Superintendencia de Industria y Comercio

Bogotá D.C.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RADICACION: 25-349777- -0-0 **FECHA**: 2025-07-23 14:57:27
DEPENDENCIA: 12 GRUPO DE TRABAJO DE REGULACIÓN **EVENTO:** SIN EVENTO
TRAMITE: 334 REMISIINFORMA **FOLIOS**: 7
ACTUACION: 425 REMISIONIFORMACI

Señores
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
medidasantifraude@crcom.gov.co
atencioncliente@crcom.gov.co

Asunto: Comentarios de la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** al Documento de formulación del problema denominado "*IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES*" (en adelante el "*documento*").

Respetados Señores:

Esta Superintendencia realiza un seguimiento permanente de los proyectos normativos que puedan incidir en las funciones que le han sigo asignadas[1]. En ese orden de ideas, y después de haber adelantado la revisión del documento referido en el asunto, considera necesario presentar los siguientes comentarios y recomendaciones:

1. Comentarios Generales

El documento relaciona los modos utilizados para realizar los fraudes de acuerdo con la "*Cartilla Metodológica de Atención de Delitos Informáticos*" de la **FISCALÍA GENERAL DE LA NACIÓN**. No obstante, desde la Delegatura para la Protección del Consumidor, se ha advertido que el denominado "*SIM swapping*", es una práctica que consistente en el bloqueo de la tarjeta SIM del usuario y la posterior solicitud de reposición sin autorización del titular. En algunas oportunidades, esta situación se presenta con una cesión previa de la línea a un tercero, y, en ocasiones tiende a ser facilitado por los operadores ante la ausencia de mecanismos de seguridad que permitan verificar la identidad del usuario.

Esta práctica facilita la realización de fraudes bancarios o la contratación de servicios no solicitados, accediendo a los códigos únicos de verificación que envían las Fintech, las aplicaciones móviles de las entidades bancarias o las billeteras digitales asociadas a la línea móvil.

En atención a lo anterior, y considerando el aumento progresivo de estas prácticas fraudulentas prácticas fraudulentas que afectan los derechos de los usuarios en múltiples dimensiones, se considera oportuno que la **COMISIÓN DE REGULACIÓN DE COMUNICACIONES** (en adelante **CRC**) adopte medidas respecto de esta modalidad denominada "*SIM swapping*", así como frente a las portabilidades fraudulentas realizadas mediante la utilización de la red móvil.

[1] Decreto 4886 de 2011 "[p]*or medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones*", y demás disposiciones concordantes.

2. Respuesta a la Consulta Pública

2.1. 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***".

El documento identifica adecuadamente la problemática desde la perspectiva técnica en materia de fraude cibernético. No obstante, es necesario que la formulación del problema incorpore de manera explícita **el impacto sobre los derechos de los usuarios de servicios de comunicaciones**. Esto, teniendo en cuenta que la "*ausencia de herramientas regulatorias*" puede ser una causa de la vulneración de estos derechos.

Si bien el problema planteado contempla en buena medida la mayoría de la casuística que derivan en una conducta delictiva relacionada con el fraude cibernético a través de servicios móviles, esta Superintendencia ha advertido que la modalidad conocida como "*SIM Swapping*" —o reposición fraudulenta de la tarjeta SIM— no se encuentra contemplada en la definición del problema planteado por la **CRC. Toda vez que, el problema definido se enfoca en las herramientas para prevenir y mitigar únicamente el contacto a usuarios con fines fraudulentos, excluyendo aquellos escenarios en los que se realizan fraudes cibernéticos por medio de servicios móviles sin que exista interacción con el titular de la línea móvil.**

De igual manera, para esta Superintendencia es importante resaltar que, hoy en día, la red móvil constituye un canal de acceso y autenticación de distintos servicios financieros vigilados o no por la **SUPERINTENDENCIA FINANCIERA DE COLOMBIA** (en adelante **SUPERFINANCIERA**), lo cual exige que las medidas técnicas y regulatorias que rigen el acceso a la red, así como a la información personal tratada por los operadores, deban ser mucho más exigentes con el fin de brindar una protección efectiva a los usuarios de los servicios móviles.

