Señores Comisión de Regulación de Comunicaciones,

En atención a la publicación para comentarios del Documento de formulación del problema relacionado con la "Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles" a continuación, la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, y sus Entidades Agremiadas responden a la consulta planteada y realizan algunos comentarios.

En términos generales, se evidencia que el problema formulado en el documento es acertado en su núcleo. No obstante, es necesario tomar en cuenta otros elementos para comprender la magnitud del fenómeno y los actores involucrados.

1) **Sobre si el problema definido involucra todos los elementos que evidencian las dificultades generadas en la comisión de fraude cibernético mediante la provisión de los servicios tradicionales de llamadas de voz y SMS, se considera importante plantear lo siguiente:**

   La formulación del problema se centra mayoritariamente en los agentes formalmente registrados ante la CRC (específicamente los operadores registrados en el Sistema de Información y Gestión de Recursos de Identificación (SIGRI) o en el Registro de Proveedores de Contenidos y Aplicaciones, e Integradores (RPCAI)). Si bien, estos agentes son importantes y es necesario tomar medidas concretas de una manera eficiente, se encuentra que una de las principales complejidades del fraude cibernético se basa en que buena parte de los ataques se originan desde fuentes que no cumplen cabalmente las obligaciones regulatorias para el uso adecuado de los recursos de identificación.

   Como es de su conocimiento, las llamadas y SMS son las principales vías utilizadas para ejecutar fraudes, especialmente a través de *smishing* y *vishing,* y estas prácticas afectan la confianza y seguridad de los consumidores en un sector altamente regulado pero vulnerable por el uso de vías que generan impactos reputacionales y operativos, y comprometen la seguridad del ecosistema financiero. La ausencia de herramientas regulatorias específicas para controlar el uso de recursos de identificación, como los códigos cortos y la numeración E.164, ha limitado la capacidad de respuesta del sector financiero. Por ello, se recomienda incluir la suplantación de identidad de entidades financieras como una de las manifestaciones más críticas del problema, dada su alta frecuencia e impacto económico.

   Adicionalmente, la problemática va más allá de este aspecto, ya que muchos usuarios de los servicios no están familiarizados con las diferencias de los recursos de identificación, ni la veracidad o legitimidad de éstos. Así, se suplantan todo tipo de entidades legítimas utilizando numeración falsa, envío de SMS con identificadores alterados, y llamadas desde centrales automáticas que imitan el lenguaje institucional, sin que el usuario final pueda identificar que el mensaje es fraudulento.

   En la práctica, no existe para los consumidores una forma clara y segura de verificar si una llamada o mensaje recibido proviene de su entidad financiera o de un actor

fraudulento. Esto, más allá de que las entidades financieras y otros actores implementen campañas de educación financiera y de prevención del fraude.

Por tanto, se recomienda que el documento reconozca que existe un crecimiento sostenido del fenómeno, reafirmando la necesidad de definir una nueva aproximación regulatoria de cara al problema, que resulte ágil y fácil de expedir, pero que no subestime las tecnologías por su antigüedad o decrecimiento en volumen de tráfico, sino que reconozca su papel como puntos de entrada al fraude. En este mismo sentido, resulta fundamental complementar esta visión con un enfoque particular en fraudes emergentes asociados a nuevas tecnologías —como el uso de inteligencia artificial generativa para suplantación de voz o mensajes.

2) **Sobre si las causas presentadas en este documento son las que generan el problema definido (4.2.1):**

Las causas identificadas por la CRC son pertinentes y reflejan aspectos fundamentales del problema. No obstante, se resalta que:

i. **Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso (4.2.1.1)**

Se coincide con la CRC en que el enfoque de la regulación de los recursos de identificación se ha orientado principalmente hacia su uso eficiente, en tanto se trata de un recurso escaso. No obstante, y sin desconocer la labor de la Comisión, resulta necesario contar con mecanismos regulatorios robustos que permitan distinguir entre comunicaciones legítimas y suplantadas, así como que los operadores verifiquen o monitoreen el uso adecuado de los números asignados.

