Señores Comisión de Regulación de Comunicaciones (CRC)

Atendiendo la invitación para remitir comentarios al proyecto de resolución “Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones”, la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria), con el propósito de contribuir al fortalecimiento y adecuada expedición de la regulación sometida a consulta presenta a continuación sus observaciones y comentarios:

COMENTARIOS GENERALES

En términos generales, se considera que el Proyecto de Resolución ("PR") constituye un avance relevante en la regulación antifraude, particularmente frente a las modalidades de fraude en servicios móviles (voz y SMS), en tanto recoge varias de las preocupaciones del ecosistema e incorpora herramientas que, con los ajustes adecuados, pueden contribuir de manera efectiva a enfrentar fenómenos como el vishing, el smishing y el spoofing, entre otros.

Con el propósito de aportar a la construcción de esta iniciativa, a continuación, se formulan algunas observaciones orientadas a reforzar aspectos puntuales del PR y a asegurar que las medidas antifraude se implementen bajo criterios de proporcionalidad, trazabilidad y continuidad operativa, de modo que fortalezcan la seguridad de los usuarios:

Riesgos no intencionados derivados del diseño (técnicos y reputacionales)

Sin perjuicio de los beneficios esperados, se encuentra que el Proyecto puede generar riesgos no intencionados que deben evaluarse de manera integral, entre ellos la interrupción de controles antifraude críticos como los OTP´s.

Tales riesgos no derivan necesariamente de fallas en la implementación, sino del diseño mismo de los mecanismos propuestos en el Proyecto, en particular cuando introducen dependencias centralizadas o restricciones operativas sobre canales que hoy cumplen funciones esenciales en la prevención del fraude.

Desde el enfoque de gestión de riesgos, se sugiere especificar la operatividad de los mensajes OTP, de acuerdo a la definición expuesta en el Proyecto, ya que son mecanismos de autenticación y no deberían estar expuestos a interrupciones o demoras en la entrega de su información, con el fin de que las empresas habilitadas para el uso de este mecanismo cumplan con el objetivo de mitigar casos de suplantación, y transferencias no autorizadas. Situación que deriva en la pérdida de confianza de los usuarios y la reputación de la entidad.

Riesgo de desplazamiento de fraude

Resulta fundamental considerar el riesgo de que el fraude se desplace hacia canales no contemplados por las medidas regulatorias propuestas. La evidencia a nivel internacional indica que el fortalecimiento de controles sobre SMS y llamadas tradicionales puede motivar a los defraudadores a migrar hacia plataformas over the top (“OTT”), aplicaciones de mensajería instantánea o esquemas híbridos de ingeniería social. Este fenómeno podría provocar una relocalización del riesgo hacia entornos con menor supervisión o control.

En este contexto, resulta necesario que el diseño regulatorio adopte un enfoque integral y dinámico, que contemple la evolución de las tipologías de fraude e incorpore medidas

complementarias para mitigar su migración a otros medios digitales, como redes sociales o plataformas de mensajería. De lo contrario, la concentración de controles en canales específicos podría derivar en vacíos regulatorios y reducir la efectividad de las medidas implementadas.

Coordinación institucional e información

El Proyecto demanda una coordinación institucional efectiva que debería permitir la implementación de un régimen escalonado de responsabilidad, atendiendo a los roles, la capacidad de gestión y el nivel de control de cada actor en la cadena de prevención y respuesta al fraude. En ese sentido, se propone incorporar en el Proyecto un mandato expreso de articulación interinstitucional entre la CRC, la Unidad de Proyección Normativa y Estudios de Regulación Financiera (“URF”), la Superintendencia Financiera de Colombia ("SFC") y la Superintendencia de Industria y Comercio ("SIC"), orientado a diseñar reglas comunes de prevención, reporte, trazabilidad, corrección de incidentes y atención al usuario, de modo que las medidas del sector de telecomunicaciones se complementen con las obligaciones propias del sistema financiero y con acciones pedagógicas dirigidas a los consumidores.

