esta estrategia fortalece la confianza del usuario, reduce la suplantación de entidades financieras y mejora la trazabilidad de eventos fraudulentos. No obstante, su implementación conlleva desafíos, como la necesidad de garantizar la interoperabilidad técnica con los operadores; por lo cual, se recomienda estudiar la mejor forma de ejecutarlo acompañada de una supervisión coordinada y de acciones de concientización dirigidas a los usuarios.

La implementación de este registro es una medida recomendable desde el punto de vista operativo y de protección al consumidor, ya que aumentaría la trazabilidad y la transparencia de las comunicaciones, mejora la capacidad del usuario para identificar comunicaciones legítimas, permite a las entidades financieras encontrar patrones de fraude y facilita acciones de bloqueo preventivo ante campañas irregulares o no registradas.

Desde el punto de vista del consumidor financiero, esta medida también empodera al usuario al brindarle herramientas claras para diferenciar llamadas legítimas de intentos de fraude, reduciendo la exposición a engaños telefónicos cada vez más sofisticados.

Al contar con una identificación alfanumérica visible y confiable, el usuario puede tomar decisiones más seguras sobre qué llamadas atender, especialmente en contextos sensibles como la gestión de productos financieros. Además, el registro previo de campañas de voz brinda mayor transparencia, ya que permite al consumidor conocer con anticipación los fines de la comunicación, reforzando su derecho a recibir información clara y veraz. Para garantizar su efectividad, esta medida debe ir acompañada de campañas educativas que sensibilicen al público sobre cómo interpretar esta nueva forma de identificación y qué hacer en caso de recibir llamadas de números no registrados o sospechosos.

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?

La adopción de técnicas de filtrado (*screening*) para identificar y bloquear llamadas o mensajes sospechosos sería una medida efectiva y necesaria para disminuir el fraude. Su implementación debería incluir medidas regulatorias que permitan proteger los intereses de los consumidores y garantizar la seguridad, en lo relacionado con el uso, asignación y trazabilidad de la numeración, para que los procesos de bloqueo no afecten comunicaciones legítimas.

Sin embargo, para que esta medida proteja eficazmente al usuario sin interferir con comunicaciones legítimas, debe estar respaldada por una regulación clara sobre el uso y asignación de numeración, así como por una estrecha coordinación entre operadores, entidades financieras y autoridades de control; lo anterior, con el propósito de que el filtrado sea preciso, transparente y enfocado en preservar la seguridad del consumidor sin afectar su acceso a servicios financieros confiables.

b.3. Por favor describa de manera detallada cualquier otra alternativa regulatoria que considere podría contribuir a prevenir el uso indebido de la numeración E.164 y el contacto usuarios con fines presuntamente fraudulentos mediante llamadas de voz.

La regulación debería considerar las siguientes acciones de prevención:

- Establecer la obligación de los operadores de telecomunicaciones de mantener registros actualizados sobre el uso de numeración E.164 no geográfica.
- Crear una base de datos centralizada de todos los operadores, administrada por la autoridad competente, que consolide esta información y pueda ser consultada por entidades autorizadas para fines de análisis, monitoreo, trazabilidad e investigación de incidentes.

- Definir sanciones para los operadores o proveedores que faciliten el uso indebido de numeración o que incumplan con sus obligaciones de verificación, trazabilidad y controles.
- Difusión obligatoria de campañas de concientización sobre fraudes telefónicos, coordinadas entre el regulador de telecomunicaciones, la autoridad financiera y los operadores.

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?

Esta medida es clave para la prevención del fraude, ya que contribuye a que los usuarios tengan el conocimiento de los riesgos asociados a las técnicas que usan los defraudadores mediante SMS y llamadas suplantadas; de tal forma que, se disminuyan los engaños por ingeniería social. De otra parte, se considera importante integrar campañas del sector financiero, con las implementadas por la CRC para que existan mensajes unificados dirigidos a los usuarios, cuya divulgación y actualización se deben realizar de manera permanente.

Por ello, es fundamental que las campañas pedagógicas incluyan mensajes claros y coordinados con las entidades financieras, alertando sobre los métodos más comunes de fraude y promoviendo buenas prácticas de seguridad digital. La articulación entre operadores, integradores tecnológicos, la CRC y el sector financiero y los establecimientos de comercio permitirá generar un ecosistema preventivo más robusto

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?

