VPAC-100021-03-045 Bogotá D. C, 4 de agosto de 2025

Doctora
CLAUDIA XIMENA BUSTAMANTE
Directora Ejecutiva
COMISIÓN DE REGULACIÓN DE COMUNICACIONES -CRC-
medidasantifraude@crcom.gov.co; atencioncliente@crcom.gov.co;
Calle 59A Bis N° 5-53 Edificio Link Siete Sesenta
Ciudad

Asunto: Comentarios al Documento de formulación del problema *"Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles"* publicada por la CRC.

Apreciada Directora,

Reciba un cordial saludo por parte de Partners Telecom Colombia S.A.S., en adelante PTC. En esta oportunidad nos dirigimos a usted con el fin de presentar nuestros comentarios frente al proyecto señalado en el asunto, manifestando la relevancia y pertinencia del proyecto en el marco de un escenario complejo para la seguridad cibernética, especialmente por el uso inescrupuloso que la delincuencia realiza de los servicios móviles.

Desde PTC, manifestamos nuestra profunda preocupación en torno a la amenaza que el fraude cibernético representa para los usuarios, resaltando la importancia de este tipo de espacios para avanzar en la construcción e implementación de medidas que resulten adecuadas.

1. Comentarios generales.

A continuación se presenta un informe por país sobre las medidas regulatorias adoptadas para prevenir fraudes efectuados mediante SMS y llamadas telefónicas

País	Comentarios
 **Estados Unidos**	La regulación federal ya permite a los PRST tomar medidas de bloqueo en torno al fraude: a partir de marzo de 2023 la FCC aprobó las primeras reglas específicas contra textos fraudulentos. Estas nuevas normas (Report and Order FCC 23-21, en vigor desde mayo de 2023) obligan a las compañías móviles a bloquear a nivel de red los SMS que aparenten provenir de números inválidos, no asignados o en

	listas DNO (números que *nunca* enviarían SMS legítimos)[1].
 **Reino Unido**	El Reino Unido ha entregado herramientas regulatorias adicionales a los Operadores, en contra los fraudes telefónicos, a saber: Fraudes vía llamadas: A partir de mayo de 2023 entraron en vigor nuevas obligaciones establecidas por Ofcom (mediante modificación de las Condiciones Generales, Sección C6) dirigidas a que todos los proveedores de telefonía en el país filtren llamadas con CLI falsificado. En concreto, Ofcom exige que, *"cuando sea técnicamente factible"*, los operadores identifiquen y bloqueen: • Llamadas con datos de caller ID inválidos o no marcables (ej. números que no existen o formateados incorrectamente). • Llamadas internacionales entrantes que presenten un número de Reino Unido como identificador, cuando no debería ser el caso (spoofing de numeración nacional)[2]. Por ejemplo, una llamada originada desde el extranjero que exhiba un número fijo o móvil del Reino Unido puede ser bloqueada por defecto, ya que se presume suplantación a menos que haya casos de uso legítimos muy específicos.
 **México**	**México ha sido el escenario de un trabajo mancomunado:** La Comisión Nacional Bancaria (CNBV) y la Asociación de Bancos han trabajado con operadores para frenar mensajes falsos de banca móvil, y empresas como Meta/Facebook han apoyado campañas ("Redes Seguras") de Profeco contra fraudes

[1] https://www.federalregister.gov/documents/2023/04/11/2023-07405/targeting-and-eliminating-unlawful-text-messages#:~:text=SUMMARY%3A
[2] https://transnexus.com/blog/2022/uk-new-spoofing-blocking-rules/#:~:text=,geographic%20numbers%20as%20CLI

