Bogotá D.C., 29 de diciembre 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 alternativas regulatorias del proyecto denominado *"Identificación de medidas para mitigar el Fraude Cibernético por medio de servicios móviles"*.

Respetada Ingeniera Bustamante,

Agradecemos la publicación de este proyecto por el cual la CRC busca generar alternativas regulatorias para prevenir y/o mitigar el fraude cibernético, y que finalmente constituirá un instrumento esencial para la protección de los derechos de los usuarios de servicios de comunicaciones móviles y de los proveedores de servicios de telecomunicaciones, quienes también resultamos perjudicados con dichos actos ilícitos.

Resulta importante indicar que, el planteamiento de alternativas regulatorias agrupadas por temáticas resulta adecuado, en la medida en que permite un análisis más claro y sistemático de cada problemática, facilitando la identificación de soluciones frente al flagelo del fraude cibernético asociado a los servicios de voz y mensajes cortos de texto (SMS). En este sentido, valoramos el esfuerzo de la Comisión por consolidar de manera rigurosa y constructiva los comentarios remitidos por los distintos grupos de valor, reflejando una disposición abierta al diálogo y a la construcción conjunta de soluciones.

Adicionalmente, consideramos necesario que la CRC proceda lo antes posible a incorporar en la agenda regulatoria una segunda fase de este proyecto que aborde alternativas para prevenir o mitigar el fraude en los servicios de datos especialmente para el control de fraude a través de aplicaciones OTT. Lo anterior, en ejercicio de las facultades conferidas por el artículo 19 de la Ley 1341 de 2009 como autoridad encargada de garantizar la protección de los derechos de los usuarios en los servicios de comunicaciones, facultades que en ningún caso se restringen exclusivamente a los servicios de voz y SMS.

En ese sentido, 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), presentamos para su consideración nuestros comentarios.

CONTENIDO

1. COMENTARIOS GENERALES

1.1. Fraude cibernético a través del mercado relevante "Internet Móvil"

Al respecto evidenciamos que, las cifras relacionadas con el fraude cibernético muestran un crecimiento sostenido y preocupante. De acuerdo con cifras del Ministerio de Defensa y el Centro Cibernético de la Policía Nacional, a cierre de 2024 se registraron en Colombia 74.845 atentados relacionados con la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, así como atentados informáticos y otras infracciones , lo que representa un incremento cercano al 18,3% frente a las 63.249 denuncias del mismo periodo de 2023[1]. Otros reportes señalan, además, que entre 2020 y 2023 los delitos informáticos aumentaron cerca de un 89%, confirmando una tendencia estructural al alza de este tipo de conductas[2]. Esto confirma que el fraude cibernético es un problema social que debe ser atendido directamente por el Estado a través de sus entidades lo antes posible.

En este contexto, los ciberdelincuentes han encontrado en el envío de SMS una puerta de ataque eficaz (smishing). Distintos estudios internacionales muestran que el smishing crece a tasas de dos dígitos con incrementos estimados del orden del 18 % anual usando números de teléfono locales y con alrededor del 28 % de las campañas de phishing distribuidas a través de mensajes de texto[3].

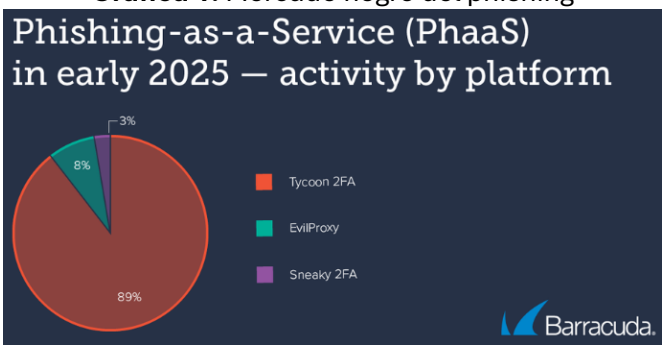
Es importante subrayar que, si bien el vector inicial suele ser el SMS, **el fraude no se materializa sino hasta el momento en que el usuario hace clic sobre el enlace incluido en el mensaje y es redirigido a una página web o aplicación fraudulenta**, donde se ejecuta la captura de credenciales o información sensible (phishing). Reportes recientes muestran, además, que los enlaces maliciosos ahora se utilizan cuatro veces más que los archivos adjuntos en amenazas de correo electrónico. Además, los ciberdelincuentes están utilizando técnicas avanzadas de **ingeniería social** y contenido generado por IA para crear sus URLs maliciosas. Esto demuestra que la causa del problema no está en el canal de transporte en sí mismo, por lo que escapa del control de los operadores.

Aunado a lo anterior, los ciberdelincuentes no se han limitado a la mensajería tradicional. Hoy es evidente su incursión masiva en aplicaciones de mensajería instantánea y redes sociales (servicios OTT), donde operan verdaderas plataformas de *"phishing-as-a-service"* que ponen a disposición de bandas criminales cientos de plantillas de páginas falsas y herramientas automatizadas para el envío de mensajes a través de SMS, **chats y redes sociales**[4], en campañas que alcanzan a usuarios en más de un centenar de países, presentándose como una evolución en la profesionalización del delito cibernético[5].

---

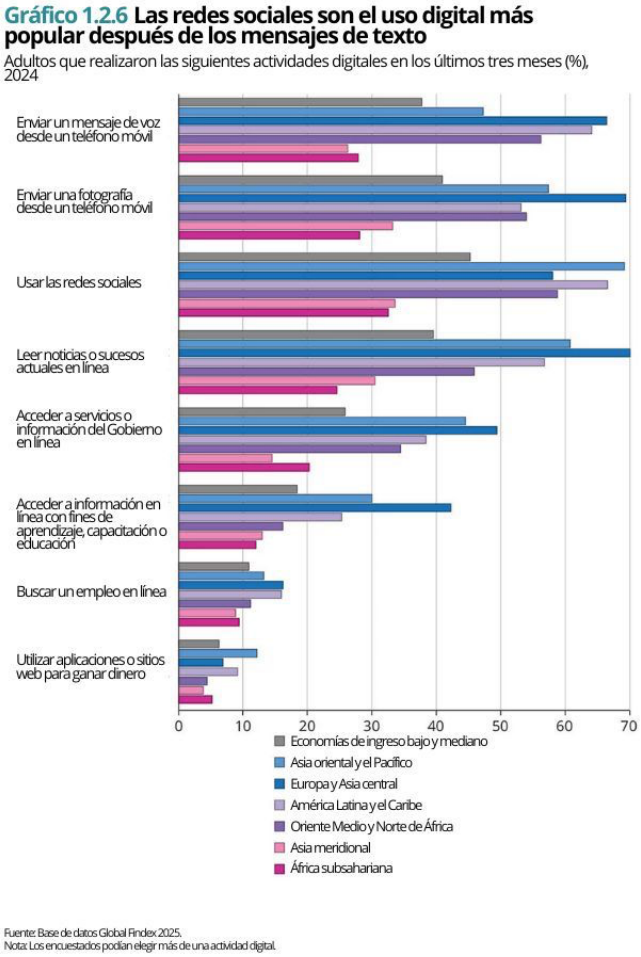
[1] https://www.mindefensa.gov.co/defensa-y-seguridad/datos-y-cifras/informacion-estadistica
[2] https://www.cali.gov.co/loader.php?idFile=100040&lFuncion=descargar&lServicio=Tools2
[3] https://keepnetlabs.com/blog/smishing-statistics-the-latest-trends-and-numbers-in-sms-phishing
[4] https://www.santander.com/es/stories/estafas-a-traves-de-aplicaciones-de-mensajeria-instantanea-como-detectarlas-y-prevenirlas
[5] https://www.opensecurity.es/phishing-as-a-service/

Grafica 1. Mercado negro del phishing



Fuente. Ibid.

Esta diversificación de canales hace que la frontera entre *"servicios de telecomunicaciones"* y *"servicios digitales"* sea cada vez más difusa desde la perspectiva del usuario y, especialmente, desde la óptica del riesgo.



En este escenario, resulta evidente que circunscribir la discusión regulatoria al ámbito de los servicios de voz y SMS móviles, como lo viene haciendo actualmente la CRC en documentos y actuaciones orientados a la mitigación del fraude cibernético y de episodios de smishing y phishing asociados principalmente al uso de mensajes de texto, no es suficiente para enfrentar la totalidad de un problema que actualmente se potencia, en su mayoría , a través del tráfico de datos y del uso intensivo de plataformas digitales.

La necesidad de revisar los impactos desde el rol de las aplicaciones de mensajería y redes sociales es también necesario para buscar una solución regulatoria integral acorde con la realidad del ecosistema digital.