La creación de un portal público que contenga una lista negra de recursos de identificación (como números telefónicos, códigos cortos o remitentes alfanuméricos) denunciados por los usuarios o identificados por la CRC como presuntamente utilizados con fines fraudulentos, sería una herramienta altamente útil desde la perspectiva de la prevención del fraude, la protección al consumidor y la transparencia del ecosistema digital. Esta lista, siempre que su información haya sido previamente validada por la CRC para evitar falsas denuncias o bloqueos indebidos, permitiría a los usuarios verificar en tiempo real si una llamada o mensaje proviene de una numeración reportada como sospechosa, fortaleciendo así su capacidad para identificar intentos de fraude como el smishing y el vishing. Adicionalmente, funcionaría como un insumo estratégico para las entidades financieras, operadores móviles y autoridades como la Superintendencia Financiera, al facilitar la identificación de patrones de fraude y la adopción de medidas preventivas en sus canales de atención y comunicación con el usuario.

Adicionalmente, se considera que los números telefónicos, códigos cortos o remitentes alfanuméricos, registrados en la lista, deberían ser parte de las técnicas de filtrado (*screening*).

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

La creación de un sistema intersectorial administrado por la CRC sería una medida positiva, debido a que permitiría centralizar la gestión de las PQRD presentadas por los usuarios, evitando su duplicidad ante diferentes actores del ecosistema.

Además, un sistema unificado facilitaría la generación de estadísticas estandarizadas y la identificación de patrones comunes de afectación, lo que contribuiría a realizar análisis más precisos y oportunos, diferenciados según las competencias de cada entidad involucrada.

Dicho sistema también permitiría no solo una atención más eficiente y oportuna de las PQRD, sino también una mayor protección de los derechos de los usuarios frente a incidentes de fraude o uso indebido de su información.

Al centralizar la gestión de estas solicitudes, se evitaría la dispersión de responsabilidades y se garantizaría un seguimiento integral a cada caso, mejorando la transparencia y la confianza del consumidor en las entidades involucradas. Además, el tratamiento unificado de las PQRD facilitaría la adopción de medidas correctivas y preventivas en función de los patrones identificados, lo cual es fundamental para fortalecer la seguridad en los canales financieros digitales.

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.

Además de las campañas educativas tradicionales, se propone:

- Establecer una línea única o código corto para denunciar intentos de fraude por mensajes o llamadas, accesible desde cualquier operador.
- Que los operadores de telecomunicaciones diseñen campañas de prevención de fraude en los diferentes medios de comunicación que consideren el nivel de familiaridad digital del usuario, su edad, ubicación geográfica o servicios, de manera que los mensajes sean pertinentes y efectivos.
- Realizar foros para compartir a nivel regional las experiencias positivas y negativas en relación con las acciones y patrones de fraude.
- La inclusión obligatoria de módulos de educación financiera digital en los canales de atención y plataformas transaccionales.
- Notificar proactivamente a los consumidores financieros sobre campañas fraudulentas activas, mediante alertas visibles en sus aplicaciones, sitios

web y SMS oficiales, a efectos de recibir información clara, oportuna y suficiente para tomar decisiones seguras en el entorno digital.

d sobre revisión 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 Resoluciones CRT 2028 de 2008 y la 5050 de 2016 contempla lineamientos para la asignación y recuperación de recursos de identificación; en ese sentido, se formulan las siguientes recomendaciones:

- Si bien la Resolución 5050 contempla la publicación del estado de asignación a través del sistema SIGRI y exige justificar el uso del recurso al momento de su solicitud, se considera necesario complementar estas medidas con mecanismos de trazabilidad en tiempo real, que permitan verificar el uso efectivo y actual de los recursos, así como su historial de asignación y uso.
- Incorporar mecanismos automatizados de monitoreo que permitan identificar patrones de fraude (como volúmenes inusuales de envío de mensajes, horarios atípicos o uso de palabras clave sensibles), activar alertas y aplicar bloqueos preventivos ante potenciales riesgos de fraude.