	en WhatsApp y SMS[3]. Estas son iniciativas de educación y coordinación más que obligaciones legales. México ha optado recientemente por un enfoque cooperativo regulado: un convenio Profeco-industria que formaliza obligaciones de filtrado y verificación para las compañías telefónicas e integradores en materia de SMS A2P[4]
 **Singapur**	Singapur ha adoptado un enfoque integral y pionero, combinando **regulación de telecomunicaciones y directrices del sector financiero para atacar el fraude por SMS y llamadas** desde múltiples ángulos. Un hito importante fue la implementación del SMS Sender ID Registry (SSIR), un registro central de identificadores de remitente de SMS similar al modelo británico, pero convertido en esquema obligatorio respaldado por el regulador IMDA. Tras una serie de estafas de *phishing* bancario a finales de 2021, la Infocomm Media Development Authority (IMDA) lanzó el SSIR en fase beta voluntaria en 2022 y lo hizo plenamente obligatorio el 31 de enero de 2023[5]. Bajo el "Full SSIR Regime", *todas* las organizaciones (locales o extranjeras) que envíen SMS a números de Singapur deben registrar previamente los Sender ID (alfanuméricos o numéricos) que utilizan. Desde febrero 2023, los operadores móviles de Singapur marcan con la etiqueta "Likely-SCAM" cualquier mensaje entrante que muestre un remitente no registrado en SSIR. En otras palabras, si un estafador envía un SMS fingiendo ser "XYZBank" y ese alias no está en la lista blanca, al usuario le aparecerá

[3] https://www.condusef.gob.mx/?p=contenido&idc=431&idcat=1#:~:text=Alerta%20CONDUSEF%20por%20nuevo%20caso,Por
[4] https://www.elfinanciero.com.mx/tech/2024/01/25/companias-telefonicas-ya-no-mandaran-spam-telcel-att-movistar-izzi-profeco-acuerdo-con-antel/#:~:text=Las%20condiciones%20del%20acuerdo%20para,prevenir%20el%20Spam%20son
[5] https://www.sgnic.sg/faq/sms-sender-id-registry#:~:text=Under%20the%20Full%20SSIR%20Regime%2C,following%20the%20Rules%20of%20Registration

	proveniente de "Likely-SCAM" (Probable Estafa) en lugar del nombre, alertándolo de la posible falsedad. El registro SSIR es administrado por SGNIC (Singapore Network Information Centre) y requiere verificación de la entidad solicitante. Solo empresas con identificación local válida (número UEN) pueden inscribir Sender IDs, lo cual significa que empresas extranjeras deben establecer una filial o representante local para registrarse, añadiendo trazabilidad. Además, los agregadores de SMS "participantes" integran sus sistemas con el SSIR: SGNIC distribuye semanalmente la lista blanca de Sender IDs autorizados a todos los agregadores y operadores adheridos.

En estos casos lo que destacamos justamente es que se reconoce que las cargas de medidas técnicas o tecnológicas en contra del fraude a través de SMS y de la provisión de contenidos y aplicaciones, no recaen solamente en los operadores, sino que vincula a los demás agentes de la cadena de valor. Esto más acorde con la realidad del funcionamiento incluso de este mercado en Colombia, en donde la mayoría de los fraudes provienen de los proveedores de contenidos y aplicaciones que cuentan con acceso a las redes de los PRST.

2. Comentarios específicos.

El problema identificado por la CRC resulta acertado, sin embargo, el mismo adolece de algunas limitaciones e imprecisiones que resulta necesario ajustar para que la problemática a resolver resulta concordante con la realidad.

2.1. Respuesta a las preguntas formuladas por la CRC.

A continuación, se relacionan las respuestas de PTC a las preguntas formuladas por la CRC:

2.1.1. ¿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?

Si bien las causas identificadas preliminarmente por la CRC coinciden con el origen del problema planteado, desde PTC presentamos ante la CRC, algunas

sugerencias y ajustes que podrían mejorar la precisión de las causas expuestas en el documento:

2.1.1.1. Respecto a la *Causa 1.* ***Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso***:

La Comisión de Regulación de Comunicaciones (CRC) acierta al reconocer que las decisiones regulatorias adoptadas en torno al uso de recursos de identificación han privilegiado, de manera prioritaria, criterios de eficiencia operativa, relegando consideraciones vinculadas a la idoneidad, comportamiento y trazabilidad del asignatario.