Un aspecto importante que se ha identificado es la falta de una taxonomía unificada en torno a este tipo de fraudes, por lo que se requiere una articulación interinstitucional en la regulación de esta materia. Igualmente, se observan diferencias entre el marco normativo aplicable a las entidades vigiladas por la Superintendencia Financiera de Colombia (SFC) y el previsto por la CRC para los Proveedores de Redes y Servicios de Telecomunicaciones (PRST), particularmente en lo relacionado con seguridad de la información, fraudes, ciberseguridad y el régimen de responsabilidad correspondiente.

En este punto, podría también resultar valiosa la experiencia de la SFC para la construcción de un marco regulatorio integral que abarque a todos los actores involucrados en los denominados “riesgos cibernéticos”, y que contenga todos los elementos necesarios para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y SMS, y los resultados negativos que esto conlleva.

Así mismo, se recomienda incluir como causa adicional la ausencia de mecanismos obligatorios de validación de identidad del originador de llamadas y mensajes, lo cual facilita la suplantación de entidades legítimas, como instituciones financieras. Este vacío ha sido aprovechado por actores maliciosos para ejecutar fraudes por

ingeniería social, afectando la confianza de los usuarios y generando impactos económicos y reputacionales significativos.

Actualmente, el sector financiero y el de telecomunicaciones cuentan con una relación estrecha en la vinculación y prestación de los servicios financieros. Esto se puede ver reflejado de diferentes maneras como, por ejemplo, en que el número de identificación de un producto financiero corresponda al número de línea de telefonía móvil del titular y que, por medio de la SIM o E-SIM, el titular de la línea pueda recibir códigos *One Time Password* (OTP), como mecanismos de autenticación durante la vinculación a un producto financiero o durante el inicio de sesión en los canales digitales de las entidades financieras o para verificar que es el titular de una cuenta quien intenta ordenar un pago o una transferencia de fondos.

Es así como el sector financiero depende muchas veces de líneas de telefonía móvil seguras y confiables para que los consumidores puedan vincularse y realizar diferentes operaciones. No obstante, actualmente los operadores no cuentan con exigencias igual de robustas a las entidades financieras, de cara a los requisitos y condiciones asociadas a los procesos de debida diligencia, conocimiento y autenticación de las personas que poseen y utilizan tarjetas SIM y E-SIM.

Todo esto, permite concluir que en Colombia existe una problemática relacionada con la ausencia de sistemas de autenticación robusta, y, por lo tanto, una falta de identificación de los titulares de las líneas móviles, lo que ha facilitado la comisión de conductas delictivas y dificulta la identificación de los perpetradores, y su consecuente judicialización.

En el contexto internacional, varios países cuentan con exigencias normativas robustas en materia de conocimiento y autenticación de los titulares de líneas móviles, tales como: Alemania, Argentina, Australia, España, México, Perú, y Sudáfrica. En particular, Argentina partió de las siguientes consideraciones como base para hacer obligatorio el registro de los titulares de líneas móviles (Ente Nacional de Comunicaciones, 2016):

- *En la última década, la telefonía móvil se ha expandido de manera exponencial, configurándose en un servicio masivo de comunicaciones.*

- *La referida expansión, que ha brindado a la mayor parte de la sociedad argentina la posibilidad de acceder a los Servicios de Comunicaciones Móviles, se ve opacada debido a la proliferación de maniobras delictivas que, mediante la utilización de dichos servicios, ponen en riesgo la seguridad de los ciudadanos.*

- *Maniobras de esta naturaleza afectan la confianza de los usuarios y lesionan las condiciones en que deben ser prestados los servicios de telecomunicaciones,*

particularmente en lo concerniente a las condiciones de regularidad, continuidad y calidad en las prestaciones.[1]

Por su parte, la Ley 25 de 2007 en España estableció como antecedente que la naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados o delictivos. Por lo tanto, su objetivo se basa en establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de permitir que ciertos agentes puedan disponer de estos. Se trata de que todos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por internet.