- **Medidas específicas aplicables a los OTT.**

De ahí que, cobre plena relevancia que la Comisión aborde un proyecto normativo que permita garantizar la protección de los derechos de los usuarios integralmente, enfocada en establecer medidas específicas que sean aplicables a los proveedores OTT, en su calidad de titulares y administradores de las plataformas digitales a través de las cuales se materializan la mayor parte de estas conductas.

Estas medidas deberían contemplar, entre otros elementos, obligaciones de debida diligencia, mecanismos de detección y bloqueo o suspensión de los contenidos manifiestamente fraudulentos, protocolos de atención a incidentes, esquemas de reporte y cooperación con las autoridades, y reglas de transparencia respecto de las campañas y cuentas que sean identificadas como vectores de fraude.

Cabe señalar que, los PRSTM cumplen, la función de canal de transmisión, a través del cual, circula información que **no puede ser interceptada, ni analizada** en cuanto a su contenido, respetando siempre los límites legales sobre la inviolabilidad de las comunicaciones y el derecho a la intimidad. Su función corresponde a la de un transportador de tráfico, y no a la de un editor o moderador del contenido que circula por sus redes.

Por ello, el análisis y las medidas de control deben centrarse en la fuente: las plataformas y servicios digitales en los que se generan, alojan y distribuyen las campañas fraudulentas a través de servicios OTT.

Sólo a partir de un enfoque que reconozca la corresponsabilidad de estos actores y, no de los operadores de red, a partir de la asignación de cargas regulatorias debidamente aplicadas, será posible diseñar un marco de intervención eficaz que reduzca de manera significativa la materialización de las distintas modalidades de hurto y fraude cibernético que hoy afectan a los usuarios. Debe reconocerse que los prestadores de servicios de telecomunicaciones somos una víctima adicional en la cadena de fraude, puesto que los ciberdelincuentes también se especializan en vulnerar todos los controles para cometer las conductas descritas.

1.2. Se requieren medidas costo-eficientes contra el dinamismo del fraude

La implementación de herramientas tecnológicas para prevenir y/o mitigar el fraude constituye un camino que ayuda a enfrentar este flagelo, en la medida en que permite fortalecer capacidades de detección, reacción y contención frente a eventos cada vez más sofisticados.

No obstante, debe reconocerse que **el fraude es un fenómeno altamente dinámico y adaptativo**. Los actores maliciosos ajustan continuamente sus métodos, infraestructuras y tácticas para evadir controles, explotando la asimetría de información y la velocidad con la que pueden cambiar de dominios, numeración, identidades o rutas de envío. En ese contexto, las herramientas tecnológicas que resultan efectivas en un momento determinado pueden perder eficacia en plazos cortos, quizás en horas, no por fallas intrínsecas, sino por la evolución natural de las técnicas de ataque y la capacidad de los defraudadores de probar, cambiar y eludir barreras de manera inmediata e iterativa.

Bajo esa realidad, la discusión regulatoria y la estrategia sectorial no deberían centrarse exclusivamente en la expectativa de *"soluciones tecnológicas definitivas"* ni imponer un estándar de control que, por su complejidad o costos, resulte difícil de sostener en el tiempo que, además, perdería su uso en el corto tiempo, tal como se ha expuesto anteriormente. Por el contrario, es necesario enfocarse y privilegiar acciones que, permitan atacar de manera contundente a los agentes fraudulentos y neutralizar de manera muy ágil las fuentes en donde se originan dichos contactos o interacciones con fines fraudulentos.

Así las cosas, cualquier paquete de medidas debe considerar criterios de proporcionalidad y sostenibilidad económica para los PRST, evitando exigir inversiones desmesuradas que serán ineficientes frente a la velocidad de adaptación del fraude.

Consideramos que una medida eficaz es robustecer el sistema sancionatorio para los asignatarios de recursos de identificación, específicamente los así como los Carrier internacionales y los Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos quienes actualmente tienen entre sí sus responsabilidades diluidas,; este aspecto resulta ser clave en la lucha antifraude, pues es una herramienta de desincentivo real del fraude; enfocar los esfuerzos sólo en la detección del fraude, sin que las autoridades investiguen e identifiquen los responsables es una estrategia costosa que sólo promueve el cambio de modalidades de los agentes delictivos. La experiencia internacional muestra que las medidas puramente técnicas generan efectos temporales, mientras que los esquemas de atribución de responsabilidad y sanción producen impactos sostenidos.

1.3. Aclaración de obligaciones de los PCA e Integradores Tecnológicos (IT)

1.3.1. Configuraciones prestación del servicio de envío de SMS A2P

Uno de los principales inconvenientes al indagar por la atribución de responsabilidades cuando se detecta un caso de smishing es la indeterminación del sujeto obligado dentro de la cadena de

provisión del servicio de mensajería A2P, debido a que la regulación carece de obligaciones especificas según el rol de cada asignatario de códigos cortos. Esta situación genera vacíos de exigibilidad y debilita la eficacia de cualquier esquema preventivo, en la medida en que no existe un marco que atribuya deberes y consecuencias para todos los actores que pueden intervenir materialmente en el envío y entrega de SMS al usuario final.

Para abordar este punto, es necesario partir de las definiciones vigentes en la Resolución CRC 5050 de 2016.

En primer lugar, el PCA se define como:

> *"**PROVEEDORES DE CONTENIDOS Y APLICACIONES (PCA):** <Definición modificada por el artículo 2 de la Resolución 7811 de 2025. El nuevo texto es el siguiente:> **Agentes responsables directos** por la producción, generación o consolidación de contenidos o aplicaciones a través de redes de telecomunicaciones. **Estos actores pueden o no estar directamente conectados con el o los PRST sobre los cuales prestan sus servicios**. Quedan comprendidos bajo esta definición todos aquellos actores que presten sus funciones como productores, generadores o agregadores de contenido." (NSFT)*

En segundo lugar, el IT se define como:

> *"**INTEGRADOR TECNOLÓGICO:** Agente responsable de la **provisión de infraestructura de conexión y de soporte** entre los PRST y los **PCA sin conexión directa con los PRST**." (NFT)*

A partir de estas definiciones, se advierte que un PCA puede, en determinados casos, solaparse funcionalmente con actividades típicas de un IT, lo que habilita múltiples configuraciones de mercado para el envío de SMS, y con ello una mayor complejidad para determinar responsabilidades cuando ocurre un caso de fraude.

En efecto, el envío de SMS hacia el usuario final puede estructurarse, al menos, bajo los siguientes escenarios:

Escenario 1: El cliente contrata un PCA que se conecta directamente al PRST.

Esta configuración permite que un PCA al tener conexión directa con un PSRT no requiera los servicios de un IT.

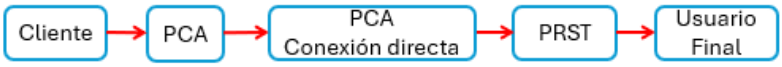
Escenario 2: El cliente contrata un PCA que no se conecta directamente al PRST, el cual contrata un IT para realizar la conexión con el PRST.

Esta configuración permite que un PCA que no tiene conexión directa con un PSRT requiera los servicios de un IT para realizar la interconexión con el PRST.

Escenario 3: El cliente contrata un PCA que se conecta directamente al PRST, pero este PCA contrata un IT para realizar la interconexión con el PRST.

Esta configuración permite que un PCA que tiene conexión directa con un PSRT, decida no establecer comunicación directamente con un PRST y en calidad de PCA prefiera hacerlo a través de un IT.

Escenario 4: El cliente contrata un PCA que no se conecta directamente al PRST, el cual contrata otro PCA que si se conecta de forma directa al PRST.



Esta configuración permite que un PCA que no tiene conexión directa con un PSRT, decida contratar un PCA que si tiene conexión directa con este, ofreciéndole los servicios de interconexión y soporte con un PRST.

Escenario 5: El cliente actúa como PCA y contrata un IT para conectarse al PRST.

Esta configuración permite que un cliente que a su vez actúa como un PCA requiera los servicios de un IT para realizar la interconexión a un PRST, condición observada en entidades financieras que se constituyen como PCA y han solicitado ser asignatarios de códigos cortos.

Escenario 6: El cliente actúa como PCA y contrata otro PCA que se conecta de forma directa al PRST.

Esta configuración permite que un cliente que a su vez actúa como un PCA contrate un PCA que si tiene conexión directa con este, el cual le ofrece los servicios de interconexión y soporte con un PRST para realizar la conexión con este.

