Bogotá D.C., 28 de julio de 2025.

Ingeniera
CLAUDIA XIMENA BUSTAMANTE OSORIO
Directora Ejecutiva
COMISIÓN DE REGULACIÓN DE COMUNICACIONES – CRC
Calle 59 A bis No. 5- 53
Ciudad.

Asunto: Comentarios al documento de formulación del problema denominado *"Identificación de medidas para mitigar el Fraude Cibernético por medio de servicios móviles"*.

Respetada Ingeniera Bustamante,

De conformidad con el plazo concedido por su entidad para la remisión de comentarios al proyecto regulatorio del asunto, desde Colombia Móvil S.A. ESP (en adelante TIGO), nos permitimos presentar para su consideración nuestros comentarios.

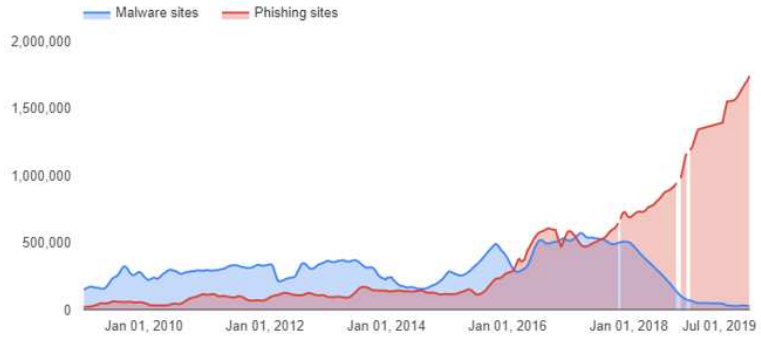
Valoramos el esfuerzo que realiza la comisión en la identificación de medidas para mitigar el Fraude Cibernético que se presenta por medio de servicios móviles considerando que, a pesar de que esta problemática desborda su marco de competencia y reconoce que esta situación exige la coordinación y definición de una estrategia conjunta, intersectorial y que, incluso, involucre a actores del sector privado y aun así se plantea abordar esta importante discusión.

1. ALCANCE DEL IMPACTO DE LOS FRAUDES CIBERNÉTICOS

La evolución tecnológica no sólo ha brindado a diversos sectores económicos la oportunidad de mejorar su eficiencia y productividad, sino que también ha servido como una premisa para que individuos y organizaciones dedicadas a actividades ilícitas expandan su ámbito de acción. Este fenómeno se ha intensificado en los últimos años con el crecimiento de la tecnología digital, la interconexión de sistemas y la dependencia creciente de internet para actividades personales, empresariales y gubernamentales.

En este sentido, de acuerdo con datos de Sectigo, los casos de phishing experimentaron un crecimiento aproximado del 800 % entre 2016 y 2019. Este dato resulta particularmente relevante si se considera que, en la actualidad, existen múltiples modalidades de delitos informáticos que han evolucionado en complejidad y frecuencia.

Gráfica 1. Evolución casos de Phishing.



Fuente. Sectigostore.[1]

A propósito, la Fiscalía General de la Nación ha podido identificar diferentes mecanismos utilizados por los delincuentes para cometer este tipo de delitos, los cuales ha documentado e incluso estableció una metodología para atención de estos delitos, entre los que destacan: ingeniería social, software malicioso, phishing, vishing, smishing, SIM swapping, explotación de vulnerabilidades, insider threats, carding, falsificación de identidad virtual y ransomware, entre otros[2].

En este contexto, el inicio de este proyecto regulatorio se presenta como una medida pertinente frente a esta situación. Asimismo, consideramos acertada la denominación del proyecto "*Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles*", en la medida que refleja adecuadamente la intención de abordar las diferentes modalidades de fraude cibernético que pueden presentarse en el mercado relevante de servicios móviles, el cual incluye los servicios de voz saliente móvil, SMS/MMS e **internet móvil**.

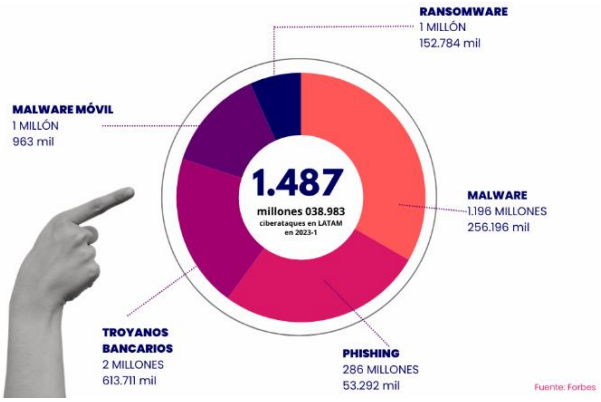
Ahora bien, en el árbol de problema, se observa que la definición del problema tiene un enfoque que se limita a los servicios de voz saliente móvil y SMS, los cuales presentan una tendencia decreciente en el uso por parte de los usuarios. En esta vía, se deja por fuera el servicio de internet móvil, que ha experimentado un crecimiento sostenido y se ha convertido en el principal canal de acceso a comunicaciones y contenidos digitales. Consideramos que incorporar este servicio en el análisis podría resultar valioso, toda vez que una parte importante de los incidentes de ciberseguridad se presentan a través de internet. Por ello, incluir este servicio permitiría una visión más completa y alineada con la realidad actual de preferencia de los usuarios para elegir su canal de comunicación móvil.

[1] https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/
[2] https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf

Es preciso señalar que la CRC puede intervenir cuando el uso de un servicio regulado, como lo es el internet móvil, habilita prácticas que afectan la experiencia del usuario o comprometen sus derechos, incluyendo, pero sin limitarse a la seguridad del acceso, la integridad del canal de comunicación y la protección frente a prácticas abusivas o riesgosas.

Una delimitación que no contemple adecuadamente todos los servicios a través de los cuales se perpetran este tipo de fraudes, en particular el internet móvil, podría limitar el impacto y alcance de las medidas regulatorias. Dado que este servicio se ha consolidado como el medio predominante de comunicación y acceso digital, su exclusión debilitaría el enfoque integral que pretende abordar este proyecto regulatorio como estrategia efectiva de mitigación del fraude.

Gráfica 2. Ciberataques en LATAM en el 1S-2023.



Fuente. Tendencias de Ciberseguridad.[3]

Asimismo, en la Gráfica 2 se observa que, del total de incidentes registrados en América Latina, los ciberataques por phishing representan el 19 %, lo que hace necesario que este proyecto regulatorio mantenga una perspectiva amplia que considere las diversas modalidades. Además, aunque este tipo de ataque puede adoptar distintas formas, como el smishing, la propagación vía correo electrónico es un factor relevante. En este tipo de fraude, el ataque se concreta a través de enlaces maliciosos que redirigen a sitios web falsos diseñados para capturar información confidencial. En estos casos, incluido el smishing, el acceso a internet es un componente indispensable para la ejecución del ataque, ya que la interacción con los sitios fraudulentos requiere conectividad.

Adicionalmente, el entorno digital se ha convertido en el principal escenario donde empresas y proveedores de contenidos enfrentan serios desafíos en materia de ciberseguridad, especialmente en lo relacionado con la protección de datos personales. Plataformas que ofrecen servicios como redes sociales, comercio electrónico o contenidos bajo demanda gestionan volúmenes significativos de información sensible que incluye datos personales, historiales de navegación y detalles de pago, lo que las convierte en blancos altamente atractivos para los

[3] https://www.linkedin.com/pulse/tendencias-en-ciberseguridad-para-2024-protegiendo-tu-futuro-iqkee/

ciberdelincuentes. Esta condición confirma la necesidad de incluir el servicio de internet móvil, así como los actores que ofrecen sus servicios mediante este canal de comunicación dentro del análisis regulatorio, en la medida en que constituye un punto crítico en la cadena de materialización del fraude, y que hoy día constituyen el verdadero origen de los problemas asociados a ciberdelitos.

Sumado a esto, la revisión de medidas de seguridad en el servicio de internet es algo que en otros espacios la Comisión ha revisado, en el Artículo 2.9.2.3 *Seguridad de la Red* de la Resolución CRC 5050 de 2016, existen disposiciones a cargo de los PRST relacionadas con el servicio de internet, condiciones que deben hacerse extensivas en su cumplimiento para otros actores.