De conformidad con lo anterior, esta Superintendencia propone la siguiente formulación al problema:

"*Ausencia de herramientas regulatorias para prevenir y mitigar conductas con fines fraudulentos mediante la red móvil que afecten los servicios y los derechos de los usuarios*".

> "***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***".

Las causas identificadas por la **CRC** en su planteamiento son acertadas para la definición del problema toda vez que, efectivamente, las medidas regulatorias implementadas en materia de recursos de identificación han estado orientadas a garantizar el recurso escaso. Sin embargo, se ha dejado la autogestión y control de la plataforma y sus recursos a los "*Proveedores de Redes y Servicios de Telecomunicaciones* – **PRST**" y "*Proveedores de Contenidos y Aplicaciones* – **PCA**" e "*Integradores Tecnológicos* – **IT**" quienes, conforme el requerimiento general formulado por la **CRC**, no han adoptado medidas verdaderamente seguras para prevenir de manera efectiva las conductas fraudulentas.

Es importante indicar que las medidas que debían haber implementado los **PRST** no debían limitarse a prevenir el contacto fraudulento con los usuarios, sino también a evitar la obtención de servicios de manera fraudulenta por medio de la suplantación de identidad de sus usuarios o de violación de sus datos personales, conforme lo reconoce la **CRC** en el documento:

> "*Los ataques cibernéticos que afectan los servicios de telecomunicaciones como el SIM swapping, la suplantación de identidad, el uso de numeración falsificada o el acceso no autorizado a plataformas de gestión suelen ejecutarse de forma rápida y sofisticada, aprovechando brechas en los sistemas de autenticación y en la interoperabilidad entre operadores*[2]".

Adicionalmente, en el desarrollo de distintas mesas de trabajo, los **PRST**, **PCA** e **IT** han manifestado que ellos son tan solo prestadores de servicios de telecomunicaciones y que el fraude por medio de sus redes es ajeno a dicha prestación del servicio, desconociendo así, la importancia de proteger los datos personales de los usuarios y establecer medios efectivos para evitar la suplantación de identidad al acceder a sus servicios o a sus redes, como es el caso de la reposición fraudulenta de la tarjeta SIM.

Por último, es importante destacar que la "*Estrategia Nacional de Seguridad Digital*" es reciente y la presente actualización regulatoria que pretende realizar la **CRC** responde a uno de los puntos críticos identificados en el desarrollo de dicha política.

> ***"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".***

Desde el punto de vista de la protección de usuarios de los servicios de telecomunicaciones, la transgresión de sus derechos se está presentando tanto por el contacto a los usuarios con fines fraudulentos —tal y como lo indica la **CRC** en el documento— así como mediante conductas fraudulentas que se ejecutan por medio de servicios móviles sin que exista contacto con el usuario.

---

[2] **COMISIÓN DE REGULACIÓN DE COMUNICACIONES** (julio 2025) "*Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles*". Documento de formulación del problema. Pág. 44.

Para esta Superintendencia, es de vital importancia reiterar que hoy en día las redes y servicios móviles se usan para el acceso a diferentes servicios, —incluidos los **financieros**, hoteleros y de diversas categorías—, lo cual impone un deber adicional a los prestadores de servicios móviles de proteger los derechos y los datos personales de los usuarios de utilizan sus redes.

La ausencia de medidas regulatorias, así como la falta de mecanismos eficaces de autocontrol y gestión contribuye al debilitamiento de la confianza de los usuarios en los servicios de telecomunicaciones, especialmente para los servicios móviles. Esto puede derivar en que los usuarios eviten —en los casos que es posible— el uso de las redes móviles para realizar sus principales transacciones.