Dicha articulación interinstitucional resulta fundamental, en la medida en que el esquema propuesto contempla flujos de información comercial y operativa hacia el validador, así como reportes periódicos. Si bien el Proyecto invoca la Ley 1581 de 2012, se considera conveniente reforzar las garantías de finalidad, minimización, seguridad y reserva sobre dicha información. Por lo anterior, se solicita incorporar de manera expresa los principios respecto de la información de los asignatarios, delimitar los usos autorizados y armonizar el régimen con la normativa de protección de datos.

Aunado a lo anterior, y en materia de intercambio de información, se observa que el Proyecto no contempla mecanismos formales entre los operadores de telecomunicaciones y el sector financiero, pese a que en múltiples ocasiones son las entidades financieras quienes identifican de manera temprana las campañas de fraude e ingeniería social, incluso antes que los propios operadores. En consecuencia, se sugiere evaluar la creación de un esquema de intercambio de información en tiempo real que permita reportar oportunamente y facilitar así acciones preventivas coordinadas entre los distintos actores del ecosistema.

Asignación de cargas elevadas sin representación clara

Se destaca como positiva la creación de instancias de coordinación y seguimiento, como el Comité Técnico de Seguimiento de Coordinación Operativa (“CTS”) y el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles (“CTLFSM”).

No obstante, su diseño actual podría limitar la participación efectiva de las entidades del sistema financiero, directamente afectadas por las conductas fraudulentas que quedarían subordinados a la operación de un único agente privado, pues su participación no es permanente al comité CTS, sino que serán invitados a sesiones específicas. Ello podría derivar en contravenciones al régimen de protección al consumidor financiero (Ley 1328 de 2009), al derecho a la intimidad (Ley 2300 de 2023) y a los deberes de seguridad y diligencia exigibles a las entidades vigiladas por la SFC, así como en una eventual afectación de los principios de proporcionalidad, igualdad y debido proceso.

Dado que el propio Proyecto admite la concurrencia de invitados a estas instancias, la propuesta consiste en extender esa lógica para que quienes soportan las obligaciones y sus efectos puedan ser tenidos en cuenta, armonizando el carácter vinculante de las decisiones con mecanismos adecuados de participación. En consecuencia, se sugiere:

- Incorporar a los asignatarios de SENDER ID, o a un representante del sector financiero a través de su gremio, como participantes con voz en el CTS e invitados permanentes en el CTLFSM.
- Garantizar la participación permanente del sector financiero, contemplar esquemas de intercambio de información en tiempo real y asegurar la articulación con los mecanismos de gestión del fraude ya existentes en el sector.
- Precisar que la excepción relativa a la no publicación de ciertos proyectos de regulación operará sin perjuicio de la implementación de mecanismos de socialización previa cuando las decisiones adoptadas en el marco del CTLFSM impongan nuevas cargas técnicas u operativas, especialmente si estas impactan a agentes que no se encuentren representados en el respectivo comité (artículo 16).

Cargas operativas relevantes

La normativa introduce nuevas obligaciones que implican cargas operativas considerables para todos los actores involucrados en los procesos de validación, monitoreo, actualización, atención de solicitudes, reclasificación, gestión de alertas, administración de consentimientos, uso de plantillas y coordinación con terceros tecnológicos. A continuación, se resaltan los elementos que presentan los mayores desafíos para una implementación efectiva:

- Los artículos 6 y 7, sobre asignación y obligaciones generales de recursos de identificación, representan un desafío jurídico relevante, al exigir el envío de autorizaciones escritas explícitas y la custodia de los soportes en la contratación con terceros.
- A ello se suma el artículo 12, que obliga a centralizar bajo el esquema de SENDER ID todas las operaciones de mensajería, hoy distribuidas en múltiples códigos cortos y a través de diversos integradores.
- El reto se agrava con el artículo 19, que prevé un período de transición de solo seis meses, plazo insuficiente para una migración de esta envergadura; de ahí la pertinencia de que estos comentarios contribuyan a enriquecer el Proyecto.
- El artículo 2 delimita de manera rígida las responsabilidades por el tráfico (pese a que algunas entidades financieras actúan como PCA apoyadas en Integradores Tecnológicos) y redefine el Código Corto A2P como un recurso individual para agentes con conexión directa a los operadores móviles, lo que reduce la flexibilidad operativa con la que hoy cuentan estas entidades.