En complemento a lo anterior, el marco normativo vigente presenta una limitación estructural al impedir la participación de actores relevantes —como los *carriers* internacionales sin presencia legal en el territorio colombiano— quienes, al no estar inscritos como proveedores de servicios TIC, se encuentran imposibilitados de figurar como asignatarios de recursos de numeración, dificultando así su sujeción al régimen regulatorio nacional.

No obstante, sin desconocer los esfuerzos regulatorios adelantados por la Comisión, debe advertirse que las medidas implementadas hasta la fecha han sido insuficientes para establecer mecanismos robustos que permitan distinguir, de manera eficaz, entre comunicaciones legítimas y aquellas que corresponden a eventos de suplantación. Del mismo modo, se carece de un régimen claro de obligaciones para que los operadores de red verifiquen, supervisen y garanticen el uso adecuado de los recursos numéricos asignados a terceros.

Bajo este contexto, se identifican diversas falencias del régimen actual que ameritan revisión y ajuste:

i) El marco normativo no genera un efecto disuasivo suficiente frente a proveedores de contenidos y aplicaciones (PCA) o integradores tecnológicos (IT) que incurren de manera reiterada en prácticas indebidas.

ii) No se prevén consecuencias regulatorias inmediatas y contundentes que afecten directamente la relación de acceso entre el infractor y los operadores de red, lo que debilita el efecto sancionatorio y preventivo.

iii) La reincidencia en conductas indebidas no está asociada a consecuencias claras ni progresivas, lo que permite la repetición sistemática de comportamientos contrarios a la regulación.

iv) Se generan incentivos perversos, en la medida en que el costo de reincidir resulta, en muchos casos, inferior al beneficio económico derivado de facilitar esquemas fraudulentos.

v) Mientras se mantenga la posibilidad de que los PCA e integradores continúen operando tras múltiples recuperaciones de numeración, el cumplimiento del marco regulatorio se percibirá como prescindible, reduciendo su eficacia real.

vi) La reiteración en el uso indebido de códigos cortos constituye evidencia objetiva de una deficiente gestión interna de seguridad y control por parte del PCA o IT involucrado.

vii) Las prácticas fraudulentas asociadas al uso irregular de recursos de identificación no solo perjudican a los usuarios finales, sino que además afectan gravemente la integridad del ecosistema de telecomunicaciones, al minar la confianza institucional y ciudadana en canales tradicionales como la mensajería SMS y la voz.

Finalmente, la necesidad constante de intervención del regulador para recuperar recursos de numeración revela un patrón sistemático de incumplimiento, y no una serie de hechos aislados, lo que refuerza la urgencia de adoptar medidas regulatorias más estrictas, articuladas y eficaces frente a estos comportamientos reincidentes. Acierta la CRC en identificar que las medidas en materia recursos de identificación se han enfocado de forma exclusiva en la eficiencia, priorizando este criterio por encima de las calidades del asignatario.

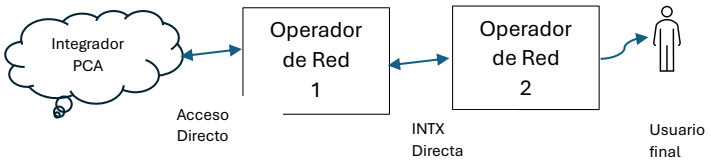
Adicionalmente, el marco regulatorio actual, impide que Actores relevantes (tales como *Carriers Internacionales*) que no tiene presencia en Colombia, y que por tanto no cuentan con registro TIC y no pueden asignatarios.

En efecto, las medidas actualmente adoptadas por la regulación para la contención de eventos de fraude asociados al uso de recursos escasos, como lo es la numeración, han resultado insuficientes. Esta insuficiencia obedece, entre otras razones, al hecho de que dichas medidas se han enfocado casi exclusivamente en la supervisión del recurso numérico en sí mismo, sin considerar de manera integral otros elementos estructurales del ecosistema. En particular, se ha omitido un análisis profundo y sistémico de los diversos actores que intervienen en la cadena de prestación de servicios A2P, tanto en comunicaciones de voz como de mensajes de texto (SMS), especialmente aquellos clasificados como Proveedores de Contenidos y Aplicaciones (PCA).