Con base en lo anterior, y aunado a las diferentes propuestas expuestas se sugiere considerar las siguientes iniciativas:

- **Obligación de los operadores de telefonía móvil de contar con mecanismos fuertes de autenticación y validación de identidad para clientes.** Desarrollar una normatividad aplicable a los operadores, en la que se espera que estos implementen mecanismos de autenticación que permitan verificar que los titulares de las líneas sean quienes dicen ser.
- **Requisitos para controlar la emisión y re-expedición de SIMS y E-SIMS por parte de operadores de telefonía móvil.** Establecer normas aplicables a los operadores de telefonía, con el fin de mitigar el fraude por *SIM swapping* y disminuir la creación de "cuentas mula", que son aquellas que reciben dinero producto de fraude y lo dispersan por el sistema financiero.
- **Creación de un registro de titulares de líneas de telefonía móvil.** Desarrollar normas que dispongan la creación de un registro que contenga a los titulares de líneas de telefonía móvil para, así, facilitar la identificación de los titulares de aquellas líneas que sean utilizadas para la comisión de conductas delictivas.

ii. Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes (4.2.1.2)

El Documento señala como una de las causas del problema la supuesta insuficiencia de las medidas adoptadas por los PRST y asignatarios de recursos de identificación, sin considerar las limitaciones regulatorias, técnicas y operativas a las que se enfrentan los agentes para actuar de forma eficaz y oportuna frente a los eventos de fraude.

Parece complejo exigir prevención sin que medie una habilitación normativa ni exista una capacidad operativa para esos efectos. Actualmente, los operadores no cuentan ni con las competencias legales, ni con una instancia de coordinación institucional

[1] Resolución 8507 de 2016. Ente Nacional de Comunicaciones.

adecuada que les permita bloquear, filtrar o prevenir proactivamente conductas fraudulentas que se materializan a través de sus redes y que se ejecutan en cuestión de segundos.

Adicionalmente, cuando los efectos del fraude se producen de forma tan rápida (como en los casos de *smishing* o llamadas falsas que inducen a transferencias bancarias) cualquier acción que se adopte una vez iniciado el evento es, naturalmente, tardía. Las medidas reactivas no son una falla de diseño, sino el único recurso disponible frente a una amenaza ya ejecutada. Este escenario es estructural y no depende solo de la voluntad de los agentes.

En este sentido, resulta importante reconocer que las limitaciones del marco regulatorio y operativo actual dificultan la implementación de medidas más eficientes y oportunas. Por esto, se sugiere que la Comisión considere las siguientes recomendaciones, con miras a fortalecer un ecosistema más orientado a la prevención que a la reacción:

- Facultar de forma expresa a los PRST y asignatarios de recursos de numeración para bloquear tráfico o numeración sospechosa de forma preventiva, sin que ello implique riesgos regulatorios por afectación de servicios legítimos.
- Implementar un protocolo de bloqueo rápido de URL maliciosas, de origen nacional e internacional, cuando éstas sean identificadas con coordinación interinstitucional entre la CRC, el Ministerio de las Tecnologías y las Comunicaciones, la SFC, las entidades vigiladas por la SFC y proveedores tecnológicos, entre otros. Algo parecido a lo que ocurre con el bloqueo de URL para prestar servicios de juegos de suerte y azar que no están autorizados por Coljuegos.

iii. Desconocimiento de los usuarios sobre privacidad de la información que facilita la obtención de datos personales con fines fraudulentos (4.2.1.3)

Sea lo primero señalar que los ataques de ingeniería social se definen como aquellas prácticas mediante la cual se obtiene información confidencial a través de manipulación de usuarios legítimos.[2] Esa manipulación proviene de los atacantes al explotar características humanas como la confianza básica en los demás, el deseo de brindar asistencia o la propensión a lucirse, y se caracteriza precisamente por adaptarse de manera sofisticada a los comportamientos del usuario.