Aunado a lo anterior, consideramos importante que la Comisión revise de fondo lo relacionado con los mecanismos de autorización expresa por parte de los usuarios para ser contactados por distintos agentes del ecosistema digital. En particular, respecto al envío de mensajes de texto (SMS), debe precisarse que la autorización otorgada por el usuario a un PRSTM no puede entenderse como una habilitación automática a otros actores, como los Proveedores de Contenido y Aplicaciones (PCA), Integradores Tecnológicos (IT) y proveedores de contenido OTT salvo que exista una autorización independiente, libre, previa, informada y expresa para tales fines. Además, si bien los PRSTM desempeñan un rol esencial en la distribución del mensaje, su función se limita a ser un canal de transmisión, y no implica necesariamente que cuenten con autorización para la contactabilidad en nombre de terceros, por lo que los PCA e integradores deben contar con su propia autorización de datos personales e imponerles la obligación de constatar con sus clientes que posean la debida autorización y que sus contratos contemplen la transferencia o transmisión de datos personales con la debida autorización previa de dichos clientes de los PCA.

Si bien la Ley 2300 de 2023, establece límites y condiciones para que proveedores de productos y servicios, incluyendo entidades financieras, contacten a los consumidores mediante llamadas, mensajes u otros canales, esta norma de rango legal se centra en la protección de la intimidad y tranquilidad del usuario, regulando la frecuencia, horario, medios autorizados y la necesidad de obtener consentimiento previo, tanto para fines de cobranza como para comunicaciones de contenido comercial.

A su vez, con la Resolución CRC 7356 de 2024 amplía el alcance del Registro de Números Excluidos (RNE), extendiendo su aplicación no solo a los proveedores de servicios de comunicaciones, sino también a otros sectores que utilicen canales de contacto como llamadas, mensajes de texto, mensajes electrónicos y aplicaciones móviles; pero se limitó a establecer la obligación de consultar el RNE antes de realizar cualquier contacto con fines publicitarios, comerciales o de cobranza.

Finalmente, es relevante mencionar el Decreto 851 de 2024, mediante el cual se establecen medidas para el bloqueo de comunicaciones no autorizadas desde los Establecimientos de

Reclusión del Orden Nacional (ERON), con el objetivo de frenar prácticas delictivas originadas desde estos centros; y complementariamente, la Resolución 743 de 2023 de la Agencia Nacional del Espectro (ANE) en la que se define la metodología técnica y operativa para la instalación, control y verificación de sistemas de inhibición de señales en los ERON, precisando niveles de señal, zonas de interferencia aceptable y parámetros técnicos de evaluación, en coordinación con el INPEC y los operadores móviles. Si bien estas medidas representan avances significativos en el control de ciertas fuentes de fraude, especialmente aquellas vinculadas a llamadas extorsivas desde centros penitenciarios, resultan claramente insuficientes frente a la complejidad del fenómeno de la contactabilidad indebida. Los esquemas actuales no abordan, por ejemplo, el enrutamiento internacional fraudulento, el uso de canales alternativos como aplicaciones de mensajería OTT, ni la generación de tráfico sospechoso desde redes móviles urbanas.

La actual ambigüedad normativa genera espacios de interpretación que dificultan el accionar efectivo de las autoridades de vigilancia y control. Por ello, se considera necesario que la regulación establezca de manera clara y explícita los límites y condiciones bajo los cuales distintos tipos de proveedores pueden contactar a los usuarios, de modo que se habilite un marco jurídico robusto y suficiente que facilite la intervención de las autoridades en caso de eventuales infracciones o prácticas abusivas.

En conclusión, **solicitamos respetuosamente a la Comisión que este proyecto no se limite exclusivamente a los servicios de llamadas de voz tradicional y mensajes cortos de texto (SMS), sino que también incorpore dentro del análisis el servicio de internet móvil**, el cual forma parte del mismo mercado relevante. Esta inclusión resulta esencial para abordar de manera integral el fenómeno de los ciberataques, considerando que una proporción significativa de estos se materializa a través de dicho servicio; por lo que se requieren lineamientos más estrictos sobre la contactabilidad, incluyendo reglas que protejan de forma efectiva al usuario final de los servicios que cursan sobre internet, tal como se mención anteriormente.

2. ENFOQUE REGULATORIO PARA MITIGAR LOS CIBER ATAQUES

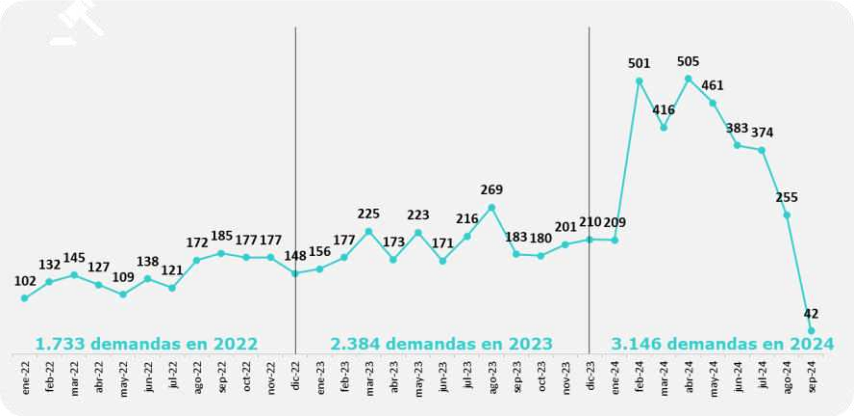
2.1 Las dinámicas de fraude cibernético trascienden el ámbito regulatorio.

El aumento de los fraudes cibernéticos no puede atribuirse a la insuficiencia de medidas regulatorias en materia de gestión y control hacia los actuales PRSTM. Por el contrario, estos ataques han surgido como una consecuencia natural del avance tecnológico y de la creciente digitalización de los servicios, motivados en muchos casos por intereses económicos, políticos o ideológicos, como el robo de dinero, la extorsión, el ciber espionaje o la desinformación; ello sin mencionar el hecho de que la tarifa de cargos de acceso por SMS que los PCA e Integradores Tecnológicos pagan a los PRSTM por el acceso a sus redes en Colombia es excesivamente baja comparada con todo el entorno regional y mundial, lo que se convierte en uno de los principales incentivos para que los fraudes cibernéticos se inicien a través de SMS por la excesiva

rentabilidad (relación costo/"beneficio") que percibirán los generadores de contenido fraudulento. En este contexto, el fraude cibernético no depende de la ausencia de normas regulatorias, pues su aparición y evolución responden a dinámicas globales complejas que exceden el campo de acción regulatorio y la velocidad en la que se emiten las normas para prevenir estos fenómenos.

Un ejemplo ilustrativo de esta situación es el sector financiero, uno de los más regulados en lo relacionado con la seguridad de la información y la protección de datos personales. Este sector cuenta con un marco normativo robusto, expedido por entidades como la Superintendencia Financiera de Colombia (SFC), que impone exigentes estándares de cumplimiento, protocolos de autenticación reforzada y mecanismos de gestión de riesgos avanzados. Sin embargo, a pesar de estas estrictas disposiciones, los ataques cibernéticos no solo persisten, sino que han venido en aumento (gráfica 3), adaptándose de forma continua a las nuevas tecnologías y a las conductas cambiantes de los usuarios.

Gráfica 3. Evolución de demandas por fraude sector Financiero.



Fuente. Superfinanciera[4].

A continuación, se exponen algunas de las disposiciones normativas[5] expedidas por la SFC que evidencian el nivel de exigencia regulatoria en este sector y que, a pesar de su existencia, no han sido suficientes para contener el incremento de incidentes de seguridad:

Norma	Concepto
Ley 1735 de 2014	Medidas servicios financieros transaccionales.
Decreto 2076 de 2017	Modificación Decreto 2555 de 2010 SEDPE.
Circular Externa 050 de 2016	Sociedades Especializadas en Depósitos y Pagos Electrónicos SEDPE.

[4] Superintendencia Financiera de Colombia. Retos importantes en seguridad y disponibilidad en el sector financiero. https://www.superfinanciera.gov.co/publicaciones/10115458/discursos-y-presentaciones-2024/
[5] https://www.superfinanciera.gov.co/publicaciones/20149/normativanormativa-generalcirculares-externas-cartas-circulares-y-resoluciones-desde-el-ano-20149/

Norma	Concepto
Resolución 0331 de 2017	Creación InnovaSFC.
Circular Externa 007 de 2018	Requerimientos mínimos para la gestión del riesgo de ciberseguridad.
Circular Externa 008 de 2018	Fortalecimiento gestión del riesgo. Pasarelas de pago.
Circular Externa 005 de 2019	Uso de Computación en la nube.
Circular Externa 006 de 2019	Seguridad y calidad para la realización de operaciones mediante códigos QR.
Circular Externa 026 de 2019	Uso de dispositivos móviles en sucursales.
Circular Externa 029 de 2019	Seguridad y calidad para la realización de operaciones y acceso e información al consumidor financiero y uso de factores biométricos.
Circular Externa 012 de 2020	Medidas preventivas para el uso de dispositivos de autenticación biométrica.
Circular Externa 027 de 2020	Instrucciones relativas a SARLAFT 4.0
Circular Externa 033 de 2020	Indicadores CS y SI
Resolución 0143 de 2020	Instrucciones InnovaSFC
Circular Externa 002 de 2021	Corresponsales.
Circular Externa 017 de 2021	Instrucciones relativas a SARLAFT 4.0
Circular Externa 020 de 2021	Sistemas de Pago de Bajo Valor.
Circular Externa 011 de 2022	Instrucciones relativas a SARLAFT 4.0
Circular Externa 005 de 2023	Operaciones que se realizan mediante el uso de códigos QR.
Circular Externa 004 de 2024	Finanzas abiertas y comercialización de tecnología e infraestructura a terceros.