Adicionalmente, la complejidad se acentúa porque el ordenamiento reconoce expresamente que tanto PCA como IT pueden ocupar una posición jurídica equivalente frente al recurso de

numeración. En particular, el artículo 6.4.1.3 de la Resolución 5050 de 2016 (modificado por la Resolución 7811 de 2025) dispone que:

> *"ARTÍCULO 6.4.1.3. ASIGNATARIOS DE LA NUMERACIÓN DE CÓDIGOS CORTOS PARA SMS Y USSD. <Artículo modificado por el artículo 97 de la Resolución 7811 de 2025. El nuevo texto es el siguiente:>* ***Podrán solicitar y ser asignatarios de códigos cortos los PCA y los integradores tecnológicos (IT)*** *que provean servicios de contenidos o aplicaciones a través de SMS y USSD, así como los PRST en su condición de PCA.*
>
> *Los PCA e IT extranjeros podrán ser asignatarios de códigos cortos siempre que hayan establecido una sucursal en Colombia, en los términos de las disposiciones legales y reglamentarias previstas para el efecto." (NFT)*

Sin embargo, pese a que ambos actores pueden ubicarse en una posición equivalente desde el punto de vista de la asignación del recurso (códigos cortos), el régimen vigente sólo contempla de manera expresa obligaciones para los PCA respecto del acceso a las redes móviles para la provisión de contenidos y aplicaciones mediante SMS/USSD (artículo 4.2.2.2).

> *"ARTÍCULO 4.2.2.2. OBLIGACIONES DE LOS PCA. <Artículo modificado por el artículo 76 de la Resolución 7811 de 2025. El nuevo texto es el siguiente:>* ***Son obligaciones de los PCA respecto del acceso a las redes de telecomunicaciones de servicios móviles*** *para la provisión de contenidos y aplicaciones prestados a través del envío de SMS/USSD las siguientes: (...)" (NFT)*

De igual forma, las obligaciones relacionadas con la identificación del asignatario recaen únicamente sobre los PCA, dejando por fuera a los IT, pese a que estos también pueden ostentar la calidad de asignatarios de códigos cortos.

> *"ARTÍCULO 2.1.19.9. IDENTIFICACIÓN DEL PCA. <Artículo adicionado por el artículo 5 de la Resolución 6522 de 2022. El nuevo texto es el siguiente:> En el envío de mensajes a través de SMS o USSD, con fines comerciales o publicitarios, se deberá informar a los usuarios el nombre, la marca* ***o la razón social del PCA*** *responsable de la provisión de contenidos y aplicaciones. El cumplimiento de esta obligación deberá hacerse al principio o al final de cada sesión, mensaje o un grupo de mensajes concatenados según lo que aplique." (NFT)*

En consecuencia, se evidencia una asimetría regulatoria: la norma reconoce que los IT y PCA pueden ser asignatarios y pueden intervenir materialmente en la cadena de envío, pero sólo impone obligaciones explícitas a los PCA en el marco del acceso. Esta brecha facilita tanto el "traslado" como la dilución de responsabilidades entre estos agentes y debilita el esquema de prevención del fraude, pues un eslabón relevante (IT) puede quedar sin deberes expresos pese a desempeñar un rol crítico de conexión y soporte. Por lo anterior, resulta necesario que el marco regulatorio incorpore obligaciones específicas para los IT en relación con el acceso a las redes móviles y la provisión de SMS/USSD; **incluso tales obligaciones deberían ser idénticas para ambos agentes** y así revertir el efecto nefasto de dilución de responsabilidades que hoy se observa, convirtiéndolo en un círculo virtuoso en el que ambos agentes, de manera colaborativa

para evitar la sanción y propender por el bien de los usuarios finales, tienen que preocuparse, mutuamente, y responsabilizarse, mutuamente, de velar por la calidad de los contenidos que envían hacia las redes de los PRST. Así entonces, tanto quien puede solicitar el recurso de identificación, como quien tiene el rol de utilizarlo a través del acceso que establezca con las redes de los PRST **no puede quedar fuera del régimen de obligaciones mínimas**, independientemente de su rol contractual. de forma coherente con su participación efectiva en la cadena y con la posibilidad de ser asignatarios de códigos cortos, cerrando así las zonas grises que hoy permiten diluir responsabilidades frente a eventos de smishing.

Finalmente, es importante mencionar que, la conducta irresponsable y negligente de algunos PCAs y sus Integradores Tecnológicos ponen en riesgo la reputación y la imagen de las compañías que prestan el servicio de la red de acceso, toda vez que, los suscriptores de la red suelen señalar a las Compañías de red de acceso como responsables de los ataques de "Phishing" o "Smishing" de que son víctimas, sólo por ser la red de acceso, cuando, como lo establece la regulación vigente, el PCA asignatario del código es el responsable del uso del mismo.

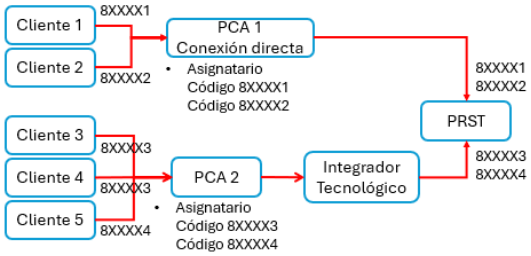
1.3.2. Autorización del uso de Códigos Cortos (CC) entre Asignatarios

Aunado a lo expuesto en el numeral anterior, se han evidenciado situaciones en las que un asignatario autoriza o "presta" a un tercero el uso de un CC asignado a su nombre, para que este último lo utilice en el envío de SMS/USSD. Esta práctica genera dificultades desde el punto de vista regulatorio, toda vez que, no se encuentra expresamente prevista ni regulada en la Resolución CRC 5050 de 2016, lo que limita la posibilidad de restringir, condicionar o prohibir su implementación y, en particular, dificulta la determinación del sujeto responsable ante usos indebidos asociados a fraudes como el smishing.

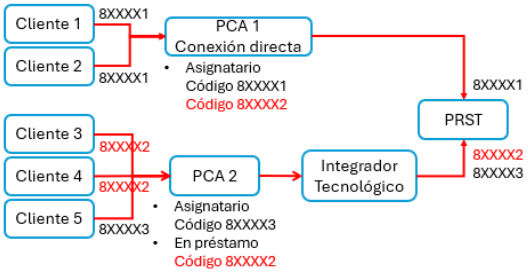
En efecto, el marco normativo contempla mecanismos formales de cesión o transferencia de la asignación de los recursos de identificación, bajo condiciones y procedimientos específicos. Sin embargo, la figura de una "autorización de uso" o "préstamo temporal" sin transferencia formal del recurso, puede generar un desalineamiento entre (i) quien figura como asignatario ante el administrador del recurso, y (ii) quien efectivamente origina el tráfico, gestiona campañas o define el contenido del mensaje. Esta brecha crea un escenario propicio para la dilución de responsabilidades, al permitir que, ante incidentes, se alegue que el uso fue realizado por un tercero "autorizado", sin que exista un marco claro de deberes, obligaciones, trazabilidad y control sobre dicha autorización. El "autorizado", si la CRC continúa permitiendo dicha figura, como generador de tráfico también debería tener las mismas obligaciones asociadas a la prevención del fraude, que las que tiene el asignatario.

Bajo esta lógica, se identifican los siguientes escenarios que podrían estarse configurando y que incrementan el riesgo de uso indebido:

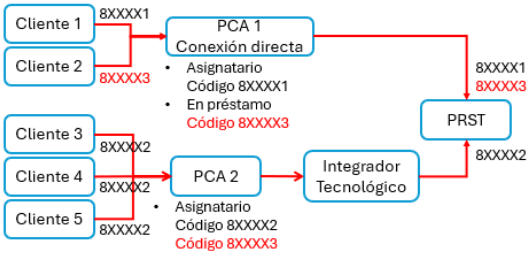
Escenario 1: El PCA es asignatario del CC y hace uso propio. (Situación esperada).



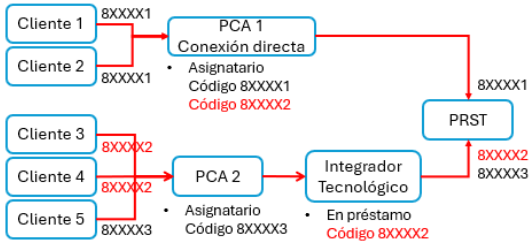
Escenario 2: El PCA 1 es asignatario de un CC y "autoriza" su uso al PCA 2.



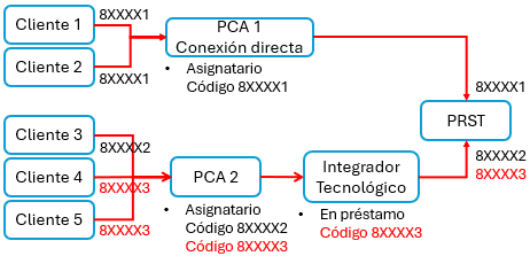
Escenario 3: El PCA 2 es asignatario de un CC y "autoriza" su uso al PCA 1.



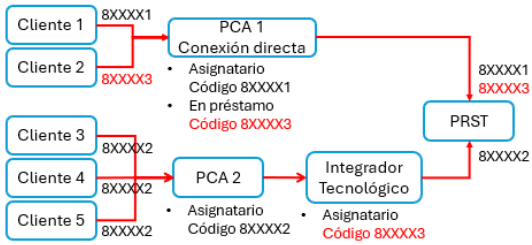
Escenario 4: El PCA 1 es asignatario de un CC y "autoriza" su uso al IT.