De conformidad con lo previsto en la Cartilla metodológica de Atención de Delitos Informáticos de la Fiscalía General de la Nación, se ha identificado un aumento en denuncias ciudadanas por la afectación a la información y a los datos, como consecuencia del aumento en el uso de las tecnologías de la información y las comunicaciones en la vida cotidiana. Adicionalmente, la Corporación Excelencia en la Justicia expone un indicador que mide el número de delitos informáticos

[2] Fiscalía General de la Nación. Cartilla Metodológica de Atención de Delitos Informáticos.

registrados por el Ministerio de Defensa, en el que se destaca un crecimiento significativo de esta tipología de delitos desde 2020 a nivel nacional. [3]

Sin perjuicio de la responsabilidad individual del usuario en la protección de su información personal, existe un conjunto de variables estructurales que están directamente asociadas al *modus operandi* de los criminales en la ingeniería social.

El incremento reciente en la comisión de estos delitos demuestra que se trata de una amenaza dinámica, que ha escalado en sofisticación y volumen en un entorno digital cada vez más complejo.

La acelerada digitalización de los diferentes ecosistemas ha ampliado de forma significativa la superficie de ataque a la que están expuestas las personas. Esto, ha permitido que los actores criminales desarrollen y apliquen con mayor frecuencia y sofisticación campañas de *phishing*, ataques a la cadena de suministro, técnicas avanzadas de ingeniería social, *ransomware* y otros mecanismos de acceso ilegítimo a la información.[4]

Por tanto, se sugiere tener en cuenta que, si bien la socialización y concientización de los usuarios sobre los riesgos asociados a fraudes digitales puede prevenir escenarios de ataques cibernéticos, la ingeniería social tiene muchas variantes en las que el usuario puede caer desprevenidamente en estos escenarios.

3) Grupos de valor (5.2):

Se sugiere incluir como grupo de valor no solo a las entidades financieras sino también a las Fintech, dado que son actores altamente expuestos al fraude cibernético mediante servicios móviles. Para éstas, los canales de contacto con clientes (SMS, llamadas, notificaciones, entre otros) son esenciales para la operación, y cualquier afectación en su seguridad impacta directamente la relación con el cliente y la estabilidad del ecosistema financiero.

Adicionalmente, se sugiere incluir dentro de los grupos de valor identificados a actores clave como lo son la SFC, la Superintendencia de Economía Solidaria y el Ministerio de Hacienda y Crédito Público, entre otros, con el fin de lograr una coordinación interinstitucional alineada y coordinada, que someta a sus vigilados a reglas homogéneas y de aplicación igualitaria a las Telcos y, de esa forma abordar de manera integral la problemática, conectando inclusive con Fiscalía y otros agentes que doten de herramientas a todos los actores.

4) Sobre las posibles alternativas de solución:

a) Respecto al uso indebido de la numeración de códigos cortos, los siguientes comentarios:

---

[3] Corporación Excelencia en la Justicia. Delitos Informáticos en Colombia. Disponible en: https://cej.org.co/indicadores-de-justicia/criminalidad/delitos-informaticos-colombia/

[4] Cámara Colombiana de Informática y Telecomunicaciones 2024. Ciberseguridad en el sistema financiero colombiano: entre la amenaza y la resiliencia.

i. La creación de un registro de remitentes con códigos alfanuméricos y campañas identificadas es una medida positiva que facilitaría la identificación de emisores legítimos y permitiría a los usuarios reconocer con mayor claridad las comunicaciones oficiales, reduciendo el riesgo de suplantación. Esta medida sería útil para proteger marcas reconocidas que son blanco frecuente de fraude, como las entidades financieras.