Este panorama evidencia que, si bien la regulación es un componente importante en la protección contra el cibercrimen, su sola existencia no basta para frenar su evolución. La proliferación normativa, sin una estrategia integral que articule educación de los usuarios en materia de identificación y prevención de fraudes con acciones orientadas a impedir el modus operandi de ciertos actores en la cadena del fraude, no garantiza una contención efectiva del fenómeno.

En consecuencia, aunque la regulación es necesaria para establecer estándares, responsabilidades y límites, esta debe ser vista como un instrumento dentro de una estrategia más amplia, transversal y proactiva. El verdadero impacto se logra no sólo mitigando los efectos del fraude, sino previniendo su ocurrencia desde el origen. Para ello, es indispensable controlar las condiciones que permiten o incentivan la generación de acciones fraudulentas. Sólo mediante este enfoque preventivo será posible enfrentar de manera más eficaz los riesgos asociados al entorno digital.

En este sentido, hay que tener en cuenta que actualmente los operadores de telecomunicaciones prestadores de los servicios, específicamente los PRSTM que estamos obligados a otorgar el acceso a los PCA e Integradores Tecnológicos, interponemos las denuncias respectivas ante el Ministerio de TIC, SIC y la Fiscalía General de la Nación, al momento de detectar que PCA conectados a las redes presentan prácticas fraudulentas repetitivas; sin embargo, dichas

denuncias casi nunca prosperan o se dilatan en el tiempo indefinidamente, lo que implica que dichas conductas delictivas se mantengan impunes. Por el otro lado, los PRSTM igualmente informamos a la CRC periódicamente sobre ciertos integradores y PCA que realizan repetitivamente estas prácticas, sin embargo, por la protección del régimen de acceso, no es posible tomar medidas de control, como la desconexión en la prestación del acceso, o al menos la suspensión unilateral de los códigos a través de los cuales se materializan las conductas fraudulentas; contrario a ello, ante el intento de proteger a los suscriptores de nuestra red móvil se reciben de la CRC la imposición de medidas de control restrictivas a TIGO y liberadoras de la responsabilidad que debería corresponderle a los PCA y sus Integradores tecnológicos, y/o, por parte el MinTIC requerimientos de inicio de indagaciones o investigaciones que incluso han terminado en sanciones a TIGO por intentar proteger su red y sus usuarios y sin que a la fecha se conozca actuación alguna que tenga como consecuencia sancionar a los PCA y sus integradores que son los verdaderos responsables del tráfico que envían hacia la red móvil. Mas grave aún es que, de forma por lo menos desconsiderada, los PCA se escudan en argumentar que son sus clientes finales los responsables del contenido y por su parte los Integradores Tecnológicos (que en ocasiones son también PCA que fungen como integradores) se escudan a su vez en argumentar que son los PCA los responsables, quedando así entre ambos diluida su responsabilidad y sin consecuencias.

Por lo anterior, instamos a que antes de pensar en medidas adicionales, la CRC genere el fortalecimiento de la colaboración interinstitucional entre SIC, Fiscalía, Ministerio TIC y Operadores para lograr que las denuncias que se presenten lleguen a sanciones efectivas en contra de PCA y sus integradores tecnológicos quienes, valga advertirlo, son dentro de esa industria un grupo reducido, ya identificado y que desarrollan sistemáticamente estas actividades fraudulentas.

Como consecuencia de lo anterior, los PRSTM también somos víctimas de estas prácticas fraudulentas al ser el medio para la comisión de los diferentes delitos, lo que nos hace no solo destinatarios del control por ser el medio a través del cual se ejercen las acciones delictivas, sino que también requerimos de la intervención oportuna de las entidades de vigilancia y control. Se reitera que desde TIGO ya se han realizado, además de las denuncias relacionadas con los PCA y su Integrador, otro tipo de acciones ante la Fiscalía General de la Nación.

2.2 Regulación asimétrica con menores cargas para los PCA e IT frente a su responsabilidad en el tráfico fraudulento.

A propósito, según las cifras presentadas por la Comisión en el documento soporte, en 2024 se reportaron 570.144 incidentes de fraude cibernético por la modalidad de smishing, de un total de 587.573 casos (Tabla1). Esto representa un 97% del total de incidentes detectados por las empresas que participaron del requerimiento de información, lo que evidencia que esta modalidad concentra la mayoría de los ataques. Se reitera aquí que una de las principales

razones de que este sea actualmente el medio preferido para la comisión de fraude cibernético a través de servicios móviles es que la tarifa de cargos de acceso por SMS que los PCA e Integradores Tecnológicos pagan a los PRSTM por el acceso a sus redes en Colombia es excesivamente baja comparada con todo el entorno regional y mundial, lo que se convierte en uno de los principales incentivos para que los fraudes cibernéticos se inicien a través de SMS por la excesiva rentabilidad (relación costo/"beneficio") que percibirán los generadores de contenido fraudulento. Esta realidad representa una oportunidad clara para focalizar los esfuerzos regulatorios, técnicos y educativos en esta tipología, con el fin de lograr avances sustantivos en la lucha contra este flagelo.

Tabla 1. Cantidad de incidentes de fraude cibernético detectados por las empresas.

Modo de Fraude	2022	2023	2024
Smishing	40.902	259.973	570.144
Vishing	2.291	3.552	17.429
Total	**43.193**	**263.525**	**587.573**

Fuente: Requerimiento de información de la CRC sobre el fraude cibernético por medio de llamadas de voz o mensajes cortos de texto.

Ante esta problemática, resulta pertinente señalar la existencia de asimetrías regulatorias entre los PRSTM y los PCA o IT, las cuales ameritan una revisión cuidadosa. Un ejemplo claro de esta diferencia se encuentra en la Resolución CRC 5050 de 2016, donde en sus artículos 2.1.10.7 y 2.9.2.3 se establece que los PRSTM deben implementar herramientas tecnológicas y modelos de seguridad orientados a la autenticación, el acceso, la confidencialidad y la integridad de los datos, con el fin de garantizar la seguridad de la red y la inviolabilidad de las comunicaciones.

En contraste, a los PCA en el artículo 2.1.18.6 únicamente se les exige el uso de herramientas tecnológicas para la prevención de fraudes y el seguimiento de su efectividad, sin que se impongan requerimientos equivalentes en términos de alcance o estándares de seguridad. Esta diferencia evidencia una carga regulatoria más exigente para los PRSTM, pese a que el origen de muchas modalidades de fraude cibernético se encuentra precisamente en el presunto uso indebido de canales por parte de estos actores.

En este sentido, incrementar la carga regulatoria sobre los PRSTM, sin duda alguna, no necesariamente contribuirá a la mitigación de los fraudes cibernéticos. Tal como se ha mencionado anteriormente, los PRSTM actúan como canal de comunicación de los mensajes generados por terceros, y por disposición legal no tienen la posibilidad de inspeccionar ni controlar el contenido de dichos mensajes, en cumplimiento del principio de inviolabilidad de las comunicaciones.

Cabe destacar que los PRSTM han venido cumpliendo con las múltiples obligaciones regulatorias que les son aplicables, tales como garantizar el acceso a redes, velar por la ciberseguridad en sus redes de acuerdo con las disposiciones establecidas en la Resolución CRC 5569 de 2018 y asegurar el mantenimiento adecuado de su infraestructura, incluyendo la suspensión del servicio

en caso de fallas o daños que lo ameriten. En este contexto, resulta importante reconocer que el cumplimiento de estos deberes ya representa una responsabilidad significativa para los PRSTM, con los costos que ello ha implicado.