En un ecosistema digital, la confianza en las redes de telecomunicaciones, así como en los medios electrónicos es fundamental y, como lo identificó la **CRC**, la falta de prevención y mitigación de conductas fraudulentas por medio de los servicios móviles lleva a un estancamiento de la evolución de dicho ecosistema.

2.2. Respecto 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".***

Si bien la **CRC** precisa en el documento de formulación de problema que "*es consciente de que esta problemática desborda su marco competencial y reconoce, como lo han hecho otros reguladores en el mundo, que exige la coordinación y definición de una estrategia conjunta, intersectorial y que, incluso, involucre a actores del sector privado*"[3], se sugiere que desde el inicio del proyecto, se involucre a todos aquellos actores vinculados al CONPES 3995 de 2020 "*Política Nacional de Confianza y Seguridad Digital*" y a la "*Estrategia Nacional de Seguridad Digital 2025 -2027*".

Asimismo, se recomienda incluir en los grupos de valor a "*Entidades del sector financiero*" como las **FINTECH**, entendidas estas como empresas que buscan innovar en el sector financiero a través de soluciones digitales, prestan servicios financieros a usuarios finales y que su principal medio de comunicación con los usuarios son los servicios móviles de telecomunicaciones, aun cuando, en muchos casos, no son entidades vigiladas por la **SUPERFINANCIERA**.

De igual forma, se considera pertinente valorar la inclusión de las **agremiaciones del sector financiero** en los grupos de valor, en función de su representatividad y el rol que desempeñan en la articulación de prácticas y estándares dentro del ecosistema financiero.

2.3. Sobre posibles alternativas de solución a la problemática identificada:

[3] Ibidem. Página 5.

Frente a las posibles alternativas de solución a la problemática planteada, esta Superintendencia realizará los comentarios de manera general.

En primer lugar, frente al uso indebido de la numeración de códigos cortos es importante que los **PCA** y los **IT** cumplan con la normativa vigente aplicable a los **PRST**, particularmente en lo relativo a la verificación y contenido (remitente, información) de los SMS comerciales y publicitarios.

Por otra parte, la propuesta de establecer un registro de remitentes, desde el punto de vista técnico puede ser una herramienta eficaz para disponer de la información de los diferentes actores que remitan los SMS. De acuerdo con lo identificado por la **CRC** en la revisión de experiencias internacionales el "*Registro de Identificación (ID) de Remitentes: Las organizaciones legítimamente constituidas que deseen remitir SMS publicitarios o realizar algún tipo de notificación comercial a sus usuarios, deben registrarse y acceder a los identificadores alfanuméricos que utilizarán para su envío*"[4].

No obstante, **es necesario que se precise la relación de la medida frente al usuario**, a fin de evitar que la implementación del registro genere cargas adicionales para el consumidor, como la verificación previa de cada SMS recibido, lo cual podría restarle efectividad al propósito de prevención del fraude.

En segundo lugar, la adopción de una medida regulatoria que prohíba la inclusión de mensajes y URL en el contenido de SMS podría mitigar los riesgos de fraude por la modalidad de "*Smishing*", siempre y cuando exista una amplia difusión y divulgación pedagógica frente a los usuarios.

Cabe destacar que, en otros momentos, desde la regulación y con el apoyo de las autoridades competentes, se ha logrado que los operadores implementen soluciones tecnológicas que permiten el control y bloqueo de contenidos desde sus redes. Estas acciones, son objeto de seguimiento permanente desde el ejercicio de funciones de control, inspección y vigilancia del sector, donde se garantiza la protección de los usuarios en cumplimiento de obligaciones de la normatividad, que a continuación se detallan:

- **Bloqueo de las URL ordenado por autoridad judicial o administrativa:** Las autoridades de inspección, vigilancia y control, las autoridades de Policía y la **POLICÍA NACIONAL** pueden hacer monitoreo a los canales, entidades financieras, páginas de Internet y medios que de cualquier forma sirvan a la explotación, operación, venta, pago, publicidad o comercialización de juegos de suerte y azar no autorizados, y ordenar las alertas y bloqueos correspondientes (Parágrafo 3, Artículo 93, Ley 1753 de 2015[5] y sus modificatorias).