Por las razones expuestas, se considera que la CRC debería evaluar la proporcionalidad de dichas exigencias, los plazos de implementación y la capacidad operativa real de los sujetos obligados, toda vez que la aplicación simultánea de todas estas obligaciones, sin fases progresivas, podría generar riesgos para la continuidad del servicio, reprocesos, costos elevados y afectaciones no deseadas sobre servicios legítimos. En consecuencia, se propone adelantar pruebas piloto y establecer etapas escalonadas que permitan ajustar los parámetros técnicos, validar los impactos reales y corregir fallas antes de avanzar hacia una implementación generalizada.

Régimen de responsabilidad compartida.

El Proyecto introduce un régimen de responsabilidad compartida para combatir el fraude en servicios móviles, a partir del reconocimiento de que este no se origina en un único punto de la cadena, sino que demanda obligaciones diferenciadas según el rol, la capacidad de control y el acceso a la información de cada actor (PRSTM, IT, PCA, entidades financieras, autoridades y usuarios). En esa línea, la industria financiera enfatiza que la efectividad de las medidas de prevención del fraude digital requiere un esquema que articule proporcionalmente dichas obligaciones, fomentando acciones coordinadas y complementarias,.

Como referente de esta aproximación, se cita el Shared Responsibility Framework (SRF) de Singapur, adoptado por la Monetary Authority of Singapore (MAS) y la Infocomm Media Development Authority (IMDA), en el cual las responsabilidades se distribuyen entre instituciones financieras, operadores de telecomunicaciones y usuarios conforme a deberes específicos de prevención y respuesta. Este modelo demuestra que la mitigación del fraude es más efectiva cuando las obligaciones se asignan según la posición real de cada actor en la cadena de riesgo. A partir de esta premisa, se resalta la necesidad de atender los siguientes escenarios de asignación de responsabilidad:

En primer lugar, los riesgos derivados de fallas en la entrega, validación o clasificación de comunicaciones críticas pueden generar incertidumbre en la atribución de responsabilidades, especialmente cuando la afectación proviene de infraestructuras o procesos ajenos al control directo de las entidades financieras. Por tanto, el marco regulatorio podría contemplar reglas claras de atribución que consideren el grado de control efectivo de cada actor sobre el riesgo, así como mecanismos de resolución de controversias que brinden seguridad jurídica a los usuarios y a los participantes del sistema.

En segundo lugar, y en relación con los escenarios de atribución (previstos en los artículos 6.13.4.4, 6.12.2.2.3 y 6.12.3.2), el Proyecto contempla la recuperación del SENDER ID por mal uso de plantillas, junto con un período de inhabilidad para su reasignación. No obstante, dado que en este proceso intervienen terceros (en particular el integrador tecnológico), existe el riesgo de que conductas no imputables a la entidad financiera terminen afectando su recurso de identificación, privándola por un plazo prolongado de un canal esencial de comunicación con sus clientes, perjudicando también al consumidor.

Por lo anterior, se solicita que el mal uso atribuible al integrador no pueda derivar en la no recuperación del SENDER ID de la entidad financiera. Asimismo, se recomienda excluir del período de inhabilidad las modalidades de autenticación y transaccionalidad de las entidades vigiladas o, en su defecto, reducir sustancialmente dicho plazo e informar de manera inmediata a la entidad financiera el sobre el comportamiento de su proveedor.