Por lo anterior, de manera respetuosa, sugerimos que la Comisión considere enfocar sus esfuerzos en el fortalecimiento de los mecanismos de control relacionados con la asignación y el uso de códigos cortos por parte de los PCA. Esto implica revisar y limitar la cantidad de recursos asignados a cada operador, así como establecer requisitos más rigurosos para su otorgamiento, especialmente en los casos en los que existan antecedentes de fraude asociados a códigos previamente asignados, los cuales deberían inhabilitar nuevas asignaciones.

También se considera necesario que el régimen aplicable a PCA contemple obligaciones específicas en materia de prevención de fraudes y riesgos asociados al lavado de activos y financiación del terrorismo (LA/FT). Dado que los PCA son los encargados de distribuir los recursos de identificación (Códigos y Numeración) que le son asignados por la CRC a terceros – sus clientes -, sin que medie necesariamente una relación contractual entre estos terceros y un operador tradicional; por lo tanto, se hace indispensable exigir a los PCA y a los Integradores Tecnológicos, en igual medida, prácticas empresariales responsables, incluyendo procesos de debida diligencia, verificación de antecedentes y trazabilidad del uso de los recursos asignados. Adicionalmente, se debería analizar la viabilidad de establecer un marco de corresponsabilidad, tanto para el PCA como para su Integrador Tecnológico (cuando el PCA recurra a esta figura) sobre el contenido de los mensajes cursados, especialmente cuando se usen recursos de numeración asignados por el PCA para fines ilícitos o abusivos, como el fraude, el spam comercial no autorizado o el phishing. Esta medida permitiría cerrar brechas de control frente a la explotación de recursos críticos como la numeración, cuya administración responsable es fundamental para la seguridad del ecosistema digital.

Asimismo, sería pertinente ajustar los procedimientos de recuperación de estos recursos en casos donde se detecte un uso indebido, incluyendo medidas preventivas y correctivas más eficaces. Entre ellas, que ante la notificación de un tercero de mensajes fraudulentos con la evidencia correspondiente, el operador de red este habilitado para proceder con el bloqueo inmediato del código en cuestión y paralelamente informar a la CRC para que pueda iniciar la investigación correspondiente.

Igualmente, resulta importante definir consecuencias claras, proporcionadas y disuasorias frente a conductas reiterativas o malintencionadas. Una propuesta seria permitir la terminación unilateral de la relación de acceso y proceder con su desconexión, o ante casos repetitivos de fraude que involucren a varios operadores de telecomunicaciones la posibilidad de suspender temporalmente al PCA, hasta tanto se concluya la investigación del uso fraudulento o no de los códigos cortos.

2.3 Liberación del servicio SMS A2P de la lista de mercados relevantes.

Como se ha señalado en distintos espacios, consideramos necesario que la Comisión revise integralmente el servicio de mensajería de texto corto (SMS), diferenciando los impactos asociados a su oferta en las modalidades A2P (Application to Person) y P2P (Person to Person). La creciente relevancia del fenómeno del smishing hace indispensable que cualquier análisis regulatorio parta de una caracterización precisa de la oferta que presenta mayores riesgos, en este caso, la modalidad A2P.

Este análisis cobra especial importancia si se tienen en cuenta los antecedentes regulatorios. En el año 2009, mediante el análisis que sustentó la expedición de la Resolución CRT 2058 de 2009, la CRC concluyó que el mercado de *"voz saliente móvil"* incluía tanto las llamadas móviles como los mensajes cortos de texto (SMS) y mensajes multimedia (MMS), en virtud de su agrupación como un *"clúster"* en el que los usuarios típicamente contratan servicios móviles para realizar y recibir tanto llamadas como mensajes de texto.

No obstante, con el avance del ecosistema digital, este supuesto de mercado ha evolucionado. En el 2022, durante el desarrollo del proceso que culminó con la expedición de la Resolución CRC 7007, la Comisión reconoció las diferencias entre los mensajes P2P y A2P, y adoptó metodologías de remuneración diferenciadas para los cargos de acceso: una para los intercambios entre PRSTM (mensajes P2P) y otra para los mensajes enviados entre PRSTM y PCA o IT (mensajes A2P). Sin embargo, dicha diferenciación se sustentó únicamente en observaciones de los grupos de interés, sin que se desarrollara un análisis estructural de mercado o de riesgos asociados.

En este contexto, es importante señalar que el envío de mensajes SMS a través de PCA o IT corresponde a un servicio masivo y automatizado, cuyas características difieren sustancialmente del servicio P2P que opera bajo condiciones típicas de usuario final. Por ello, consideramos que los mensajes A2P no deberían incluirse dentro del mercado minorista *"voz saliente móvil"*, dada su naturaleza distinta en términos de propósito, comportamiento del consumidor y nivel de riesgo.

En consecuencia, proponemos a la Comisión analizar la exclusión del servicio A2P del mercado relevante *"voz saliente móvil"* y avanzar hacia una diferenciación clara entre los servicios SMS P2P y A2P, más aun considerando que la problemática del smishing se concentra de forma abrumadora en la modalidad A2P.

Esta diferenciación permitiría adoptar medidas regulatorias más focalizadas y eficaces, sin trasladar cargas innecesarias a los actores que no están directamente vinculados con la generación de los riesgos identificados.

Se insiste en que una de las principales razones de que los SMS A2P sean actualmente el medio preferido para la comisión de fraude cibernético a través de servicios móviles es que la tarifa de cargos de acceso por SMS que los PCA e Integradores Tecnológicos pagan a los PRSTM por el

acceso a sus redes en Colombia es excesivamente baja comparada con todo el entorno regional y mundial, lo que se convierte en uno de los principales incentivos para que los fraudes cibernéticos se inicien a través de SMS por la excesiva rentabilidad (relación costo/"beneficio") que percibirán los generadores de contenido fraudulento. Por ello un trato diferenciado de los SMS P2P, e incluso una liberación del techo tarifario de los cargos de acceso para los mensajes A2P podría generar una corrección del mercado distorsionado por la tarifa de esos cargos de acceso y que, como lo hemos dicho, incentiva y propicia el tráfico fraudulento.

2.4 La regulación requiere herramientas específicas para la prevención de técnicas de fraude mediante llamadas de voz.

En relación con modalidades de fraude como el Vishing, es importante destacar las tácticas utilizadas por los ciberdelincuentes, que incluyen la "suplantación de identidad", donde los estafadores se hacen pasar por entidades bancarias, empresas de telecomunicaciones o proveedores de servicios, con el objetivo de ganar la confianza de las víctimas. Estas tácticas también incluyen llamadas de "emergencia", diseñadas para generar una sensación de urgencia y presionar a la víctima a actuar rápidamente sin reflexionar, así como técnicas de manipulación psicológica para inducir confianza y lograr que las personas compartan información confidencial.

Estas prácticas dependen en gran medida de la capacidad del usuario para detectar que está siendo víctima de un fraude y, así, evitar compartir datos sensibles. Sin embargo, existen otras tácticas como las llamadas automatizadas o "robocalls", en las cuales se utilizan sistemas automatizados para realizar llamadas masivas. Aunque las llamadas automatizadas pueden ser utilizadas legítimamente por empresas para campañas de telemarketing o para brindar información relevante, se vuelve preocupante cuando se emplean con fines fraudulentos. Por ejemplo, algunas empresas emplean tácticas de "llama y cuelga" para perfilar las líneas telefónicas y determinar cuáles son atendidas por personas reales, lo que luego se utiliza para lanzar campañas de fraude o para vender estas bases de datos a terceros con fines lícitos y desafortunadamente también ilícitos.

2.5 Marco regulatorio para la protección de los derechos de los usuarios ante riesgos de fraude en plataformas digitales.

Conforme a lo establecido en el artículo 19 de la Ley 1341 de 2009, uno de los principales deberes de la CRC es garantizar la protección de los derechos de los usuarios. En el mismo marco, el artículo 2 de dicha ley señala que el Estado velará por la adecuada protección de los derechos de los usuarios de las Tecnologías de la Información y las Comunicaciones (TIC), así como por el cumplimiento de los derechos y deberes derivados del Hábeas Data en el contexto de la prestación de los servicios.

Acá es importante reconocer que los usuarios de las TIC no solo reciben un servicio de conectividad, sino que también reciben servicios y contenido digital a través de diversas

plataformas digitales. Hasta el momento, el enfoque del regulador se ha centrado principalmente en regular a los proveedores de conectividad, mientras que la regulación sobre contenidos ha sido más limitada, principalmente relacionada con el servicio de televisión tradicional y buscando proteger a los usuarios de contenido inapropiado. Sin embargo, hoy en día, el panorama ha cambiado significativamente con la expansión de los servicios OTT, que incluyen plataformas como WhatsApp, Messenger, YouTube, y otras aplicaciones de mensajería y video. Estas plataformas, en su mayoría, carecen de una regulación clara que brinde protección adecuada a los usuarios respecto al contenido que consumen.