No obstante, el principal desafío será la adopción de tecnología avanzada y de fácil implementación, para garantizar la interoperabilidad entre operadores y la gestión del registro en tiempo real, asegurando que los datos estén actualizados y que exista validación efectiva de identidad para cada remitente. Otro desafío será garantizar la seguridad y privacidad de la información, teniendo en consideración la información que se está manejando y cómo la misma va a ser protegida, así como la trazabilidad de la responsabilidad de quien la debilita o vulnera.

ii. La creación de un registro unificado que incluya tanto códigos cortos como numeración E.164 no geográfica (como el NDC 940) es una medida viable y deseable. Esta integración permitiría una trazabilidad más robusta de las campañas de mensajería y una gestión más eficiente de los recursos de identificación, facilitando la detección de usos indebidos. El principal reto estaría en garantizar que los operadores implementen filtros adecuados y que los usuarios comprendan la diferencia entre los tipos de numeración, evitando confusiones que puedan ser aprovechadas por actores maliciosos.

iii. La prohibición de enlaces en SMS podría reducir significativamente la materialización del riesgo de fraudes tales como el *phishing*. Sin embargo, afectaría la experiencia del usuario en procesos como autenticación o notificaciones u alertas transaccionales e incluso podría interferir con la innovación tecnológica. Así mismo, esta prohibición podría limitar la comunicación entre usuarios y los diferentes grupos de valor, teniendo en consideración que personas con acceso limitado o población de escasos recursos, no tiene acceso a otros canales de forma inmediata. Una alternativa sería permitir enlaces únicamente desde dominios previamente registrados y verificados.

iv. La exclusividad de uso por código corto es una medida efectiva para evitar la suplantación. Sin embargo, podría generar escasez de numeración, por lo que se recomienda evaluar la ampliación del rango disponible o permitir la migración a numeración E.164 no geográfica, con reglas claras de uso exclusivo por entidad. La asignación de códigos debe realizarse acorde con las validaciones previas sobre la legitimidad de la actividad económica de las empresas en los registros oficiales y que se encuentren debidamente acreditadas. La reventa de códigos no debería ser considerada debido a que generaría desconfianza y podría constituir eventos de fraude.

v. La migración a numeración E.164 no geográfica es una alternativa robusta, especialmente si se acompaña de autenticación reforzada y monitoreo continuo. No obstante, requeriría ajustes técnicos y regulatorios, así como campañas de educación al consumidor. De manera que esto implica desafíos técnicos y de implementación.

vi. Implementar un sistema de "*firma digital*" del remitente en los SMS, que permita verificar la autenticidad del mensaje en el dispositivo del usuario, podría integrarse con soluciones de validación de identidad como DKIM (*DomainKeys Identified Mail*) para correo electrónico, adaptadas al canal SMS o con protocolos similares al STIR/SHAKEN en llamadas.

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

i. La creación del registro de originadores de llamadas comerciales es una medida recomendable para permitir que los usuarios puedan identificar llamadas legítimas, facilitando el bloqueo de llamadas fraudulentas, toda vez que se han identificado múltiples casos de suplantación de numeración en llamadas de *vishing* y *spoofing*.

Las técnicas de filtrado tecnológicas (*screening*) para identificar y bloquear llamadas o mensajes sospechosos resultan positivas. No obstante, se sugiere que estas sean contempladas en una regulación sobre el uso de numeración. Esto, permitiría hacer un filtro de los mensajes y llamadas que posiblemente, estén siendo utilizados para cometer algún tipo de fraude, adoptando herramientas tecnológicas de Inteligencia Artificial o *machine learning*, para robustecer el sistema y permitir una identificación efectiva.

En particular, se recomienda establecer rangos dedicados para llamadas comerciales legítimas, con validación previa del originador. En este contexto resulta fundamental garantizar el cumplimiento de los principios rectores de la Ley 1581 de 2012.