Tratamiento diferenciado de comunicaciones de servicios financieros críticos

El Proyecto incorpora obligaciones de etiquetado, validación y bloqueo que pueden incidir en servicios financieros críticos dependientes de los canales de SMS y voz (alertas transaccionales, mensajes de seguridad, códigos OTP y confirmaciones de identidad, entre otros). A diferencia de la mensajería comercial, estas comunicaciones forman parte de la arquitectura de prevención del fraude, por lo que su interrupción, demora o clasificación errónea podría comprometer la seguridad de las transacciones, abrir ventanas de

exposición o retrasar la reacción frente a operaciones sospechosas. En ese contexto, se señalan los siguientes puntos:

- **Bloqueo de llamadas internacionales**. El bloqueo de llamadas entrantes con numeración nacional (CLI), salvo el roaming debidamente identificado, podría afectar comunicaciones legítimas de entidades que se apoyan en centros de contacto o enrutamiento internacional. Por ello, se solicita prever un tratamiento específico para su tráfico internacional legítimo.

- **Monitoreo y restricción del tráfico P2P**. Se sugiere precisar el detalle operativo por el cual se va a tener seguimiento en el monitoreo de tráfico P2P. El numeral 2.1.10.7.2.1.1 exige a los PRST acreditar ante la CRC la detección de al menos seis patrones de uso atípico (volumen inusual, dispersión de destinatarios, homogeneidad del contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red), y en voz se exigen sistemas en tiempo real para robocalls y numeración fraudulenta.

Por lo anterior, se estima necesario prever procedimientos diferenciados y prioritarios para las comunicaciones de las entidades vigiladas por la SFC (especialmente mensajes transaccionales, alertas de seguridad y autenticación reforzada), de modo que no queden sujetas a restricciones que generen latencia o bloqueos, sino a controles posteriores, trazabilidad reforzada y mecanismos ágiles de corrección.

Indicadores de monitoreo

Se propone que el esquema regulatorio incorpore indicadores de desempeño y efectividad que permitan monitorear de manera continua el impacto de las medidas adoptadas, tales como las tasas de falsos positivos en el etiquetado, los niveles de disponibilidad de los servicios de validación, los tiempos de entrega de mensajes críticos y las métricas asociadas a la evolución de los eventos de fraude. Su definición facilitaría la adopción de ajustes oportunos, permitiría evaluar la proporcionalidad de las medidas y contribuiría a asegurar que los controles cumplan efectivamente su propósito de mitigación del riesgo.

Gobernanza de listas, clasificación de numeración y mecanismos de corrección

Si bien el Proyecto prevé mecanismos de revisión periódica, expiración automática y corrección para el etiquetado de comunicaciones y las listas Do Not Originate (DNO), conviene fortalecer su gobernanza y operación. A tal efecto, debería precisarse la autoridad encargada de administrar, supervisar y actualizar estos registros; los criterios para incluir, excluir, revisar o retirar numeración; y las condiciones de acceso para los PRSTM y demás actores autorizados.

De manera concurrente, se destaca la preocupación sobre la gobernanza del validador centralizado y los tiempos de respuesta para el takedown de campañas de smishing y URLs, toda vez que este proceso exige hoy que el titular legítimo de la URL reporte el dominio y, en plataformas como Shopify o WooCommerce, la revisión por parte del propietario retrasa el takedown, lo que incrementa la efectividad de las campañas fraudulentas.

En esa misma línea, resulta necesario definir con mayor precisión quién determina que una línea, número o identificador debe clasificarse como fraudulento y bajo qué criterios

técnicos, probatorios y procedimentales, en tanto ello es indispensable para evitar decisiones arbitrarias, mitigar los falsos positivos y garantizar mecanismos oportunos de validación, revisión y corrección. Dicha clasificación debería sustentarse en evidencia técnica suficiente, patrones verificables de comportamiento irregular o reportes consistentes de actores autorizados, y acompañarse de plazos específicos de reclasificación (diferenciados según la criticidad del servicio afectado) y de canales que permitan a las entidades financieras reportar falsos positivos, advertir afectaciones operativas y contribuir a la mejora continua del sistema.