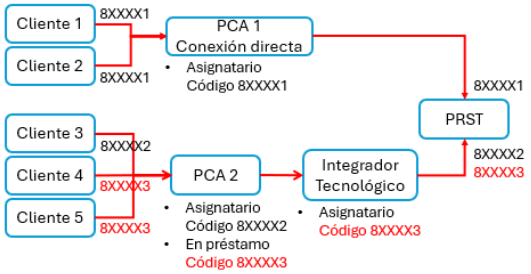
Escenario 5: El PCA 2 es asignatario de un CC y "autoriza" su uso al IT.



Escenario 6: El IT es asignatario del CC y "autoriza" su uso al PCA 1.



Escenario 7: El IT es asignatario del CC y "autoriza" su uso al PCA 2



Colombia Móvil S.A. E.S.P.
Cra 50 # 96-12
Bogotá.D.C.
Conmutador (601) 325 15 05

En conclusión, la ausencia de tipificación y regulación expresa de la "autorización de uso" o "préstamo" del código corto por terceros permite configuraciones contractuales y técnicas que debilitan la trazabilidad, facilitan el desplazamiento y/o la dilución de responsabilidades y reducen la efectividad de las medidas de prevención de fraude. Por ello, resulta necesario que en el marco regulatorio **se prohíba de forma explícita** este tipo de prácticas.

2. COMENTARIOS ALTERNATIVAS REGULATORIAS

2.1. Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

Durante la presentación de alternativas para abordar esta temática, se incorpora la definición de ***agregador*** como *"empresas que envían SMS en nombre de otras"*. Sin embargo, dicha definición no se encuentra actualmente prevista en la Resolución CRC 5050 de 2016, por lo que resulta necesario precisar su alcance y efectos regulatorios. En particular, no es claro si esta categoría pretende **cobijar o diferenciar** a los actuales agentes que, en la práctica, pueden ostentar la calidad de asignatarios de códigos cortos, tales como los PCA y los IT.

En esa misma línea, el documento sugiere que los agregadores deben verificar la legitimidad de sus clientes (marcas), lo cual podría interpretarse como una obligación dirigida principalmente a quienes mantienen una relación comercial directa con dichas marcas (típicamente, los PCA). Si esa fuese la intención, la medida quedaría incompleta en su alcance y ámbito de aplicación, debido a que se estarían dejando por fuera a los IT quienes, además de los vacíos de responsabilidad actuales para estos agentes, ellos también pueden ser asignatarios de códigos cortos y, por tanto, podrían habilitar directa o indirectamente el envío de SMS bajo su asignación. En tal escenario, se generaría una asimetría regulatoria y un incentivo a reconfigurar modelos de operación para eludir controles, trasladando el riesgo hacia los eslabones menos exigidos.

Por lo anterior, las medidas que se definan deberían estructurarse bajo un principio de cobertura completa del riesgo: las obligaciones de debida diligencia, trazabilidad, controles de abuso y verificación de legitimidad **deben recaer sobre todo asignatario de códigos cortos y sus integradores tecnológicos**, así como, **sobre los asignatarios de numeración E.164** (en el caso de que se habilite esta numeración para el envío de mensajes SMS con fines comerciales o publicitarios y mensajes transaccionales), con independencia de la denominación comercial o rol operativo que adopten (PCA, IT u otras figuras que se introduzcan). Excluir a alguno de estos sujetos no sólo crearía zonas grises, sino que podría facilitar la persistencia de prácticas fraudulentas, al permitir que actores maliciosos migren hacia el canal menos regulado dentro de la misma cadena de valor.

2.1.1. **TEMÁTICA 1: Falta de identificación clara del remitente en SMS A2P**

2.1.1.1. Alternativa 1: Statu quo

RTA. Conforme al problema identificado, es necesario establecer medidas regulatorias que permitan mitigar los fraudes que se cometen a través del servicio de mensajería de texto corto SMS, por tanto, **se descarta esta alternativa**.

2.1.1.2. Alternativa 2: Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID)

RTA. Si bien esta alternativa podría facilitar que el usuario identifique el nombre de la entidad originadora del mensaje (marca), ello no garantiza, por sí mismo, que el usuario no termine siendo víctima de una campaña de smishing. En la práctica, la simple visualización del *"remitente"* puede incluso generar una **falsa sensación de legitimidad**, especialmente cuando los atacantes logran suplantar marcas reconocidas o replicar elementos de identidad que el usuario asocia con comunicaciones auténticas.

De hecho, se han presentado casos recientes en los que usuarios recibieron mensajes de texto que aparentaban provenir de su propio operador móvil; lejos de evitar el fraude, la aparente identificación del remitente aumentó la credibilidad del mensaje y facilitó que el usuario realizara acciones de riesgo (p. ej., abrir enlaces o entregar información). Esto evidencia que la identificación del originador, entendida como una medida de *"visibilidad"* para el usuario, no es necesariamente una barrera efectiva frente a amenazas basadas en ingeniería social.

En ese sentido, esta medida, considerada de manera aislada, no constituye una respuesta suficiente para enfrentar el fraude. Su mayor valor podría materializarse si se articula como insumo dentro de un esquema de trazabilidad y atribución del tráfico como el planteado en la temática 2, en el cual la identificación del originador no solo sea un elemento informativo, sino un componente que permita rastrear el recorrido del mensaje de inicio a fin.

2.1.1.3. Alternativa 3: Asignación y uso de código alfanumérico solo para tráfico transaccional

RTA. En línea con lo señalado en la respuesta anterior, la posibilidad de que el usuario identifique el supuesto origen del mensaje no necesariamente reduce el riesgo de smishing; por el contrario, puede convertirse en un factor habilitante para la materialización del fraude, en la medida en que incrementa la percepción de legitimidad del mensaje y facilita la efectividad de la ingeniería social empleada por el estafador.

Conforme lo anterior, consideramos que ninguna de estas alternativas tendría un impacto directo en el fin propuesto que es mitigar el fraude cibernético mediante SMS, por lo que de manera respetuosa solicitamos no implementar estas medidas.

En este sentido, consideramos que las medidas con mayor potencial de efectividad son aquellas orientadas a **fortalecer la atribución única de un código corto por**

marca que permita tener la trazabilidad del origen del mensaje, así como, el asignatario responsable del debido uso del código corto. Bajo esa lógica, destacamos que las alternativas planteadas en la Temática 2 abordan una mejor perspectiva para abordar esta problemática.

2.1.2. TEMÁTICA 2: Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude

Las alternativas planteadas en esta temática las cuales están orientadas a garantizar la asignación de un identificador único por marca, ya sea mediante la implementación de Sender ID o mediante la asignación de un código corto o un E.164 exclusivo, podrían generar un impacto significativamente más efectivo en la contención del fraude a través de SMS, en la medida en que fortalecen la atribución del tráfico, mejoran la trazabilidad y reducen la posibilidad de suplantación del originador. Este efecto se potencia, además, si dichas medidas se complementan con obligaciones de debida diligencia (KYC) sobre la marca/cliente y con la habilitación de mecanismos para bloquear o restringir tráfico no verificado o que no cumpla requisitos mínimos de autenticidad.

No obstante, se observa que dentro de esta misma temática se plantea una medida asociada a la categorización del contenido y consentimiento del usuario (articulación con RNE), la cual no guarda una relación directa con la problemática específica de fraude cibernético en la modalidad de smishing. En términos regulatorios y operativos, incorporar este tipo de obligaciones podría implicar el despliegue de capacidades adicionales, con impactos relevantes en recursos y costos de implementación, sin que ello se traduzca necesariamente en una reducción efectiva del fraude.

Sobre este punto, resulta pertinente recordar que recientemente se adelantó la implementación de la Resolución CRC 7356 de 2024 *"Por la cual se modifican disposiciones sobre el Registro de Números Excluidos contenidas en el Capítulo 1 del Título II de la Resolución CRC número 5050 de 2016 y se dictan otras disposiciones."*, cambio motivado por las disposiciones contenidas en la Ley 2300 de 2023 conocida como la Ley *"Dejen de fregar"*. En consecuencia, introducir nuevas obligaciones regulatorias sobre consentimiento y categorización, podría desbordar el alcance del proyecto, generar solapamientos normativos y elevar la complejidad de articulación con una norma de jerarquía superior ya vigente e implementada, sin aportar una solución real y proporcional al núcleo del problema: la prevención y mitigación del fraude cibernético materializado mediante SMS.

2.1.2.1. Alternativa 1: Statu quo

RTA. Conforme al problema identificado, es necesario establecer medidas regulatorias que permitan mitigar los fraudes que se cometen a través del servicio de mensajería de texto corto SMS, por tanto, se descarta esta alternativa.