A continuación, se presenta una gráfica ilustrativa de la cadena de agentes involucrados en la prestación de servicios de comunicaciones tipo A2P-SMS. Entre ellos se destacan:

i) **El Cliente**, quien administra la aplicación desde la cual se origina el mensaje. Este actor, en muchos casos, se encuentra registrado como PCA y puede contar o no con numeración corta SMS asignada por la CRC. Usualmente, no dispone de acceso directo a las redes de los Operadores Móviles o Fijos.

ii) **El Integrador o Agregador**, quien intermedia entre el Cliente y los Operadores de Red. Este actor comercializa servicios al Cliente, cuenta con numeración corta SMS asignada por la CRC, y posee acceso directo a la totalidad de los operadores de red, lo cual le permite canalizar los mensajes hacia los destinatarios finales.



2.1.1.2. Respecto a la Causa 2. Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso:

Resulta preocupante que el documento identifique como una de las causas del problema la supuesta insuficiencia de las acciones implementadas por los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) y los asignatarios de recursos de identificación, sin considerar de manera adecuada las limitaciones de carácter regulatorio, técnico y operativo a las que dichos actores se ven enfrentados al momento de intentar responder de manera oportuna y eficaz frente a eventos de fraude.

En primer lugar, debe resaltarse que no es jurídicamente admisible exigir la adopción de medidas preventivas sin que exista una habilitación normativa expresa ni la capacidad operativa mínima necesaria para su implementación. Los operadores, en general, carecen tanto de competencias legales como de un mecanismo institucional de coordinación que les permita bloquear, filtrar o anticiparse de manera proactiva a conductas fraudulentas que se cursan a través

de sus redes y cuya ejecución ocurre, en muchos casos, en lapsos de tiempo extremadamente breves. Esto, a pesar de las obligaciones regulatorias generales antifraude, como única fuente jurídica a la que se puede apelar por parte de los operadores.

A ello se suma que los efectos derivados de ciertos esquemas de fraude –como es el caso del smishing o de llamadas falsas que inducen transferencias bancarias inmediatas– se materializan en cuestión de segundos. En tales escenarios, cualquier acción adoptada con posterioridad al inicio del evento resulta, por definición, tardía. Las medidas de carácter reactivo, por tanto, no deben interpretarse como una falla en el diseño del sistema, sino como el único mecanismo actualmente disponible ante amenazas que ya se han consumado. Esta situación es estructural y no puede ser atribuida exclusivamente a la voluntad o inacción de los agentes involucrados.

En este sentido, lo apremiante no es reprochar la ausencia de actuaciones por parte de los PRST o de los asignatarios de numeración, pues por el contrario son los operadores o PRST quienes están soportando mayoritariamente no solo las cargas antifraude sino también el impacto negativo reputacional y ante autoridades de vigilancia y control del actuar fraudulento de usuarios de los PCA e integradores tecnológicos, sino reconocer que el marco regulatorio y operativo vigente no proporciona las herramientas necesarias para actuar con mayor eficacia. Por ello, se recomienda a la Comisión de Regulación de Comunicaciones (CRC) considerar las siguientes medidas orientadas a promover un enfoque preventivo más robusto:

A) Incorporar dentro del marco regulatorio una habilitación expresa para que los PRST y los asignatarios de recursos de numeración puedan proceder, de manera preventiva, al bloqueo de tráfico o numeración que resulte sospechosa de estar asociada a prácticas fraudulentas, garantizando al mismo tiempo que dichas actuaciones no generen consecuencias regulatorias adversas cuando, en ejercicio de su deber de diligencia, afecten eventualmente servicios legítimos.

B) Establecer un protocolo expedito para el bloqueo de URLs maliciosas –tanto de origen nacional como internacional– mediante mecanismos de coordinación interinstitucional entre la CRC, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Superintendencia Financiera de Colombia (SFC), las entidades vigiladas por esta última, y los proveedores tecnológicos, entre otros actores relevantes. Esta herramienta podría estructurarse con base en experiencias exitosas como la implementada para el

bloqueo de sitios web no autorizados por Coljuegos en el marco de la regulación sobre juegos de suerte y azar.