Finalmente, la efectividad de estas medidas dependerá de la capacidad del sistema para mantener bases de información actualizadas de forma continua, pues en un entorno donde los defraudadores migran rápidamente entre números, dispositivos y canales de contacto, una actualización tardía puede reducir materialmente la utilidad de las herramientas de protección y afectar comunicaciones legítimas. Por lo anterior, se considera que el Proyecto debería precisar la periodicidad, los responsables y los estándares mínimos de actualización de las bases de información empleadas para las listas DNO, el etiquetado, los validadores, los registros de originadores y demás herramientas de prevención.

Trazabilidad técnica e intercambio seguro de información

Las medidas propuestas podrían derivar en una trazabilidad meramente formal si no permiten identificar técnicamente el origen real de las comunicaciones fraudulentas a lo largo de la cadena. En efecto, modalidades como el spoofing, el enmascaramiento de llamadas o la utilización sucesiva de múltiples numeraciones exigen mecanismos de verificación robustos que determinen quién origina, cursa, intermedia o modifica una comunicación.

Por ello, se considera que deberían incorporarse mecanismos de trazabilidad técnicamente verificables, interoperables y auditables, que identifiquen el origen real de la comunicación y los actores que intervienen en su transmisión. Dicha trazabilidad debería servir no solo para fines de monitoreo, sino también para activar medidas correctivas, suspender conductas fraudulentas, facilitar la actuación coordinada de las autoridades y alimentar canales seguros de intercambio de información entre PRSTM, Integradores Tecnológicos (IT), Proveedores de Contenidos y Aplicaciones (PCA), entidades financieras y demás actores autorizados.

Ahora bien, En concreto, el Proyecto permite que los actores autorizados reporten modalidades de fraude, falsos positivos, patrones de tráfico sospechoso y numeración asociada a eventos fraudulentos y, a su vez, habilitar que los PRSTM retroalimenten a los demás actores sobre alertas relevantes, patrones emergentes y medidas adoptadas frente a comunicaciones irregulares. Sin embargo, el intercambio de información enfrenta desafíos significativos en materia de seguridad, oportunidad y claridad regulatoria, por lo que debería operar bajo reglas claras de necesidad, proporcionalidad, finalidad específica, reserva y protección de datos personales, limitándose a lo estrictamente necesario para prevenir, detectar y mitigar el fraude y asegurando trazabilidad sobre el acceso, uso, conservación y eliminación de la información.

Finalmente, resulta conveniente que la información obtenida por los operadores móviles en sus procesos de debida diligencia y validación reforzada de usuarios pueda compartirse, en lo posible sin cobro o a costo mínimo y bajo condiciones apropiadas de seguridad y protección de datos, con las entidades que emplean estos canales para autenticación,

validación de identidad y envío de OTP. Resultaría de especial utilidad la información sobre los mecanismos de autenticación aplicados en procesos como la expedición de líneas, la reposición de SIM, los cambios de titularidad o las validaciones de identidad, toda vez que ello fortalecería los controles de prevención del fraude de las entidades financieras y demás actores legítimos del ecosistema.

COMENTARIOS ESPECÍFICOS

Implementación del SENDER ID y aprobación rápida - (Artículos 6.12.1.3.1. y ss.)

La obligatoriedad de contar con SENDER ID único, validación previa, pasar por un proceso de KYC y aprobación de plantillas, introduce cargas operativas y tiempos adicionales que podrían afectar la agilidad en el envío de comunicaciones críticas, particularmente aquellas asociadas a autenticación, seguridad o alertas de fraude. Por lo anterior, se surgiere incorporar un régimen diferencial o expedito para asignatarios de SENDER ID que requieran enviar mensajes de naturaleza crítica, garantizando: i) Una aprobación automática o fast-track de plantillas, para comunicaciones asociadas a prevención del fraude, autenticación de clientes, envío de códigos OTP (One Time Password), alertas de seguridad y notificaciones transaccionales; y ii) Definir de manera expresa los términos máximos niveles de servicio aplicables a los procesos de validación y aprobación del validador centralizado, así como los mecanismos de contingencia que deberán activarse en caso de indisponibilidad, fallas operativas o demoras en la respuesta.