- **Bloqueo temporal de datos ante vulneración de derechos fundamentales**: Cuando, a partir de una solicitud y pruebas aportadas por el titular de los datos, se identifique un riesgo cierto de afectación a sus derechos fundamentales (Artículo 15

[4] Ibidem. Página 58.
[5] Ley 1753 de 2015 "*Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país"*".

de la Constitución Política de Colombia; Ley 1273 de 2009[6]; y, artículos 1 y 21 de la Ley Estatutaria 1581[7] de 2012).

- Establecer mecanismos técnicos de bloqueo por medio de los cuales se puedan impedir la difusión de material ilegal, ofensivo o contenido sexual relacionado con menores de edad. (Artículo 7, numerales 2 y 4 del artículo 8 de la Ley 679 de 2001[8]; Decreto 1078 de 2015[9]).

Por último, es necesario que la **CRC** establezca medidas regulatorias que fortalezcan la verificación de identidad para el acceso a los servicios de telecomunicaciones y a los elementos de red como es la reposición de la tarjeta SIM, para evitar así prácticas fraudulentas como el "*SIM swapping*" y las portabilidades ilegítimas realizadas por terceros mediante el uso indebido de la infraestructura de red.

2.3.1. 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?"

Desde el equipo de respuesta a Incidentes de Seguridad Informática de la **POLICÍA NACIONAL** ya se adelantan, de forma periódica, actividades educativas orientadas a la divulgación y prevención de riesgos informáticos tales como el "*Phishing*" y otras modalidades de fraude digital provenientes de SMS que, haciéndose pasar por entidades bancarias o de mensajería, solicitan datos personales a los usuarios de servicios móviles.

En este sentido, un usuario puede desde esta entidad disponer de herramientas de seguridad en línea para revisar archivos, URL y Apps maliciosas en los equipos terminales de voz móvil.

Por lo anterior, a las acciones educativas y de divulgación que ya se vienen ejecutando, deben sumarse aquellas medidas proactivas de educación al usuario sobre las formas más comunes de fraude (phishing, smishing, vishing, SIM swapping), a través de campañas continuas y obligatorias de manera periódica por parte de los **PRST**, **PCA** e **IT**.

"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?"

---

[6] Ley 1273 de 2009 "*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*".
[7] Ley 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales*".
[8] Ley 679 de 2001 "*Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución*".
[9] Decreto 1078 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*".

La creación de un portal que incluya una lista negra con los recursos de identificación denunciados e identificados como fraudulentos tiene un efecto informativo y disuasorio. No obstante, no sería una medida eficaz frente a la prevención del fraude, toda vez que traslada la carga de verificación a los usuarios y no a los **PRST**, **PCA** o **IT** quienes deben ser vigilantes de la información que cursa por los recursos de identificación a ellos asignados.

> ***"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?"***

La creación del sistema propuesto podría ser una herramienta útil para los asignatarios de recursos de identificación que realizan cesión de estos, al facilitar su trazabilidad y control. Sin embargo, desde el ámbito de protección de los usuarios frente al fraude cibernético, se reitera que la **CRC** debe indicar el alcance de esta medida, de modo que se configure como un instrumento efectivo de protección sin imponer cargas adicionales al usuario final.

De esta forma esperamos haber contribuido al enriquecimiento de tan importante iniciativa, quedando a disposición para resolver cualquier inquietud que se presente sobre el particular.

Cordialmente,

ALEJANDRO BUSTOS MENDOZA
JEFE OFICINA ASESORA JURÍDICA

Elaboró: David Mancera
Revisó: Carolina Ramírez / Juan David Lozano
Aprobó: Alejandro Bustos