2.1.2.2. Alternativa 2: Proceso de validación centralizado de originadores de contenido

RTA. Para un adecuado entendimiento y correcta implementación de esta iniciativa, resulta indispensable que, de manera previa, se aclare y delimite la definición de ***"agregador"***, conforme se expuso anteriormente. Desde TIGO, consideramos que las obligaciones asociadas a estos actores deben recaer, de forma expresa, sobre quienes ostentan la calidad de asignatarios de códigos cortos, esto es, PCA e IT, en tanto son a quienes les habilitaron su uso y deben velar por el uso eficiente de este recurso escaso. En este sentido, medidas como la debida diligencia (KYC) y la adopción de reglas mínimas de monitoreo y control (filtros antifraudes o Firewall) constituyen requisitos necesarios para que los agregadores contribuyan efectivamente a la prevención y mitigación del fraude.

Por otra parte, la alternativa orientada a habilitar un proceso de validación centralizado a través de un tercero podría dar mayor control sobre el tráfico SMS, en la medida en que permitiría validar, de forma previa, la marca, el agregador y la campaña asociada al tráfico, habilitando una gestión preventiva frente a intentos de suplantación o campañas fraudulentas. En principio, este enfoque contribuiría a robustecer la trazabilidad y reducir la dependencia de controles reactivos posteriores al incidente. En este aspecto se sugiere que la Comisión en calidad de Administradores de los Recursos de Identificación este a cargo del seguimiento y control de las actividades que el validador este ejecutando.

No obstante, es necesario que la CRC precise expresamente la asignación de responsabilidades sobre los costos de implementación, operación y soporte del proveedor que centralice dicha validación. En particular, estos costos deberían ser asumidos por los asignatarios de los códigos cortos (PCA e IT), quienes se benefician directamente del uso del recurso y controlan la relación con la marca/campaña; en ningún caso deberían trasladarse a los PRST, que actúan como red de transporte y terminación del tráfico y que no controlan el origen comercial del mensaje.

En lo que respecta a los PRST, su carga debería limitarse a los costos estrictamente asociados a la implementación técnica de los mecanismos necesarios para: (i) consultar o verificar el "paquete" de identificadores válidos; y (ii) ejecutar la suspensión temporal del tráfico que no incorpore dicha validación. Esto, en la medida en que se trata de adecuaciones de red para hacer exigible una regla definida por el esquema de validación, sin que ello implique asumir el costo del proceso de certificación/validación en sí mismo.

Sin embargo, esta iniciativa plantea inquietudes relevantes sobre el esquema de inspección, vigilancia y control aplicable al proveedor que ejercerá las funciones de validador. Adicionalmente, existe el riesgo de que se cursen mensajes hacia los PRST con validaciones adulteradas o manipuladas, ya sea por alteración del paquete de identificadores únicos, suplantación del validador, o uso de credenciales comprometidas.

Asimismo, la posibilidad de que los PRST suspendan o restrinjan el tráfico no validado se considera una medida necesaria. Sin embargo, desde una perspectiva de eficiencia y control del riesgo y operativa, el tráfico que no cuente con el paquete de identificadores válidos no debería siquiera llegar a ser cursado hacia los PRST. El bloqueo debería realizarse en el origen de la cadena, es decir, por parte del agregador, PCA o IT, quienes deben asumir la responsabilidad por la filtración articulada y preventiva, así como las consecuencias regulatorias y operativas derivadas de no hacerlo. Permitir que el PRST se convierta en el punto primario de contención incrementa cargas de trafico de red innecesarias, complejiza la operación y mantiene abierta la posibilidad de que el tráfico fraudulento circule parcialmente antes de ser descartado.

Finalmente, se considera necesario que la Comisión acompañe estas alternativas con un análisis costo–beneficio que evalúe su pertinencia, proporcionalidad y viabilidad, incluyendo costos de implementación y operación comparadas frente a las demás alternativas. Este análisis es clave para asegurar que las medidas adoptadas sean idóneas, necesarias y eficientes frente al objetivo de mitigación del fraude cibernético.

2.1.2.3. Alternativa 3: Proceso de validación distribuido (DLT)

RTA. En línea con lo señalado en la respuesta anterior, las medidas planteadas de trazabilidad son un atributo importante para poder identificar responsables en la prestación del servicio A2P.

Por otra parte, acá se presenta la implementación de un mecanismo de validación distribuido lo cual podría incorporar ventajas propias de los sistemas descentralizados tales como integridad de la información, trazabilidad, inmutabilidad de registros y una mayor resiliencia frente a manipulaciones, atributos comúnmente asociados a arquitecturas tipo blockchain.

No obstante, para determinar su conveniencia regulatoria y operativa, resulta indispensable que la Comisión adelante un análisis costo–beneficio que permita evaluar su pertinencia y viabilidad, considerando, entre otros aspectos, los costos de implementación y operación, la complejidad de gobernanza del esquema, los impactos en tiempos de procesamiento y la interoperabilidad entre actores.

2.1.2.4. Alternativa 4: Identificación exclusiva mediante códigos cortos y numeración E.164, o códigos alfanuméricos

RTA. **Consideramos que esta alternativa es la más propicia para abordar esta temática**. Esta numeración permite configurar texto para que el usuario pueda identificar el remitente (temática 1) y con la asignación única de un identificador por marca, permitiría la trazabilidad de las campañas que se ejecutan, facilitando la identificación y gestión de incidentes en caso de presentarse fraude.

Una ventaja relevante frente a las alternativas previas es que no requiere la intervención de un tercero (centralizado o distribuido) para validar marcas, agregadores, campañas o la estructura/contenido del mensaje, lo que podría traducirse en **menores costos de implementación** y en la reducción de costos recurrentes asociados a operación, mantenimiento y soporte de un proveedor externo, simplificando además el modelo de gobernanza del esquema.

Adicionalmente, al eliminarse la necesidad de esperar una validación externa para autorizar el envío de campañas, se reduce el riesgo de demoras operativas que puedan afectar el tiempo de salida al mercado (time-to-market). Esto resulta particularmente relevante en entornos competitivos, donde la capacidad de reaccionar de manera oportuna (por ejemplo, frente al lanzamiento de una campaña legítima de un competidor) puede contribuir a estimular la competencia y evitar barreras indirectas derivadas de procesos de aprobación o certificación.

Ahora bien, en esta alternativa, la validación recaería en un mecanismo de verificación a cargo de los agregadores (KYC), lo cual añade una capa preventiva orientada a asegurar, al menos, que las empresas que originan tráfico estén legalmente constituidas, cuenten con un responsable identificable y exista un punto de contacto verificable para responder ante incidentes. Esta medida, aunque no equivale a una validación exhaustiva del contenido o de la campaña, sí contribuye a reducir el anonimato y a mejorar la capacidad de atribución de responsabilidades.

Finalmente, resulta igualmente **necesario que los PRST cuenten con la facultad de restringir o suspender tráfico cuando se identifiquen indicios de campañas fraudulentas**. No obstante, dado que en esta alternativa no existiría un paquete de identificadores previamente validados por un tercero, se hace indispensable establecer criterios objetivos y verificables de actuación, mediante reglas basadas en patrones de tráfico con parámetros claramente definidos por la Comisión. La implementación operativa de dichas reglas debería recaer en los agregadores (PCA e IT), en su calidad de asignatarios de códigos cortos y de responsables de la relación de acceso hacia los PRST, de manera que puedan suspender preventivamente los envíos que cumplan con tales criterios antes de su cursado hacia las redes de los PRST.

Adicionalmente, resulta pertinente habilitar mecanismos de reacción ante reportes de usuarios por la recepción de mensajes con contenido sospechoso, que **permitan a los PRST adoptar medidas de suspensión temporal preventiva** del tráfico asociado al identificador reportado. En estos eventos, podría contemplarse la suspensión mientras se adelanta la verificación con el agregador.

2.1.3. TEMÁTICA 3: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

2.1.3.1. Alternativa 1: Statu quo

RTA. La regulación vigente contempla disposiciones orientadas a la prevención del fraude, conforme a los lineamientos establecidos en el Artículo 2.1.10.7 de la Resolución CRC 5050 de 2016. En virtud de este marco, los operadores se encuentran facultados para hacer uso de herramientas tecnológicas destinadas a prevenir la comisión de fraudes a través de sus redes, facultad que no se circunscribe exclusivamente al tráfico A2P, sino que puede extenderse a otros escenarios de uso, incluido el P2P.

En ese contexto, no se evidencia la situación descrita en esta temática según la cual, en el mercado colombiano, "no se contempla un control" sobre el tráfico SMS P2P. Por lo tanto, consideramos que los supuestos identificados en esta temática ya se encuentran amparados por el esquema normativo actual.