Mensajes comerciales o publicitarios - Artículo 6.12.1.3.3

La norma obliga a los operadores a implementar monitoreo en tiempo real con algoritmos de analítica de datos, por lo cual se sugiere que esta misma exija que las comunicaciones de cobranza o recuperación de cartera y comerciales estén debidamente parametrizadas e inscritas ante los operadores móviles para no ser catalogadas erróneamente como "sospechosas".

De igual manera, se propone evaluar un esquema de registro o identificación de las numeraciones utilizadas por las entidades vigiladas en procesos como cobranza, atención al cliente, autenticación y gestión operativa. Dicho mecanismo debería permitir acreditar la finalidad legítima de las comunicaciones y garantizar que las numeraciones registradas no sean objeto de etiquetado automático como sospechosas, sino que reciban un tratamiento diferencial basado en el análisis de riesgo.

Finalmente, se recomienda considerar la implementación de un *sandbox* regulatorio que permita validar en entornos controlados las medidas propuestas (en especial las relativas a la identificación de remitentes, el monitoreo de tráfico y el etiquetado de comunicaciones) antes de su despliegue a nivel nacional.

Plan de contingencia del validador - Artículos 6.13.2.2, 6.13.4.1 y 6.13.4.7.2

Se sugiere que el proyecto establezca estándares mínimos de disponibilidad, tiempos máximos de respuesta, mecanismos de auditoría, trazabilidad de las decisiones y procedimientos expeditos de revisión frente a bloqueos o clasificaciones erradas.

Cabe resaltar que el propio Proyecto ofrece una base para esta solución, pues el artículo 6.13.2.2 ya permite cursar el tráfico asociado a registros previamente validados durante las

contingencias, bastaría con extender esa previsión a estas modalidades. En concreto, se propone que durante la indisponibilidad del validador no se interrumpa el curso de las plantillas de autenticación y seguridad ya aprobadas y vigentes; que se establezca un trámite expedito para las plantillas de alertas de fraude, atendida su naturaleza urgente y cambiante; y que se reconozca el carácter crítico de este tráfico en los niveles de servicio del validador.

Debida diligencia de los asignatarios de código corto A2P – Artículos 6.13.3.1 y siguientes

La debida diligencia sobre los agentes que acceden a los recursos de identificación constituye un control necesario para la integridad del ecosistema, por lo que se respalda su incorporación. En efecto, las entidades vigiladas por la SFC son objeto de comprobación permanente de su existencia, representación, estructura de propiedad, beneficiario final y perfil de riesgo, en el marco de la supervisión y de sus sistemas de administración de riesgos. Por ello, exigir que un agente privado rehaga esa verificación sobre una entidad ya supervisada no añade seguridad al esquema, sino que impone una carga redundante y multiplica la circulación de información sensible, en tensión con el principio de proporcionalidad que debe guiar la actuación administrativa.

Cabe agregar que el propio Proyecto reconoce la condición de entidad vigilada como elemento relevante del esquema (por ejemplo, al regular las plantillas de las modalidades de autenticación y transaccional en el artículo 6.13.4.2.7), lo que confirma que dicha calidad es un criterio idóneo para graduar la intensidad del control.

Por lo anterior, se solicita que, tratándose de entidades vigiladas por la SFC, el proceso de conocimiento del cliente pueda satisfacerse mediante la acreditación de tal condición y de la titularidad del signo distintivo, de modo que el validador y el asignatario de código corto A2P puedan apoyarse en la información ya verificada por el supervisor natural y se cumpla la finalidad del control sin duplicar diligencias ya practicadas.

Enfoque diferencial en campañas educativas - Artículos 6.14.2.2. y 6.14.3.1.