Así las cosas, sugerimos la siguiente redacción: *Los PRST y demás asignatarios de recursos de identificación no cuentan con herramientas regulatorias efectivas que les permitan gestionar adecuadamente el riesgo de fraude cibernético a través de servicios móviles*

2.1.1.3. Respecto a la Causa 3. Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso:

Resulta preocupante que el documento identifique como una de las causas del problema la supuesta insuficiencia de las acciones implementadas por los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) y los asignatarios de recursos de identificación, sin considerar de manera adecuada las limitaciones de carácter regulatorio, técnico y operativo a las que dichos actores se ven enfrentados al momento de intentar responder de manera oportuna y eficaz frente a eventos de fraude.

En primer lugar, debe resaltarse que no es jurídicamente admisible exigir la adopción de medidas preventivas sin que exista una habilitación normativa expresa ni la capacidad operativa mínima necesaria para su implementación. Los operadores, en general, carecen tanto de competencias legales como de un mecanismo institucional de coordinación que les permita bloquear, filtrar o anticiparse de manera proactiva a conductas fraudulentas que se cursan a través de sus redes y cuya ejecución ocurre, en muchos casos, en lapsos de tiempo extremadamente breves.

A ello se suma que los efectos derivados de ciertos esquemas de fraude —como es el caso del *smishing* o de llamadas falsas que inducen transferencias bancarias inmediatas— se materializan en cuestión de segundos. En tales escenarios, cualquier acción adoptada con posterioridad al inicio del evento resulta, por definición, tardía. Las medidas de carácter reactivo, por tanto, no deben interpretarse como una falla en el diseño del sistema, sino como el único mecanismo actualmente disponible ante amenazas que ya se han consumado. Esta situación es estructural y no puede ser atribuida exclusivamente a la voluntad o inacción de los agentes involucrados.

En este sentido, lo apremiante no es reprochar la ausencia de actuaciones por parte de los PRST o de los asignatarios de numeración, sino reconocer que el marco regulatorio y operativo vigente no proporciona las herramientas necesarias para actuar con mayor eficacia. Por ello, se recomienda a la Comisión de

Regulación de Comunicaciones (CRC) considerar las siguientes medidas orientadas a promover un enfoque preventivo más robusto:

> A) Incorporar dentro del marco regulatorio una habilitación expresa para que los PRST y los asignatarios de recursos de numeración puedan proceder, de manera preventiva, al bloqueo de tráfico o numeración que resulte sospechosa de estar asociada a prácticas fraudulentas, garantizando al mismo tiempo que dichas actuaciones no generen consecuencias regulatorias adversas cuando, en ejercicio de su deber de diligencia, afecten eventualmente servicios legítimos.
>
> B) Establecer un protocolo expedito para el bloqueo de URLs maliciosas –tanto de origen nacional como internacional– mediante mecanismos de coordinación interinstitucional entre la CRC, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Superintendencia Financiera de Colombia (SFC), las entidades vigiladas por esta última, y los proveedores tecnológicos, entre otros actores relevantes. Esta herramienta podría estructurarse con base en experiencias exitosas como la implementada para el bloqueo de sitios web no autorizados por Coljuegos en el marco de la regulación sobre juegos de suerte y azar.
>
> Así las cosas, sugerimos la siguiente redacción: *"Desconocimiento de los usuarios sobre privacidad de la información facilita la obtención de datos personales con fines fraudulentos"*.

2.1.1.4. Respecto a la Causa 4. *Cargas regulatorias lapsas dirigidas a PCA e integradores tecnológicos*:

Como ya lo ha expuesto PTC en otros escenarios, las cargas regulatorias en materia de gestión del fraude dirigidas específicamente a PCA e integrado Tecnológicos resultan desproporcionadas si se comparan con las dirigidas a los PRST.