En este sentido, es crucial que el regulador empiece a evaluar y, en su caso, regular el contenido ofrecido a través de los proveedores de contenido y plataformas OTT. Dentro de las actividades ilícitas que se realizan a través de plataformas como WhatsApp, se encuentran casos donde los ciberdelincuentes emplean tácticas de suplantación de identidad o envían enlaces maliciosos para robar información personal (phishing), lo que puede derivar en fraudes o extorsiones.

Además, las videollamadas se han convertido en un vehículo para ejecutar fraudes a través de engaños, como falsas ofertas de empleo, que tienen como objetivo no solo obtener acceso a información personal, sino también manipular a las víctimas para realizar pagos o compartir datos bancarios sensibles[6].

Por lo anterior, dada la evolución de las plataformas de comunicación y la aparición de nuevas amenazas digitales, es esencial que la CRC amplíe su enfoque regulador para incluir los servicios OTT y otros canales digitales que hoy están en el centro de la actividad fraudulenta y que es materializada a través del servicio de internet. Mediante una regulación adecuada y la implementación de medidas preventivas podremos garantizar la protección efectiva de los usuarios frente a los riesgos asociados con el uso de estas tecnologías. La regulación debe adaptarse a los nuevos desafíos, asegurando que los derechos de los usuarios estén protegidos en un entorno digital cada vez más complejo y vulnerable.

Este tema se ha venido evaluando mundialmente en específico, se pueden citar los siguientes estudios de fuentes oficiales:

- Informe de la Unidad Fiscal Especializada en Ciberdelincuencia (Ufeci), Argentina (2024): Este informe oficial documenta un récord de 34,468 reportes de ciberdelitos, con más de 5,500 casos vinculados a WhatsApp, especialmente por fraudes y usurpación de identidad mediante acceso ilegítimo a cuentas. Además, destaca el aumento significativo en casos de violencia digital[7].

[6] https://www.lafm.com.co/tecnologia/modalidad-de-estafa-por-videollamada-de-whatsapp-asi-lo-roban-en-segundos
[7] https://www.lanacion.com.ar/seguridad/ciberdelitos-en-alza-record-de-denuncias-whatsapp-como-blanco-principal-y-crecen-los-casos-de-nid30062025/

- Estudio y predicciones de BTR Consulting (2024-2025): Firma global que hizo un informe titulado Predicciones 2025, en el que se describen tendencias crecientes del cibercrimen a nivel global, incluyendo ataques mediante plataformas de mensajería las plataformas más utilizadas para realizar estafas fueron WhatsApp, Telegram, Instagram, TikTok y Facebook. Los delincuentes suelen crear mensajes personalizados relacionados con problemas financieros, como supuestas deudas, ayudas económicas o emergencias; señala el aumento del ransomware, uso de inteligencia artificial para estafas, y el impacto en generaciones más jóvenes.

- Informe de Group-IB sobre delitos tecnológicos 2025: Reporta el crecimiento significativo de ciberataques avanzados (APT), aunque no exclusivamente enfocado en mensajería, aporta contexto a la evolución del ciberdelito tecnológico global.

- Análisis de Keeper Security sobre canales de mensajería en 2024: Documento que destaca que WhatsApp y Telegram son vectores importantes de phishing y fraudes mediante mensajes maliciosos que suplantan entidades financieras para engañar a usuarios.

- Informe Sofistic (2025)[8] explora las vulnerabilidades a las que se están vieestas las empresas actualmente y cuales medidas deberían tomarse ante el ataque desmedido de ciberdelincuentes.

3. MESAS DE TRABAJO CONJUNTAS.

Proponemos, realizar mesas de trabajo conjuntas con La Fiscalía General de la Nación, el Ministerio de TIC y de Defensa, la CRC, la Superintendencia de Comercio – SIC desde las delegaturas de protección de los datos personales y la delegatura de protección al consumidor, la Superintendencia Financiera de Colombia – SFC, los PRSTM, PCA, y los demás actores que consideren interesados con el fin de revisar un esquema de senda de reducción que permita reducir el fraude cibernético móvil, articulando capacidades institucionales, compartiendo información estratégica y adoptando medidas coordinadas y progresivas que habiliten respuestas más eficaces frente a este fenómeno creciente, al tiempo que se fortalece la confianza del usuario en los servicios digitales y se promueve un entorno más seguro para las transacciones electrónicas.

CONSULTA PÚBLICA.

1. Sobre el problema planteado:

[8] https://cuatroochenta.com/landings/tendencias-ciberseguridad/

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.

RTA. De acuerdo con lo señalado en los comentarios generales, consideramos que la definición del problema no aborda de manera integral la problemática del fraude cibernético.

En primer lugar, el alcance planteado se encuentra limitado a los servicios tradicionales de voz y mensajes de texto, sin considerar de forma adecuada la totalidad de los servicios que conforman el mercado relevante de "servicios móviles". En este sentido, resulta fundamental incluir el servicio de internet móvil en el análisis regulatorio, dado que este medio es ampliamente utilizado para la ejecución de fraudes cibernéticos y, por tanto, constituye un factor clave en la materialización de estos incidentes.

En segundo lugar, consideramos que el problema no radica en la ausencia de herramientas regulatorias porque como ya se indicó al principio de la comunicación, ya se han contemplado algunas de orden legal y regulatorio, sino en incorporar herramientas específicas y establecer consecuencias claras por su no implementación y/o aplicación. Un ejemplo de ello es el artículo 2.1.18.6 de la Resolución 5050 de 2016, que establece la directriz para que los PCA e IT utilicen herramientas tecnológicas para prevenir fraudes a través del envío de SMS. Sin embargo, no se tiene claridad sobre si estas herramientas están siendo efectivamente implementadas. Además, la norma no contempla mecanismos para que las autoridades de vigilancia y control tomen acciones ante la falta de implementación de estas medidas.

En tercer lugar, la "ausencia de normas" no es un problema en sí mismo, es una de las causas del problema al que se enfrentan los usuarios de los servicios de SMS, voz y datos móviles, así como los PRSTMs que están obligados a proveer el acceso a los PCAs e Integradores Tecnológicos, quienes son la fuente del tráfico presuntamente fraudulento que se origina desde sus clientes finales, y al mismo tiempo los PRSTMs están obligados a responder por cargas regulatorias de responsabilidad similares a las de los originadores de ese tráfico

Profundizando un poco más en nuestra afirmación de que la "ausencia de normas" no es un problema en sí mismo, manifestamos también que es la responsabilidad difusa de que adolecen las normas existentes entre lo que atañe a los PCAs y lo que le atañe a sus Integradores Tecnológicos, lo que propicia también la proliferación del fraude cibernético a través de algunos de estos agentes.

En cuarto lugar, no se observa que el planteamiento del problema esté abordando una de las causas estructurales que propicia que los SMS sean actualmente el medio preferido para la comisión de fraude cibernético a través de servicios móviles, y es el correspondiente a que la tarifa de cargos de acceso por SMS que los PCA e Integradores Tecnológicos pagan a los PRSTM por el acceso a sus redes en Colombia es excesivamente baja comparada con todo el entorno regional y mundial, lo que se convierte en uno de los principales incentivos para que los fraudes cibernéticos se inicien a través de SMS por la excesiva rentabilidad (relación costo/"beneficio") que percibirán los generadores de contenido fraudulento.

En este contexto, sugerimos revisar y replantear la definición del problema, de manera que refleje adecuadamente los factores estructurales involucrados. A continuación, presentamos una propuesta de redacción para tal fin.

> *"El contexto actual requiere que la regulación incorpore herramientas específicas para reducir el riesgo de fraude cibernético ejecutados a través de los servicios móviles frente a los cuales aún no existen lineamientos de intervención directa."*

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.

RTA. Conforme a la respuesta anterior, es necesario realizar una reconsideración de las causas que impulsan la problemática de fraude cibernético en las redes móviles.

Al respecto, planteamos algunas causas que pueden estar ocasionando la problemática expuesta:

- **Falta de herramientas para realizar un debido control y vigilancia de los recursos de identificación por parte del administrador y entidades de vigilancia y control.**
    - **Asignación de códigos cortos:** Actualmente, se han identificado casos en los que ciertos proveedores continúan accediendo a nuevos códigos cortos, aun cuando han estado involucrados en investigaciones por presunto uso indebido o fraude asociado a estos recursos. Esta situación genera preocupación en términos de control y prevención del uso fraudulento. En este sentido, consideramos que, en aras de fortalecer la confianza en el ecosistema digital, la Comisión debería evaluar

mecanismos más estrictos para la asignación de estos recursos. En particular, podría contemplarse la posibilidad de restringir la asignación de nuevos códigos a los PCA que presenten reiteración en comportamientos asociados a prácticas fraudulentas, de acuerdo con los principios de uso eficiente y seguro de los recursos de numeración. Dado que es posible que se cree una nueva razón social con el fin de continuar con prácticas indebidas previamente identificadas, se sugiere que, al momento de asignar recursos de numeración, se evalúe la composición accionaria de la empresa solicitante. Esto permitiría verificar si existen vínculos con personas naturales o jurídicas previamente asociadas a conductas irregulares, y así evitar que los mismos actores reincidan en dichas prácticas bajo una nueva estructura empresarial.