2.1.3.2. Alternativa 2: Control de patrones de tráfico atípicos

RTA. Conforme la respuesta anterior, no consideramos necesario la implementación de medidas adicionales, por lo que de manera respetuosa solicitamos descartar esta alternativa.

2.1.3.3. Alternativa 3: Límite de SMS P2P por usuario

RTA. Conforme la respuesta a la alternativa 1, no consideramos necesario la implementación de medidas adicionales, por lo que de manera respetuosa solicitamos descartar esta alternativa.

2.2. Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

La CRC ha propuesto las siguientes cuatro alternativas relacionadas con el fraude a través de los servicios de voz:

- Limitar el enmascaramiento de la identidad de la línea llamante de origen internacional.
- Establecer mecanismos de filtrado del tráfico de voz.
- Establecer diferencia de la numeración de uso personal de la de uso comercial y publicitario.
- Estandarizar la aplicación de listas de no originación (DNO)

Identificamos que, entre las propuestas orientadas a la detección y prevención, diferenciar la numeración de uso personal de la numeración de uso comercial resulta técnicamente viable en el mediano plazo, con una implementación a costos razonables. Esta medida permitiría que, a través de la experiencia del usuario y campañas de comunicación, la ciudadanía reconozca con mayor facilidad el origen comercial o

publicitario de las llamadas, fortaleciendo su criterio para rechazar comunicaciones potencialmente riesgosas.

Adicionalmente, dicha diferenciación facilitaría, cuando sea aplicable, asociar el número a entidades o campañas específicas, incrementando la trazabilidad del tráfico. Finalmente, permitiría al sector segmentar estadísticamente el uso de la numeración comercial, identificar tendencias de este mercado y, con base en evidencia, ajustar progresivamente las condiciones de uso y explotación de este recurso.

Sobre las demás alternativas no encontramos mayores beneficios respecto del control del fraude, y de manera general exponemos las siguientes dificultades que son ampliadas en el análisis particular de cada una de ellas.

- Respecto del enmascaramiento la CRC propone que se prevenga en tiempo real y se bloqueen las llamadas en las que se identifique esta práctica, sobre esto resaltamos la imposibilidad técnica para detectar el enmascaramiento en tiempo real, y el perjuicio que se puede ocasionar al usuario en los casos en que el bloqueo resulte en un falso positivo.

- Sobre las estrategias de filtrado de voz la CRC propone el análisis en tiempo real de valores estadísticos como los tiempos de duración de llamada o el volumen de llamadas realizadas por un número específico y, a través de estos análisis advertir al usuario o ejecutar acciones de bloqueo. Sobre estas estrategias anotamos que su implementación en tiempo real es técnicamente inviable. El procesamiento de análisis estadísticos durante el tiempo de establecimiento de la llamada puede implicar afectaciones en los tiempos normales de funcionamiento.

  Mencionamos además, que actualmente por ejemplo, aunque en modo offline se pueden recoger estadísticas que podrían dar presunción de fraudes o mal uso de la numeración, los PRSTs no pueden adoptar medidas como bloqueos, desconexión provisional, o cuarentenas que ejerzan alguna presión sobre los carrier internacionales y mitiguen la proliferación de estos eventos de llamada, de tal manera que se han presentado en el caso de TIGO conflictos por el uso indiscriminado de las interconexiones de Larga Distancia Internacional, sin que exista alguna restricción para que los originadores hagan esfuerzos en el control y gestión de su tráfico anómalo.

- La gestión de las listas de originación en un esquema centralizado o no, puede generar ineficiencias en el uso de la numeración, por cuanto motivaría a los agentes de fraude a reemplazar con mayor rapidez la numeración que se va anexando a las listas de no originación, y no sería un mecanismo eficiente para reducir el fraude, entorpecería moderadamente la actividad, sin tener un efecto real o definitivo en su materialización. El proceso de centralización de las distribuidas implicaría establecer un mecanismo de intercambio de bases

cruzadas que causaría mayores costos en la operación, sin que esto tengan efectos significativos en el control del fraude.

En particular la implementación de las metodologías STIR/SHAKEN, requieren alcanzar una mayor globalidad y escalabilidad para que puedan ser efectivas. La implementación de estas metodologías implica esencialmente que:

- Que el Origen de las llamadas sea certificado y, que exista un tercero que controle el registro y autenticación de los originantes.

- El establecimiento de acuerdos internacionales para certificar las llamadas del exterior. La responsabilidad de la certificación debe trasladarse también a los operadores de tránsito internacional (carriers internacionales).

- Esta metodología no sería viable para protocolos de señalización SS7/ISUP y la migración a SIP es una modificación de largo plazo.

Además, las estrategias de etiquetado de las llamadas con las alertas a los usuarios ("Aceptar/Rechazar llamadas") no son gestionadas desde el CORE de las redes, y su implementación es una acción que debe coordinarse con los desarrolladores de APPs, o los fabricantes de los dispositivos, por tanto, la responsabilidad de esta implementación no puede recaer en los PRSTs.

Por último, solicitamos a la CRC considerar que la detección es sólo un mecanismo de prevención del fraude, y que la imposición de obligaciones excesivas respecto a las estrategias de detección puede tener implicaciones negativas en la percepción del servicio de los usuarios (como expusimos brevemente el potencial bloqueo de llamadas de origen legal, o el incremento en tiempos de espera para el establecimiento de llamada). De tal forma que si bien se deben gradualmente buscar alternativas de detección es importante fortalecer los procesos de investigación que permitan identificar y sancionar severamente a las entidades que originen, participen o promuevan acciones fraudulentas.

2.2.1. TEMÁTICA 1: Mecanismos de verificación, autenticación e identificación del originador de la llamada de voz, o limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) (Spoofing)

2.2.1.1. Alternativa 1: Statu quo

RTA. La CRC indica que de optar por el Statu Quo, "… *las llamadas internacionales podrían seguir presentándose ante el usuario como si fueran colombianas, sin que el PRST tenga la capacidad o la obligación de validar la autenticidad del número mostrado o la identidad de la línea llamante ….".* Llama la atención que la CRC enfoque las obligaciones únicamente en los PRSTs, sin contemplar la responsabilidad

de los carrier en la gestión y control del tráfico que originan, e incluso de establecer para ellos sanciones que motiven la verificación del tráfico que gestionan.

En el escenario actual es importante que los carrier adopten una posición determinante en el control del tráfico que gestionan, a partir de la transparencia y confiabilidad de sus acuerdos internacionales.

2.2.1.2. Alternativa 2: Prohibición total del enmascaramiento de la identidad de la línea llamante (CLI)

RTA. Esta alternativa propuesta por la CRC presenta dificultades de carácter técnico, al ser imposible o altamente costoso determinar una condición de enmascaramiento en el proceso de establecimiento de la llamada. La red recibe la información de un tercero y este tercero puede sustituir el encabezado de la llamada sin que este cambio pueda ser detectado mediante mecanismos estándar por el operador que termina la llamada.

Por otra parte, la transformación del número es en muchos casos un procedimiento estándar y completamente legal, como ocurre con el cambio de algunos numerales cortos, esta condición dificulta también la determinación de si el procedimiento es empleado con fines fraudulentos.

Resaltamos adicionalmente que esta alternativa busca imponer cargas a los PRST de identificación de las llamadas, sin imponer alguna obligación a los Carrier que son en muchos casos responsables de la originación; es importante que las medidas contemplen también la responsabilidad de los Carrier respecto de la transformación que pueden hacer de las llamadas que originan o que entregan.

La adopción de esta medida puede en algunos casos perjudicar a los usuarios, como por ejemplo, en los eventos en los que el enmascaramiento no corresponda a una actividad fraudulenta podría impedirse la comunicación.

2.2.1.3. Alternativa 3: Permitir enmascaramiento con obligación de identificación y etiquetado de llamadas para el usuario

RTA. Si bien insistimos en la dificultad para determinar la acción de *'enmascaramiento'* de la llamada, resaltamos que esta alternativa daría al usuario la posibilidad de decidir o no la contestación, lo que sin restringir su posibilidad de comunicación, le da al usuario la posibilidad de evaluar la pertinencia o no de recibir una llamada, y puede ser una alerta ante una posible acción fraudulenta.

De esta manera se pueda alertar al usuario de un posible enmascaramiento y prevenir así posibles fraudes.

2.2.1.4. Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e internacional

RTA. Esta alternativa debe considerar que el etiquetado de las llamadas es un proceso bilateral, cuya implementación requiere no sólo el esfuerzo de los PRSTs sino también de los originadores de las llamadas internacionales, por tanto, su implementación no depende exclusivamente de la acción de los PRST, y requiere de una participación coordinada de todos los agentes del sector.

Si bien la alternativa puede ser viable, es altamente costosa y no puede pretenderse que su implementación se consolide en corto o mediano plazo.

Es importante mencionar que ninguna de estas medidas tendría un impacto directo en el fin propuesto que es mitigar el fraude cibernético mediante llamadas de voz, por lo que de manera respetuosa solicitamos no implementar estas medidas.