El proyecto propone la adición de un Capítulo 14 al Título VI de la Resolución CRC 5050 de 2016, que crea obligaciones concretas para los asignatarios de recursos de identificación y los PRST que contratan con entidades del sector financiero, orientadas a fortalecer la confianza y la verificación de las comunicaciones. En particular, estos agentes deberán incluir en sus contratos con clientes financieros la obligación de registrar los códigos cortos, los SENDER ID y la numeración utilizada para SMS y llamadas de voz en un portal habilitado por la CRC, de consulta pública, para que los ciudadanos validen la autenticidad de las comunicaciones. Asimismo, deberán apoyar la difusión de medidas pedagógicas y campañas de prevención del fraude (incluidas modalidades como el smishing y el vishing), con énfasis en la protección de datos personales.

parase sugiere mencionar directamente las responsabilidades contractuales de los asignatarios y los PRST para identificar si estas recaen directamente sobre ellas cuando actúan como PCA o IT. De ello se deriva, en particular, la obligación de mantener actualizado en tiempo real, en el portal de la CRC, el listado de todas las líneas de sus call centers (propios o tercerizados) y de sus canales de SMS, de modo que el usuario pueda verificar la legitimidad del contacto bancario.

Adicionalmente, se estima pertinente que las campañas pedagógicas previstas en el Proyecto incorporen enfoques diferenciales para las poblaciones más expuestas o vulnerables, como los adultos mayores, las personas con menor alfabetización digital y las personas con discapacidad, pues la prevención del fraude no depende únicamente de controles técnicos, sino también de que los usuarios identifiquen señales de alerta, reconozcan los canales oficiales, comprendan los riesgos de entregar información sensible y conozcan los pasos para reportar eventos sospechosos. En consecuencia, dichas campañas deberían diseñarse con lenguaje claro, formatos accesibles y canales adecuados para cada población objetivo, de manera que la información resulte comprensible, oportuna y útil para prevenir el fraude.

Régimen de recuperación de recursos y desconexión - Artículo 6.1.1.8

Las medidas de recuperación de códigos cortos y la eventual desconexión pueden generar impactos operativos relevantes para terceros (clientes finales) y afectar la continuidad de servicios financieros. Por lo anterior, se sugiere incorporar esquemas de transición reforzada para servicios críticos, la obligación de notificación previa a los usuarios finales en casos relevantes, y mecanismos de coordinación con autoridades sectoriales (SFC) cuando se involucren o se vean afectados servicios financieros.

Modificación del procedimiento de recuperación de recursos - Artículo 8

El artículo 8 permite a la CRC suspender de forma preventiva el uso de un código corto hasta por seis meses durante una investigación. Asimismo, faculta a los operadores móviles para suspender unilateralmente, por un mes, la relación con un PCA/IT cuando la CRC le haya recuperado códigos cortos en dos ocasiones, e iniciar la desconexión definitiva ante una tercera reincidencia.

Esta disposición tiene un impacto directo en la operación de las entidades financieras, pues si su proveedor de mensajería (IT) incurre en malas prácticas con otros de sus clientes corporativos y, como consecuencia, se le suspende el código corto, las comunicaciones de la entidad podrían verse interrumpidas de forma colateral, sin que medie responsabilidad alguna de su parte. Esta situación obligaría a incorporar cláusulas contractuales de contingencia con niveles de servicio (SLA) estrictos. Por lo anterior, la norma debería prever una alternativa que garantice que la suspensión del código corto no afecte a la entidad financiera ajena a la conducta sancionada.

Recomendaciones adicionales:

Con el fin de mitigar los riesgos identificados, se recomienda complementar el Proyecto con medidas que fortalezcan el enfoque preventivo, sin afectar la continuidad operativa ni la efectividad de los controles antifraude existentes. En particular, se considera positiva la incorporación de medidas como las siguientes:

- Mecanismos de redundancia y validación alternativa frente a fallas de los componentes centralizados.
- Protocolos de comunicación al usuario en escenarios de falla o de inconsistencias en el etiquetado.
- Mesas intersectoriales permanentes para la gestión coordinada de incidentes de fraude.

- La adopción, por parte de la CRC, de un enfoque de evaluación ex ante y ex post del riesgo sistémico asociado a las medidas, que asegure que los beneficios esperados superen los impactos potenciales sobre la estabilidad, la continuidad y la seguridad del ecosistema.