En todo caso, cualquier medida debe priorizar la comunicación a los usuarios sobre su alcance, al realizar análisis automatizados de la numeración, para realizar una clasificación y registro posterior en posibles bases que generen bloqueo o restricción, debido a que los números telefónicos son considerados datos privados. Adicionalmente, los bloqueos o restricciones deberán estar debidamente justificados en el marco regulatorio, especificando los criterios y parámetros para que los mismos puedan ser incluidos; así mismo se puede considerar la posibilidad de crear mecanismos y canales para atender PQRS en caso de presentarse reclamaciones sobre las mismas.

ii. La creación de un sistema de reputación de numeración, alimentado por reportes de usuarios, operadores y entidades financieras, entre otros, podría permitir clasificar números como confiables, sospechosos o maliciosos, y facilitaría su bloqueo preventivo. Adicionalmente, se propone la creación de una plataforma de validación en tiempo real que permita a los operadores verificar si una llamada o mensaje proviene de un remitente autorizado, antes de entregarla al usuario.

c) Respecto al desconocimiento de los usuarios sobre la privacidad de la información y las técnicas de ingeniería social:

i. Aunque se reconoce que la socialización tiene un impacto positivo para mitigar en los casos de ataques cibernéticos, las medidas de divulgación pedagógica no

atacan el problema de raíz. La ingeniería social usa métodos de manipulación psicológica, que permiten a los criminales manipular la decisión cognitiva del usuario.

Las entidades han desarrollado campañas educativas multicanal en torno al fraude, pero esto no ha mitigado el problema de su comisión ni los efectos negativos que esto conlleva, sobre todo cuando en el proceso se involucran suplantaciones de terceros que llevan al consumidor a un entorno de confianza (como sucede con la compra del seguro SOAT a través de páginas o SMS fraudulentas, que terminan llevando a la persona a hacer un pago que no corresponde).

ii. En línea con lo mencionado, la creación de un portal oficial de la CRC, desarrollado y reglamentado bajo estricto cumplimiento de la Constitución Política y demás normatividad vigente, constituiría una herramienta complementaria en términos de transparencia y de alerta temprana para los distintos actores del ecosistema digital, incluidos los usuarios, operadores y entidades financieras, que generaría un efecto disuasivo y contribuiría a visibilizar patrones reiterados de comportamiento delictivo. Su utilidad práctica dependerá de factores como la actualización permanente, la validación efectiva de los reportes y la capacidad de respuesta oportuna de los operadores y autoridades.

Ahora bien, la creación de dicho portal oficial debe estar debidamente reglamentada, con un alcance definido sobre competencias, actores, tiempos de permanencia y parámetros para su registro. Así mismo, quien tenga la competencia para administrar el portal, deberá velar porque la misma sea actualizada con regularidad.

iii. La creación de un sistema intersectorial de trazabilidad administrado por la CRC, con el fin de centralizar la información sobre recursos de identificación utilizados con fines presuntamente fraudulentos, permitiría una respuesta rápida y coordinada ante incidentes y facilitaría la identificación de patrones de fraude. Además, permitiría tener información con mayor detalle, que puede ser un recurso valioso para que las autoridades competentes realicen investigaciones objetivas que deriven en penas para quienes cometan hechos delictivos. Ahora bien, deben considerarse los canales por los cuales se escalarían dichas peticiones, tiempos de respuesta y los recursos que deben ser usados para atender de forma oportuna.

Sin embargo, su valor radica principalmente en su capacidad operativa y preventiva, no únicamente en su complementariedad con campañas educativas, las cuales, si bien son importantes, no deben ser el componente principal de la estrategia regulatoria. Este sistema tendría mayor impacto si se acompaña de herramientas técnicas para detección temprana, interoperabilidad con otras autoridades y obligaciones de actuación inmediata por parte de los agentes involucrados.

iv. Se propone incluir contenidos de prevención de fraude en los procesos de *onboarding* digital de los usuarios (ej. al activar una SIM, abrir una cuenta o registrarse en una App). Esto, puede incluir simulaciones de *smishing* y *vishing* para fortalecer la conciencia del usuario. Adicionalmente, puede considerarse la posibilidad de desarrollar una aplicación móvil oficial que permita a los usuarios

verificar en tiempo real si un mensaje o llamada proviene de una fuente legítima, y reportar incidentes de forma sencilla.