Bajo este contexto, esta causa debe incluirse dentro del árbol del problema, ya que el remedio regulatorio que se materialice luego del ejercicio liderado por la Comisión debe incluir instrumentos para que obliguen a los Proveedores de Contenidos y Aplicaciones (PCA) e Integradores Tecnológicos (IT) a otorgar las interconexiones a un PRST, cuando este último sea el solicitando, teniendo en cuenta que a la fecha no hay ninguna obligación del PCA que lo obligue a conectarse a un PRST o a imponer condiciones para que dicho acceso se pueda dar, situación que puede afectar de manera significativa a los usuarios, toda vez que los usuarios pueden estar requiriendo de los servicios de un PCA o IT

específico a través de su operador de red, lo cual, resultaría lesivo para la libre competencia y restringiría la libertad de elección del usuario.

Esto es importante, por cuanto los usuarios del PRST estar requiriendo de los servicios específicos de un PCA o IT, el cual, puede negarse a acceder a la red del PRST, obligando al usuario a portarse a otro Operador, so pena de no poder acceder al servicio específico que ofrece el PCA o IT.

2.1.2. Frente al problema planteado, ¿por qué considera que las causas presentadas en este documento son las que generan el problema definido? En caso de considerar lo contrario, por favor indicar las razones por las cuales no está de acuerdo con la relación que se establece entre tales causas y el problema definido, y proponga las causas que considere pertinentes.

La problemática objeto de análisis ha sido tradicionalmente abordada desde una perspectiva centrada en los agentes formalmente registrados ante la Comisión de Regulación de Comunicaciones (CRC), en particular aquellos inscritos en el Sistema de Información y Gestión de Recursos de Identificación (SIGRI) y en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores (RPCAI). Sin perjuicio de que estos actores representan nodos clave dentro del ecosistema y frente a los cuales pueden implementarse medidas regulatorias más directas y eficaces, lo cierto es que uno de los principales desafíos asociados al fraude cibernético radica, precisamente, en que buena parte de los ataques se originan desde fuentes que no se encuentran plenamente identificadas ni cumplen con las obligaciones regulatorias asociadas al uso correcto de los recursos de identificación.

Desde la experiencia de una entidad sujeta a la inspección y vigilancia de la Superintendencia Financiera de Colombia, se ha observado que los mecanismos de contacto con usuarios mediante llamadas de voz y mensajes de texto (SMS) son los canales predilectos por los delincuentes para llevar a cabo esquemas de fraude basados en técnicas de ingeniería social, tales como el *smishing* y el *vishing*. Estas prácticas afectan directamente la confianza del consumidor en un sector que, aunque altamente regulado, presenta vulnerabilidades significativas por el uso de dichos canales. Asimismo, se generan impactos negativos en la reputación institucional, se incrementan los costos operativos asociados a la atención de fraudes, y se compromete de manera crítica la integridad del ecosistema financiero en su conjunto.

La ausencia de mecanismos regulatorios específicos para el control riguroso de los recursos de identificación —como los códigos cortos o la numeración tipo E.164— ha restringido significativamente la capacidad de reacción y mitigación del sector financiero frente a este tipo de amenazas. Por consiguiente, se estima

esencial que el fenómeno de suplantación de identidad de entidades del sector financiero sea reconocido como una de las expresiones más graves y frecuentes del problema, dadas su alta incidencia y repercusión económica.

Adicionalmente, la problemática excede la esfera técnica y regulatoria de los operadores de telecomunicaciones. Afecta de manera directa a los usuarios finales, quienes no tienen por qué conocer ni comprender las particularidades técnicas de los recursos de identificación utilizados en los mensajes o llamadas que reciben. En ese sentido, los actores criminales suplantan entidades legítimas mediante el uso de numeración falsificada, alteración de identificadores en SMS, y emisión de llamadas automáticas con locuciones que replican el lenguaje institucional, sin que el usuario tenga herramientas efectivas para discernir si el origen del mensaje o llamada es legítimo o fraudulento.

En la práctica, ello se traduce en la inexistencia de un mecanismo confiable, sencillo y seguro que permita a los consumidores verificar con certeza si un mensaje de texto o llamada proviene efectivamente de su entidad financiera o de un tercero malintencionado. Esta vulnerabilidad persiste incluso a pesar de las campañas de educación financiera y prevención del fraude que adelantan muchas entidades, lo cual evidencia la necesidad de un enfoque regulatorio más robusto y coordinado que contemple todos los actores del ecosistema digital, incluidos los proveedores de contenidos, integradores tecnológicos y terceros no registrados.