2.2.2. TEMÁTICA 2: Falta de aplicación coordinada de métodos preventivos de filtrado de tráfico de voz

2.2.2.1. Alternativa 1: Statu quo

RTA. En este escenario cada operador aplica sus mecanismos de detección, y aunque estos mecanismos no son coordinados si pueden ser efectivos; pero la efectividad de estos mecanismos depende en buena medida de las acciones que cada operador pueda aplicar cuando identifica escenarios de fraude.

En este sentido la CRC no contempla que los operadores ejecuten acciones autónomas de bloqueo de tráfico, y esto facilita la continuidad en algunos casos de actividades identificadas con sospecha de fraude. LA CRC debería ampliar en este escenario la posibilidad de los PRSTs de tomar medidas que permitan contener los eventos de fraude.

2.2.2.2. Alternativa 2: Lineamientos regulatorios para monitoreo de tráfico

RTA. La CRC plantea en esta alternativa que en tiempo real del establecimiento de las llamadas se realice un análisis de patrones de tráfico, y con base en el diagnóstico si hay sospecha de fraude que la llamada sea bloqueada, o se notifique al usuario etiquetando la llamada como “probable fraude”. Los patrones por verificar los establecerá la CRC mediante lineamientos regulatorios que serán obligatorios.

Esta alternativa además de ser técnicamente compleja, es altamente costosa, y si bien puede ofrecer una solución temporal, en el mediano plazo los mecanismos de fraude pueden ajustarse para evitar su detección mediante los lineamientos que puedan establecerse. Y esto implicaría que las cargas económicas y obligaciones que

la CRC impondría exclusivamente a los PRST no serían efectivas, perjudicando significativamente al sector.

2.2.2.3. Alternativa 3: Creación de una plataforma de articulación e intercambio de alertas

RTA. La conformación de una plataforma para el intercambio de alertas no puede ser recargada exclusivamente en los PRST; En este caso los costos de implementación y mantenimiento de una plataforma de este tipo debe ser compartida por todas las entidades del sector que estén involucradas en su operación y consulta.

2.2.2.4. Alternativa 4: Implementación de STIR/SHAKEN/RCD

RTA. Atendiendo a nuestros comentarios preliminares sobre los mecanismos de STIR/SHAKEN; respecto a que la certificación y autenticación de las llamadas es un proceso bilateral, cuya implementación requiere no sólo el esfuerzo de los PRSTs, sino también de los originadores de las llamadas internacionales, y operadores de tránsito, por lo que la autenticación de las llamadas no depende exclusivamente de la acción de los PRST; el establecimiento de niveles de verificación podría ser una opción válida para determinar si el proceso de autenticación ha sido ejecutado o no.

La CRC propone 3 niveles de verificación. Nivel A: verificación completa, Nivel B: verificación parcial, Nivel C: sin verificación.

Insistimos que al ser una alternativa dependiente de los acuerdos y capacidades de todos los involucrados, no se constituye como una solución universal, sino más bien alternativa, lo que implica en que para aquellos casos en los que se tienen acuerdos y procedimientos para la autenticación criptográfica de llamadas mediante STIR/SHAKEN podrían anunciarse al usuario las etiquetas de verificación completa o parcial, y para los demás casos se indicaría la 'no verificación', ofreciendo al usuario la posibilidad de establecer o no la comunicación teniendo la oportunidad de identificar un posible fraude.

Es importante mencionar que ninguna de estas medidas tendría un impacto directo y definitivo en el fin propuesto que es mitigar el fraude cibernético mediante llamadas de voz, por lo que de manera respetuosa solicitamos no implementar estas medidas

2.2.3. **TEMÁTICA 3: Ausencia de diferenciación en rangos de numeración para comunicaciones personales, comerciales y publicitarias**

2.2.3.1. Alternativa 1: Statu quo

RTA. Actualmente si se presenta un uso indiscriminado de la numeración nacional con propósitos comerciales, y en este escenario para los usuarios es difícil distinguir cuando un evento de llamada es de una persona o de un agente comercial, por lo que

no puede discriminar con certeza cuando rechazar la contestación de llamadas que supondrían un fraude potencial.

2.2.3.2. Alternativa 2: Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias

RTA. La distinción de las llamadas de comunicaciones personales, de las llamadas con propósitos comerciales, a través de la creación de rangos específicos de numeración E.164, reservados exclusivamente para la originación de llamadas comerciales y publicitarias, es una alternativa técnicamente viable, y que ofrece ventajas potenciales respecto del control en la identificación del origen de las llamadas, y también en la métrica y evaluación de las comunicaciones de origen y propósito comercial que presentan perfiles diferentes a los ya conocidos de las comunicaciones personales.

En muchos casos las llamadas con fines comerciales son generadas a través de máquinas que generan ráfagas de llamadas que pueden saturar los recursos de red, y que además remiten mensajes de muy corta duración que no están alineadas con los parámetros de dimensionamiento actuales. Lo cual ocurre en detrimento de la calidad en el establecimiento de las comunicaciones. y en perjuicio de la seguridad y comodidad de los usuarios.

A nivel del fraude el tener una numeración diferenciada puede ofrecer a los usuarios la posibilidad de reconocer el origen de la llamada permitiéndole identificar a través del número si quien llama es una persona o una entidad, y así tener un criterio adicional para decidir si acepta o no la llamada, previniendo riesgos potenciales.

Para los operadores, los esfuerzos en la implementación de una alternativa como esta les ofrece una posibilidad para monitorear de manera particular el tráfico comercial y perfilar con mayor precisión sus patrones y riesgos.

2.2.3.3. Alternativa 3: Etiquetado obligatorio en el identificador de llamadas para contactos comerciales, usando la numeración actual

RTA. Al estar basada en los protocolos de STIR/SHAKEN, esta alternativa presenta las limitaciones ya mencionadas en las temáticas anteriores, y puede no ser tan efectiva por su falta de universalidad, es dependiente que todas las entidades, no sólo los PRSTs implementen los protocolos de etiquetado obligatorio y la aplicación de las reglas de consistencia.

Es importante mencionar que ninguna de estas medidas tendría un impacto directo en el fin propuesto que es mitigar el fraude cibernético mediante llamadas, por lo que de manera respetuosa solicitamos no implementar estas medidas

2.2.4. TEMÁTICA 4: Falta de estandarización en la aplicación de listas de no originación (DNO)

2.2.4.1. Alternativa 1: Statu quo

RTA. En esta temática encontramos que es viable mantener el statu quo, pues consideramos que la aplicación de las listas de no originación no es efectiva en la prevención del fraude, puesto que los números incluidos en estas listas pueden ser rápidamente sustituidos, y el desarrollo de esta dinámica limitaría el uso de la numeración, que es un recurso escaso, comprometiendo su gestión.

Es conveniente sin embargo que se ajuste en el proceso de bloqueo de los números portados, pues cuando estas líneas son recicladas por parte del operador de origen pueden aparecer bloqueadas en las listas del operador a las que en algún momento se portaron y se detectó el fraude.

2.2.4.2. Alternativa 2: Registro DNO nacional único administrado por la CRC

RTA. Aunque la centralización de las listas de números de originación por parte de la CRC permite consultar de manera unificada la numeración que se debe restringir, este procedimiento puede resultar ineficiente porque aceleraría la sustituibilidad de los números bloqueados por parte de los agentes generadores de fraude y esto ocasionaría dos inconvenientes, la actualización oportuna de las listas de no originación administrada por la CRC, y la disminución de los recursos de identificación por el crecimiento de los recursos que se restringen.

2.2.4.3. Alternativa 3: Estándar mínimo obligatorio de DNO con listas propias por PRST

RTA. La CRC mediante esta alternativa concentra nuevamente las obligaciones, y seguramente las responsabilidades por la ocurrencia de fraudes en los PRSTs, abstrayendo de responsabilidades y acciones a otros agentes del sector.

2.2.4.4. Alternativa 4: Sustitución funcional de DNO por autenticación del CLI y reglas anti-spoofing internacional STIR/SHAKEN/RCD

RTA. No es una alternativa que se pueda aplicar de modo universal, y la alternativa regulatoria concentra la responsabilidad en los PRSTs sin reconocer la participación y responsabilidades de otros agentes como los Carrier internacionales, los MVNO, e incluso las OTT.

Es importante mencionar que ninguna de estas medidas tendría un impacto directo en el fin propuesto que es mitigar el fraude cibernético mediante llamadas de voz, por lo que de manera respetuosa solicitamos no implementar estas medidas.