Finalmente, se reitera que, aunque se reconoce la relevancia de socializar con los usuarios los riesgos de fraude cibernético, este no puede ser el eje central en el proyecto regulatorio, toda vez que los mecanismos de control no han resultado suficientes para resolver los escenarios de delitos cibernéticos, por lo que el enfoque, más allá de instruir sobre la materia, debería estar en los medios de control aplicables para evitar los delitos cibernéticos.

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

i. Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto

Se coincide con la CRC en que la falta de articulación interinstitucional efectiva es una de las causas estructurales del problema y, en efecto, es un componente relevante para avanzar hacia una estrategia coordinada, efectiva y transversal frente al fraude cibernético. Sin embargo, el Documento no hace referencia al sector financiero y, en particular, a la necesidad de fortalecer los controles especialmente en lo relacionado con los ataques cibernéticos a los usuarios de este sector, a pesar de que una proporción significativa de los ataques cibernéticos a través de servicios móviles tiene como objetivo final la afectación patrimonial de los consumidores financieros, mediante transferencias de dinero no autorizadas o suplantación de la entidad bancaria para pedir información personal del usuario.

En este sentido, se recomienda que las medidas regulatorias y de interoperabilidad institucional contemplen de manera estructural la articulación con el sistema financiero y los usuarios de este sector, teniendo en cuenta que, según datos reportados por la SFC, para el año 2021, ha habido un 99% de incremento en los delitos de transferencia no consentida de activos y daño informático[5]. Esta cifra evidencia que los delitos cibernéticos dirigidos contra los consumidores financieros constituyen un foco de especial interés para los criminales, resultando imperativo que la regulación y coordinación interinstitucional incorpore de manera transversal y efectiva al sector financiero como parte esencial de la estrategia de prevención de fraude.

Finalmente, se incluyen otras recomendaciones generales:

- Automatizar los procesos de asignación y recuperación de recursos de identificación mediante plataformas interoperables.
- Establecer criterios de “uso seguro” de dichos recursos de identificación además del uso eficiente.

[5] Superintendencia Financiera de Colombia. 2021. Ciberseguridad en el sector financiero: ¿A la velocidad de la digitalización?

- Incluir cláusulas de revocación inmediata ante evidencia de uso fraudulento.
- Permitir auditorías cruzadas entre operadores, CRC y entidades afectadas.
- Encaminar esfuerzos a mitigar y gestionar deepfakes y contenido dañino generado por inteligencia artificial (IA).
- Publicar reportes periódicos de asignación y recuperación para transparencia sectorial.
- Sumar a la ecuación de responsables, los intermediarios en el flujo de envíos de SMS.
- Implementar un mecanismo de verificación de los códigos, similar a la verificación de cuentas en WhatsApp.
- Verificar las URLS contenidas en los SMS de manera previa al envío.
- Definir marco de controles mínimos de seguridad que deben tener todos los actores que accedan a plataformas o herramientas a través de las cuales se envían los SMS.
- Definir y exigir el cumplimiento de un estándar de seguridad para la comunicación y administración de las plataformas por las que se envían los SMS.
- Definir los lineamientos de seguridad para los PCA para registrarse, usar códigos cortos propios y responder ante alertas.
- Fortalecer la coordinación interinstitucional entre autoridades, así como integrar esfuerzos con la Estrategia Nacional de Seguridad Digital 2025–2027.
- Permitir esquemas de autenticación adaptativa según el tipo de transacción o nivel de riesgo (Multifactor), así como reconocer que el uso de OTP por App (TOTP) y biometría combinada puede ser más seguro que SMS tradicional.