- **Recuperación de códigos cortos.** De igual forma, es necesario optimizar los procedimientos asociados a la recuperación de códigos cortos en los casos en donde se identifiquen usos indebidos. Uno de los principales retos actuales es la duración del proceso investigativo por parte de la Comisión, durante el cual el PCA puede continuar utilizando el código presuntamente comprometido, aumentando el riesgo de afectaciones a los usuarios.

  Como PRSTM, hemos puesto en conocimiento el uso indebido de códigos cortos, los cuales, de manera presunta, están siendo empleados para actividades fraudulentas. Un ejemplo de ello fue el reporte del código 85949 reportado a la CRC el 3 de mayo de 2023, junto con la respectiva denuncia en la Fiscalía. El 2 de julio de 2025 se efectuó un nuevo reporte a la CRC indicando que dicho código sigue activo y continúa utilizándose con fines inapropiados. A pesar de haber transcurrido aproximadamente dos años, la CRC aún no ha tomado medidas al respecto. Entendemos que los procesos de atención pueden ser complejos, pero sería muy beneficioso ajustar los procedimientos para que las acciones puedan tomarse de manera más oportuna, protegiendo así a los usuarios de posibles fraudes.

- **Ausencia de herramientas especificas regulatorias para que los PRSTM implementen acciones preventivas y colaborativas que puedan mitigar el fraude cibernético.** Es urgente que la Comisión adopte medidas más contundentes para enfrentar el creciente uso del canal SMS con fines fraudulentos y que los PRSTM como contacto directo del usuario tengamos herramientas para mitigar estas acciones.

En este sentido, sugerimos que en casos en los que se identifique una reiteración de estas prácticas por parte de un mismo PCA o IT, se debería habilitar la posibilidad al PRSTM de dar por terminada la relación de acceso y proceder con su desconexión de la red del operador. Esta acción contribuiría a desincentivar la reincidencia de este tipo de prácticas.

- **Desconocimiento de los usuarios sobre las modalidades de fraude cibernético y como ellos se constituyen en un pilar clave para mitigar este flagelo.** Uno de los retos actuales en la lucha contra el fraude cibernético es el limitado conocimiento que muchos usuarios tienen sobre las diferentes modalidades de ataque y sobre el papel tan importante que ellos mismos pueden desempeñar en su prevención. Consideramos valioso promover una mayor conciencia sobre estas prácticas, así como orientar a los usuarios respecto a sus deberes y pasos a seguir cuando se enfrentan a situaciones de posible fraude.

  La experiencia demuestra que muchos ataques cibernéticos no tendrían éxito si el usuario actuara de forma informada y consciente frente a señales de alerta. En este contexto, la educación y sensibilización del usuario se convierte en una herramienta tan importante como la regulación o la tecnología para la contención del fraude cibernético.

  Por lo anterior, sugerimos que la Comisión, en su calidad de entidad reguladora y como administrador de los espacios institucionales en los canales de televisión abierta que cuentan con amplia capacidad de divulgación, impulse campañas pedagógicas que informen de forma clara, práctica y accesible a los ciudadanos las situaciones a las que pueden verse enfrentados y cómo actuar ante estas.

  Asimismo, se le indique al usuario que la CRC tiene facultades para suspender el uso de los códigos cortos desde donde están siendo objeto de ataques. De esta forma, los usuarios podrían reportar estas acciones ante la CRC para que se tomen medidas al respecto. En este sentido, sugerimos a la CRC habilitar un canal directo para que los usuarios realicen las denuncias.

- **Las obligaciones regulatorias recaen sólo sobre unos actores de la cadena de valor, son asimétricas y en otros casos difusas.** Al analizar el marco regulatorio vigente, se evidencia un enfoque en el que las obligaciones más estrictas y las consecuencias más gravosas recaen principalmente sobre los PRSTM, quienes están obligados a otorgar el acceso sin importar las calidades o el comportamiento de los PCAs y sus Integradores Tecnológicos que se lo solicitan. Si bien estos actores cumplen un rol clave en la cadena de prestación del servicio, es importante señalar que en el caso de TIGO, productos de bolsas de mensajes, por ejemplo, han sido eliminadas del portafolio comercial, por tanto, la

responsabilidad en la prevención del fraude cibernético debe radicar en los PCA e Integradores, que son los que en mayor medida comercializan este tipo de servicios hacia terceros.

En este sentido, consideramos necesario que la Comisión revise y ajuste las cargas regulatorias, promoviendo una mayor equidad y haciendo más vinculantes las obligaciones para los otros agentes, como los PCA y los IT, e incluso obligando a que las cargas y responsabilidades que tienen que asumir sean exactamente las mismas entre ellos, porque la realidad es que con el marco normativo actual algunos PCAs y sus respectivos Integradores soslayan sus responsabilidades, los unos (algunos PCAs) alegando que son sus clientes finales los que generan el contenido fraudulento y los otros (sus Integradores) argumentando que son los PCAs los responsables del contenido . Así entonces solicitamos que las revisiones y ajustes que haga la CRC a la normatividad estén enfocados en que todos los actores tengan una participación activa, coherente y corresponsable en la implementación de medidas para combatir este tipo de amenazas. Fortalecer las obligaciones regulatorias de estos actores permitirá una respuesta más efectiva y articulada frente al fraude cibernético.

- **Contacto sin el consentimiento previo y explícito de los usuarios.** Es necesario precisar que el consentimiento otorgado a un PRSTM no puede extenderse a todos los actores que intervienen en la cadena de valor de la comunicación por SMS, llamadas y correos electrónicos, y es necesario que cada actor gestione las respectivas autorizaciones. Esto incluye no sólo a las entidades originadoras de los mensajes, sino también a sus socios comerciales, PCA, los integradores tecnológicos y proveedores de contenido OTT.

- **Escasa coordinación entre PRSTMs, la CRC, la SIC y las demás entidades y autoridades que intervienen en la prevención, vigilancia y control de fraudes cibernéticos.** Aunque estos actores tienen funciones complementarias en materia de vigilancia, protección al usuario, ciberseguridad y regulación, actualmente no se cuenta con protocolos conjuntos de actuación ni mecanismos interoperables para el reporte, análisis y respuesta frente a estos eventos. Esta fragmentación institucional debilita la capacidad del ecosistema para identificar patrones emergentes, generar alertas tempranas y actuar de forma articulada, lo que retrasa la prevención y contención efectiva de los fraudes que utilizan servicios de comunicaciones como canal de contacto.

- **La regulación focaliza sus esfuerzos en los servicios de conectividad, mientras que la regulación relacionada con servicios sobre contenidos mediante plataformas digitales es limitada.** Como se mencionó en el numeral 2.5 en los comentarios generales, la baja intervención regulatoria sobre

contenidos digitales esta generando un impacto sobre los derechos y protección de los usuarios, y para este caso concreto, se están viendo impactados por las modalidades de fraudes que se están ejecutando a través de plataformas OTT de mensajería y video.

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.

RTA. Conforme a lo expuesto en la respuesta al literal 1a, consideramos pertinente que se revalúe el enfoque actual sobre las consecuencias derivadas de la problemática del fraude cibernético en las redes móviles, donde, si bien las consecuencias señaladas en el documento pueden representar un primer acercamiento, es importante profundizar en ellas para reflejar de forma más completa la dimensión del problema considerando incluir el impacto causado en el servicio de internet móvil.

Adicionalmente, se plantea incluir la siguiente consecuencia:

- **Crecimiento sostenido de las modalidades de fraude dirigidos a los usuarios a través de los servicios móviles.** Si bien se observa una problemática pronunciada en los casos de fraude por la modalidad de smishing, esta no es la única modalidad que genera consecuencias, Modalidades como el “Robocall”, están generando un impacto relevante en las empresas y usuarios. Asimismo, al incluir el servicio de internet móvil en el alcance del proyecto, se pueden abordar de una forma más amplia las medidas para los casos de phishing y otras modalidades que se presentan sobre el servicio de internet.

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.