En este punto de los comentarios, consideramos pertinente traer a colación cómo los principales casos de fraude que desde esta empresa hemos detectado, de acuerdo con nuestra experiencia en el mercado, provienen del actuar de PCA o integradores tecnológicos, o de sus usuarios.

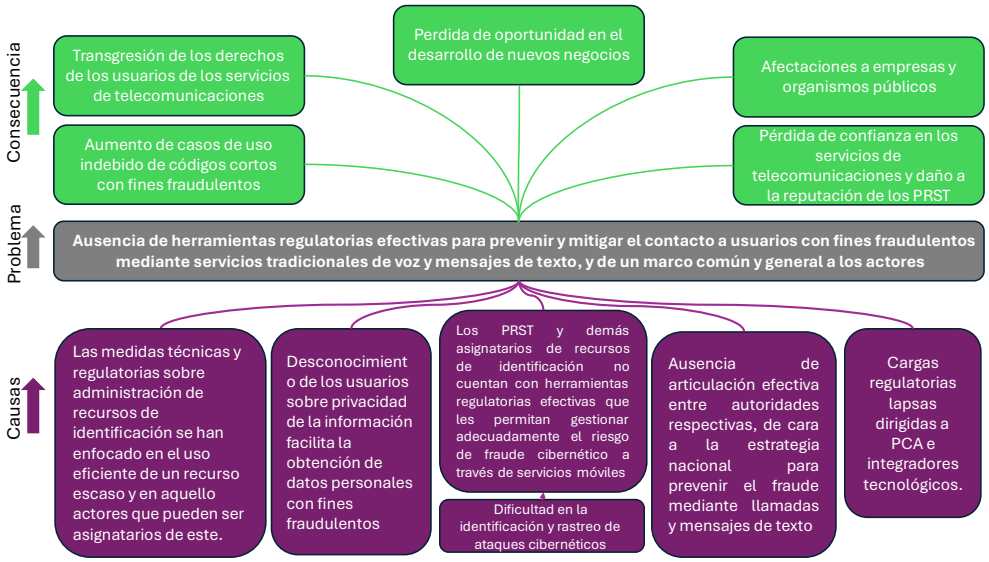
Esto ha hecho que, desde esta empresa, nos hayamos visto obligados a reforzar nuestro seguimiento y actividad antifraude, de forma tal que podamos notificar de forma pronta y expedita a los PCA e Integradores con el fin de que tomen acciones de prevención o corrección del fraude. Sin embargo, muchas de éstas no toman ningún tipo de acción adicional, lo que pone a los operadores, en una situación desventajosa, en tanto que, si no toman acciones contra el fraude, como por ejemplo bloqueos temporales de códigos cortos, como deber establecido en la regulación, pueden continuar exponiendo a sus usuarios a este tipo de delitos, mientras se surten actuaciones administrativas por parte de la CRC de recuperación o bloqueo de códigos cortos.

Incluso, de forma contraria a derecho y temeraria, o abusiva del derecho, algunos PCA e Integradores, denuncian acciones de prevención de fraude que toman los operadores, lo que demuestra que se requieren de mecanismos establecidos en

la regulación que eviten que los operadores puedan ser puestos en riesgo sancionatorio, por tomar acciones antifraude en defensa de sus usuarios.

2.1.3. ¿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.

En concordancia con lo previamente expuesto, sugerimos el árbol del problema que relacionamos a continuación:



Confiamos en que con estos comentarios podamos contribuir positivamente en el devenir de los proyectos regulatorios listados y que confiamos sean tenidos en cuenta por la Comisión, reiterando nuestra total disposición para contribuir de manera efectiva al proceso regulatorio en beneficio de los usuarios y en la prevención del fraude.

Cordialmente,

EMILIO SANTOFIMIO JARAMILLO
Director de Regulación
PARTNERS TELECOM COLOMBIA S.A.S. EN REORGANIZACIÓN