RTA. Consideramos que existen otros grupos de valor que deberían ser tenidos en cuenta en el desarrollo del presente proyecto regulatorio, especialmente si se busca una estrategia integral y sostenible de mitigación de este flagelo a todos los actores que intervienen en las redes móviles. En la lista de grupos de valor falto incluir:

1. **OTT:** Estos actores juegan un papel fundamental en el ecosistema de seguridad cibernética, ya que diversas modalidades de fraude, especialmente aquellas basadas en ingeniería social se ejecutan a través de sus plataformas. Actualmente, las campañas de phishing no se limitan únicamente a los mensajes de texto (SMS), sino que también se propagan mediante aplicaciones de voz y mensajería de texto en aplicaciones como WhatsApp, Telegram y Messenger. Por tanto, es clave incluir a estos proveedores en las estrategias integrales de prevención, detección y reacción frente al fraude cibernético relacionadas con patrones de comportamiento, suplantación de identidad, canales de verificación, entre otros.

2. **Entidades del ecosistema de ciberseguridad del Estado.** Aunque la CRC tiene un rol claro en la regulación del servicio y la protección de los derechos de los usuarios, el fenómeno del fraude cibernético también involucra aspectos de persecución penal, prevención digital y análisis forense, que son competencia de otras autoridades. Incluir a actores como el Centro Cibernético de la Policía Nacional, la Fiscalía General de la Nación, ColCERT del MinTIC, y eventualmente la UIAF, permitiría fortalecer los canales de intercambio de información, construir alertas tempranas y mejorar la trazabilidad de eventos.

3. **Titulares de datos y representantes de derechos digitales.** Las personas afectadas no siempre son técnicamente "usuarios" de los operadores móviles. Muchas veces el fraude alcanza a ciudadanos sin una relación contractual directa (niños, adultos mayores, turistas, etc.), lo que justifica involucrar a asociaciones de consumidores, defensores de derechos digitales, y expertos en protección de datos personales, para garantizar un enfoque centrado en las personas, con especial énfasis en los grupos más vulnerables.

   El fenómeno del fraude cibernético es multidimensional y transinstitucional, por lo que la inclusión de estos grupos de valor no solo es deseable sino necesaria para asegurar la coherencia, eficacia e interoperabilidad del marco regulatorio que se está construyendo. Una visión sistémica del problema permitirá diseñar intervenciones más robustas, sostenibles y alineadas con el interés público.

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

a) <u>En relación con el uso indebido de la numeración de códigos cortos:</u>

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?

RTA. Consideramos que la medida propuesta seria efectiva si el registro de remitentes incluye la razón social de la empresa o persona natural que contrató el envío de los mensajes, es decir, dentro de los eslabones de la cadena de valor que presento la Comisión, la información debe corresponder a la Entidad Originadora. Esta información es clave para que los PRSTM, los usuarios y las autoridades puedan identificar al verdadero remitente y, en caso de detectarse prácticas fraudulentas, replicar acciones o tomar medidas directamente contra el responsable del envío.

Actualmente se han observado casos donde ni siquiera el PCA puede identificar el remitente del mensaje. Incluir esta trazabilidad en el registro fortalecería los mecanismos de control y responsabilidad, y contribuiría de forma más eficaz a mitigar el uso indebido de este canal.

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?

RTA. Consideramos que incluir la numeración no geográfica en un registro de remitentes para prevenir el uso indebido de códigos cortos, por si sola, no representa una medida que aporte valor a combatir la modalidad de fraude smishing. Esta medida combinada con la prohibición de la reventa de la numeración tendría un efecto más relevante. No obstante, al igual que la respuesta anterior, el registro de remitentes debe incluir la razón social de la empresa o persona natural que contrató el envío de los mensajes.

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?

RTA. Si bien la medida podría tener un impacto directo en los casos de smishing, desde TIGO consideramos que esta propuesta podría generar dos impactos negativos.

En primer lugar, esta medida podría comprometer la funcionalidad y sostenibilidad económica del servicio de mensajes cortos (SMS), particularmente en su uso masivo. Esta restricción podría desincentivar su adopción por parte de actores del mercado, especialmente pequeñas y medianas empresas, que ven en el SMS una alternativa asequible frente a otros canales de difusión más costosos.

La medida podría traducirse en una menor demanda del servicio, debilitando su viabilidad comercial.

En segundo lugar, esta medida impactaría directamente en los beneficios que reciben los usuarios, al limitar su acceso a información útil y oportuna. Dado que los mensajes de texto tienen un número restringido de caracteres, la inclusión de enlaces URL se convierte en una herramienta clave para ofrecer contenidos ampliados, detallados y personalizados. Estos enlaces permiten a los usuarios acceder a promociones, actualizaciones, servicios o trámites relevantes de manera rápida y sencilla. Restringir esta funcionalidad podría afectar negativamente su experiencia, reduciendo el valor agregado del servicio y limitando su capacidad para tomar decisiones informadas o acceder a beneficios ofrecidos por diferentes entidades.

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?

RTA. Consideramos que la prohibición de la intermediación del uso del código corto constituye una medida adecuada, en la medida en que se orienta a mitigar una modalidad de fraude que se ha presentado justamente a través de la reventa y uso indebido de este tipo de numeración ante las dificultades que representa identificar el responsable de la acción fraudulenta. De esta manera, el remitente sería el responsable del uso del código corto y del contenido de los mensajes.

Adicionalmente, teniendo en cuenta que este tipo de numeración es un recurso escaso, estimamos pertinente considerar la posibilidad de combinar este esquema con el uso de numeración E.164 no geográfica de servicios atribuida en el NDC 940, lo cual permitiría ampliar la disponibilidad de numeración sin comprometer la trazabilidad, seguridad y control que se busca con la medida propuesta.

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?

RTA. En línea con lo señalado previamente, consideramos que la propuesta permitiría ampliar la disponibilidad de recursos de numeración para servicios de mensajería de texto, lo cual resulta positivo para atender la demanda de este tipo de servicio. No obstante, es importante precisar que dicha numeración no debería habilitarse para su uso en plataformas de voz, a fin de preservar su propósito específico.

Adicionalmente, coincidimos en la necesidad de establecer reglas claras y estrictas que garanticen la exclusividad en el uso del recurso, imponer al remitente la responsabilidad de la integridad del contenido, así como la prohibición expresa de su compartición o reventa. Esta medida, en particular, se perfila como la herramienta más efectiva para prevenir y reducir los eventos fraudulentos que se han identificado en torno al uso de numeración corta.

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.

RTA. La propuesta de establecer reglas de exclusividad en el uso de la numeración y prohibir su reventa es una medida necesaria para enfrentar los riesgos asociados al uso fraudulento de este recurso escaso. No obstante, para que esta acción sea realmente efectiva, debe complementarse con mecanismos de control más robustos aplicables tanto a los PCA como a los Integradores Tecnológicos. Ambos actores deben estar sujetos al mismo nivel de responsabilidades y obligaciones, dado su rol activo en la distribución del contenido e imponerles la obligación de validar la existencia y representación de las personas naturales o jurídicas (Clientes) que serían usuarios y remitentes de los mensajes

En este sentido, resulta indispensable que se establezcan consecuencias claras frente al uso indebido de numeración, como que en casos de reincidencia o afectaciones graves, rechazar de plano las nuevas solicitudes de asignación de códigos cortos y la revocación de la licencia del operador responsable.

Asimismo, debe quedar claramente definido que la responsabilidad sobre el contenido recae exclusivamente en el PCA y el IT, quienes deben garantizar su

legalidad e integridad. Esta responsabilidad no puede trasladarse a los PRSTM, en virtud del principio de inviolabilidad de las comunicaciones y derechos de intimidad y privacidad de los usuarios.

En este sentido, es importante que la Comisión profundice en lo relacionado con los mecanismos de autorización expresa por parte de los usuarios para ser contactados por distintos agentes del ecosistema digital. En particular, respecto al envío de mensajes de texto (SMS), debe precisarse que la autorización otorgada por el usuario a un PRSTM no puede entenderse como una habilitación automática a otros actores, como PCA o IT, salvo que exista una autorización independiente, libre, previa, informada y expresa para tales fines. Además, si bien los PRSTM desempeñan un rol esencial en la distribución del mensaje, su función se limita a ser un canal de transmisión, y no implica necesariamente que cuenten con autorización para la contactabilidad en nombre de terceros.

b) <u>Respecto del uso inadecuado de la numeración E.164:</u>

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?

RTA. Con el establecimiento de reglas de exclusividad en el uso de la numeración y la prohibición de su reventa, consideramos que no sería necesario implementar medidas adicionales de trazabilidad. Al asignarse un único responsable por cada código, se garantiza la plena identificación del titular y, por ende, del responsable del contenido de los mensajes asociados a dicho recurso.

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?

RTA. Consideramos que el proyecto regulatorio debería enfocarse prioritariamente en establecer medidas preventivas que impidan el inicio de acciones fraudulentas, en lugar de centrarse únicamente en técnicas de detección cuando el fraude ya está en curso.

En el caso de los mensajes de texto corto SMS, medidas como el establecimiento de reglas de exclusividad en el uso de la numeración y la prohibición de su reventa tendrían un mayor impacto en la mitigación de acciones fraudulentas, al atacar la raíz del problema. Así como establecer las mismas responsabilidades y obligaciones a cargo de los PCA e IT.

Sin embargo, si la Comisión contempla la implementación de medidas adicionales orientadas al uso de herramientas tecnológicas, es importante tener en cuenta que los PRSTM no cuentan con facultades legales para revisar el contenido de los mensajes, salvo en las excepciones expresamente previstas en la ley. Por esta razón, cualquier medida en este sentido debería estar dirigida a los actores que originan la comunicación, es decir, los PCA e IT.

Por otra parte, en el caso de las llamadas de voz, se presentan acciones de fraude con prácticas asociadas a llamadas automáticas o robocalls. Esta metodología de fraude suele comenzar con un alto volumen de llamadas generadas automáticamente hacia rangos de numeración, con el objetivo de identificar líneas activas y perfiles de usuario, para luego iniciar un intento de fraude más elaborado. En estos casos, los mecanismos de detección son limitados, pues la primera llamada suele cortarse tan pronto se identifica actividad en la línea, lo que dificulta establecer alertas tempranas.

En este caso, también se recomienda que las medidas regulatorias se orienten a ejercer controles en las fases iniciales de la llamada. La identificación de una llamada como sospechosa o fraudulenta suele depender, en última instancia, del receptor, especialmente cuando se trata de una segunda llamada, luego de haberse perfilado previamente al usuario. Por ello, deberían establecerse restricciones ante el uso de este tipo de prácticas. En todo caso, reiteramos que los PRSTM no tenemos autorización para intervenir, escuchar o analizar el contenido de las llamadas de voz, por lo que cualquier solución debe ajustarse a este marco legal.

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.

RTA. Reiteramos lo expuesto en el punto anterior.

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

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?

RTA. Conforme lo expuesto en los comentarios generales, consideramos que la Comisión en su calidad de entidad reguladora con espacios institucionales en los canales de televisión abierta, cuenta con amplia capacidad de divulgación, es el medio óptimo para impulsar campañas pedagógicas que informen de forma clara, práctica y accesible a los ciudadanos.

Si bien valoramos los esfuerzos orientados a la prevención del fraude cibernético, consideramos que las obligaciones de divulgación pedagógica deben diseñarse bajo un enfoque de asimetría regulatoria, en atención a las múltiples cargas que ya asumimos los PRSTM en materia de protección al usuario, incluyendo la prevención de fraudes por suplantación del cual somos víctimas, la portabilidad numérica móvil, la activación de líneas prepago y en general todas las obligaciones de divulgación establecidas por la CRC y la SIC en materia de usuarios.

La regulación ya establece mecanismos para que los usuarios dejen de recibir mensajes de texto provenientes de códigos cortos mediante la utilización de palabras clave como "SALIR" o "CANCELAR"[9] según lo establecido en la Resolución 6522 de 2022 en su Artículo 4to. No obstante, dichos mecanismos no son conocidos por la mayoría de los usuarios de servicios móviles; por lo tanto, proponemos que la CRC utilice los medios de los que dispone para realizar campañas de comunicación para posicionar esta posibilidad existente como medida para mitigar el fraude.

En ese sentido, apoyamos la idea de campañas conjuntas lideradas por la CRC, complementadas con un portal institucional de denuncias de remitentes, siempre que se evite duplicar esfuerzos y se garantice una distribución proporcional de responsabilidades entre PRSTM, PCA e integradores tecnológicos.

[9] Resolución 6522 de 2022 en su ARTÍCULO 2.1.19.7. ESTANDARIZACIÓN PALABRAS CLAVE. Los PCA deben adoptar las siguientes palabras clave estandarizadas (sin importar la utilización de letras mayúsculas o minúsculas) para los distintos procedimientos.
(…)
2.1.19.7.6. La palabra clave "salir" o "cancelar": indica la solicitud para restringir la recepción de mensajes de un determinado PCA. En el caso de los servicios de suscripción, indica la cancelación de todos los servicios desde un determinado código corto.

A su vez, en caso de establecer esta obligación, es fundamental que recaiga sobre los actores que ofrecen estos servicios y que tienen control sobre su contenido, como los PCA e IT, así como, los proveedores de contenido OTT. Estos actores deben involucrarse activamente en la realización de campañas pedagógicas dirigidas a los usuarios. En el caso de estos últimos, es importante tener en cuenta que las acciones de fraude también se ejecutan a través de plataformas de mensajería operadas por estos proveedores.

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?

RTA. El problema no radica en el recurso de identificación en sí, sino en la ausencia de medidas eficaces que prevengan su utilización con fines fraudulentos. En este sentido, la creación de listas negras con los recursos de identificación más denunciados tendría un impacto limitado si no se acompaña de mecanismos ágiles para su detección, validación, inclusión oportuna y notificación a los PRSTM para realizar los respectivos bloqueos.

Las acciones deben ser oportunas, porque de lo contrario el incluir un código que ha sido usado durante meses para cometer fraudes carece de utilidad práctica, ya que el daño ya ha sido causado. Por ello, se requiere un enfoque preventivo y dinámico, con acciones tempranas que permitan bloquear o restringir rápidamente estos recursos desde las primeras señales de uso indebido.

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

RTA. Consideramos que esta medida representa una carga adicional para los PRSTM, quienes son solo un medio, sin que ello implique un aporte efectivo a la prevención o mitigación de las acciones de fraude. Las medidas que se adopten en el marco de este proyecto deben priorizar la eficiencia y minimizar el impacto económico de su implementación, especialmente teniendo en cuenta que se trata de un sector que ya ha sido afectado significativamente en términos financieros, como se ha expuesto en diversas oportunidades ante la Comisión.

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.

RTA. Como se mencionó previamente, el uso de los espacios institucionales en la televisión abierta administrados por la CRC sería una medida útil para aumentar el espectro de divulgación de conocimiento para mitigar este flagelo.

También se podría estructurar un programa nacional de alfabetización digital en seguridad para el uso de servicios de telecomunicaciones, mediante el cual la CRC, en coordinación con el MinTIC y la academia, impulsarías programas transversales para fortalecer las competencias digitales básicas relacionadas con la identificación de fraudes, el uso seguro del teléfono móvil y la gestión responsable de los datos personales. Esto podría desarrollarse en alianza con bibliotecas públicas, centros de conexión comunitarios o entornos escolares.

d) <u>Sobre la revisión integral del Régimen de Recursos de Identificación</u>

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

RTA. A continuación se presentan algunas sugerencias o recomendaciones de optimización de estos procedimientos:

Respecto a los procedimientos de asignación.

- El uso de los códigos cortos debería tener una destinación especifica y restringir el uso para motivos no solicitados, por tanto, consideramos necesario ajustar las categorías de asignación para cumplir con dicho propósito.

- Al momento de evaluar los requisitos de asignación, debería evaluarse si la empresa que realiza la solicitud o sus accionistas tienen antecedentes relacionados con investigaciones o actos administrativos de recuperación de numeración por acciones fraudulentas y en dado caso, negar la solicitud de asignación.

- Se deben establecer responsabilidades y consecuencias claras en caso de un uso indebido. Además, se debe indicar que tanto los PCA como los IT tengan el mismo nivel de responsabilidades y consecuencias ante este tipo de conductas.

Respecto a los procedimientos de recuperación.

- Cuando se recupera un código corto, al momento de emitir el acto administrativo de recuperación a la empresa que tiene asignado el recurso, se debería informar a los PRSTM para proceder inmediatamente con el bloqueo de la numeración.

- Se debe mejorar la frecuencia de actualización de la página Web, para identificar los códigos retirados oportunamente y poder proceder con mayor diligencia con las debidas acciones para mitigar el impacto de las acciones fraudulentas.

Cordial saludo,

VIAFIRMA COLOMBIA - 9014654196 25/07/2025 10:18:33 COT -05
Firma con certificado digital de Ana Marina Jiménez
RJW3-FOAG-OF1O-TWD9-2175-3456-7131-66

ANA MARINA JIMÉNEZ POSADA
Vicepresidente de Asuntos Corporativos