2.3. Temáticas enfocadas en la educación de la ciudadanía

2.3.1. TEMÁTICA 1: Acciones educativas que aumenten el conocimiento de los usuarios

2.3.1.1. Alternativa 1: Statu quo

RTA. Aun cuando no corresponde a una obligación regulatoria, entendiendo el impacto de esta problemática en la sociedad, hemos realizado campañas de educación a los usuarios con el ánimo de prevenir el fraude cibernético; sin embargo, es importante precisar que en calidad de PRST nuestro rol responde a un mero transportador de tráfico, por lo que escapa de nuestro control y dominio combatir un problema social que debe ser atendido por el Estado mismo.

2.3.1.2. Alternativa 2: Pedagogía y lista de campañas más denunciadas

RTA. Consideramos que esta alternativa es viable y de alta relevancia, siempre y cuando la misma sea liderada y articulada desde la CRC, quien de manera exitosa junto a la Fiscalía General de la Nación y a la Policía Nacional pueden identificar las estrategias que estén usando estos grupos delincuenciales para persuadir a las personas y lograr que éstas sean víctimas de fraude. Consideramos que es pertinente abordar la situación identificada de desconocimiento de los usuarios sobre el cuidado que deben tener al momento en que tienen interacción con aplicaciones o mensajes, de manera que ellos mismos sean cuidadores de la privacidad de la información, conozcan sobre modalidades de fraude, técnicas de ingeniería social usadas con los delincuentes y acciones de prevención y de mitigación que podrían usar para no facilitarle la obtención de datos personales con fines fraudulentos a personas inescrupulosas que lleven a la comisión de fraudes a través de mensajes de texto y llamadas de voz.

Consideramos muy valiosa la propuesta del regulador de contar con una lista de las campañas fraudulentas más denunciadas y que en el momento tengan un impacto importante. Con base en dicha información la CRC podría diseñar y desplegar estrategias pedagógicas y de divulgación, alineadas a la realidad del momento mediante campañas de comunicación a través de canales de difusión masiva como el canal institucional de la CRC. Con ello, se tendrá mayor oportunidad en la comunicación, pertinencia y efectividad, lo cual redundará en un mayor impacto, mitigando los riesgos de materialización de fraudes en los usuarios. Los agregadores y proveedores podrían tomar este insumo para adelantar campañas pedagógicas de acuerdo con los eventos fraudulentos que estén impactando a sus clientes.

Dicha herramienta de información o lista de las campañas fraudulentas más denunciadas, al ser administrada y liderada por la CRC, podría ser alimentada de manera articulada con otras entidades que también hacen parte del sistema

antifraude, tales como el Colcert, la Policía, Fiscalía, entidades bancarias, entre otros, con esto se robustecería la información acerca de los fraudes del momento y se podría tener un mayor impacto en las campañas de prevención que adelanten los PRST, PCA, e Integradores Tecnológicos.

Ahora bien, se pone a consideración de la CRC la posibilidad de articularse con organizaciones internacionales tales como GSMA para alimentar la lista de campañas fraudulentas de manera tal que si alguna modalidad de fraude aún no ha llegado a Colombia se logre actuar anticipadamente en la socialización y preparación de los usuarios ante el potencial riesgo.

2.3.1.3. Alternativa 3: Sistema de trazabilidad de PQR relacionadas con fraude a través de mensajes de texto o llamadas de voz

RTA. Encontramos en esta alternativa un mayor enfoque en la implementación de un sistema de trazabilidad de las temáticas objeto de PQR presentadas por los usuarios a la CRC, a los PRST, PCA e IT relacionadas con fraudes a través de mensajes de texto o llamadas telefónicas dejando en un segundo plano las iniciativas de educación y sensibilización del usuario a través de estrategias de divulgación, siendo esto último, más pertinente como alternativa de solución a la situación identificada que es el desconocimiento de los usuarios sobre privacidad de la información, modalidades de fraude, técnicas de ingeniería social, acciones de prevención y de mitigación, lo cual facilita la obtención de datos personales con fines fraudulentos por parte de personas inescrupulosas y la comisión de fraudes a través de mensajes de texto y llamadas de voz.

De otra parte, de acuerdo con lo presentado en esta alternativa, el fin último de este sistema de trazabilidad es fungir como herramienta de divulgación, prevención y mitigación de conductas fraudulentas, lo cual se consigue también a través de la alternativa 2 con la herramienta de información o lista de las campañas fraudulentas con una menor inversión frente al costo de implementar un sistema de trazabilidad de PQRs.

En conclusión, por lo anteriormente expuesto, consideramos que la alternativa 2 es la más favorable para atender la situación identificada en cuanto a la dimensión de la educación de la ciudadanía del presente proyecto regulatorio.

2.4. Temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

2.4.1. TEMÁTICA 1: Elementos para la mitigación del fraude por medio de la identificación de agentes reincidentes de acciones irregulares mediante el uso de códigos cortos

2.4.1.1. Alternativa 1: Statu quo

RTA. Conforme al problema identificado, es necesario establecer medidas regulatorias que permitan mitigar los fraudes que se cometen a través del servicio de mensajería de texto corto SMS, por tanto, se descarta esta alternativa.

2.4.1.2. Alternativa 2: Establecer obligaciones y consecuencias ante reincidencia

RTA. Esta alternativa podría generar valor en la medida en que incorpora consecuencias claras para los asignatarios de códigos cortos que se encuentren vinculados a actividades fraudulentas de manera reiterada. En particular, la definición y aplicación de la categoría de "asignatarios reincidentes" permite introducir un efecto disuasivo frente a estas conductas y fortalecer los incentivos para que los asignatarios de recursos de identificación implementen controles efectivos sobre el uso de la numeración asignada para el envío de SMS.

Sin embargo, su efectividad sería limitada si la medida se restringe únicamente a sancionar o imponer restricciones a la razón social que incurre en el uso indebido. En la práctica, ese enfoque puede ser fácilmente eludible mediante la creación de una nueva personería jurídica, con lo cual se neutraliza el propósito correctivo y preventivo de esta medida.

Para que el mecanismo tenga un impacto real, es necesario que la definición de reincidencia contemple también a los **representantes legales**, de forma que las consecuencias se activen cuando **se evidencie continuidad en la conducta a través de distintas personas jurídicas donde participan los mismos representantes legales** que han participado en empresas ya catalogadas como reincidentes. De lo contrario, bastaría con "migrar" a otra empresa o razón social para continuar con las prácticas ilegales.

2.4.2. TEMÁTICA 2: Condiciones para la cesión o transferencia de la asignación de recursos de identificación en códigos cortos

2.4.2.1. Alternativa 1: Statu quo

RTA. Conforme al problema identificado, es necesario establecer medidas regulatorias que permitan mitigar los fraudes que se cometen a través del servicio de mensajería de texto corto SMS, por tanto, se descarta esta alternativa.

2.4.2.2. Alternativa 2: Adopción de condiciones para la cesión o transferencia

RTA. Conforme a lo señalado en los comentarios generales, no se evidencia que la problemática esté asociada a la cesión o transferencia formal de la numeración. El riesgo se origina, más bien, cuando el asignatario de un código corto autoriza su uso

a un tercero sin que medie una cesión debidamente registrada por la CRC ni un cambio formal de titularidad.

Este tipo de "préstamo" o habilitación informal, sumado a la utilización de un mismo código para múltiples marcas o clientes, termina por diluir la trazabilidad y la atribución de responsabilidades frente al contenido, el origen del tráfico y la atención de reclamaciones. En la práctica, se generan zonas grises que dificultan la supervisión, la investigación de incidentes y la adopción de medidas correctivas oportunas.

Por ello, esta temática debería enfocarse en **prohibir expresamente dichas prácticas de préstamo o uso por terceros**. En ese sentido, se recomienda que la regulación delimite de forma explícita que el uso de códigos cortos y, si aplica, de numeración E.164 para SMS, debe realizarse exclusivamente por el asignatario, evitando esquemas informales que habiliten su uso.

2.4.3. TEMÁTICA 3: Suspensión del tráfico cursado a través de un código corto en el marco de una actuación administrativa

2.4.3.1. Alternativa 1: Statu quo

RTA. Conforme al problema identificado, es necesario establecer medidas regulatorias que permitan mitigar los fraudes que se cometen a través del servicio de mensajería de texto corto SMS, por tanto, se descarta esta alternativa.

2.4.3.2. Alternativa 2: Suspensión preventiva del tráfico durante una actuación administrativa

RTA. Esta medida es un mecanismo efectivo para controlar la circulación de mensajes a través de códigos cortos, en particular cuando se configuran causales previstas en el parágrafo 3 del Artículo 6.1.1.8. de la Resolución 5050 de 2016.

Además, la medida también deberá contemplar la posibilidad de suspender temporalmente el tráfico si se detecta un presunto **uso ineficiente** de un recurso de identificación asignado.

No obstante, para robustecer su eficacia frente al fraude, se considera pertinente incorporar de forma expresa una causal de recuperación del recurso de identificación asociada a actividades fraudulentas cuando existan presuntos indicios de uso indebido del recurso soportados en las quejas o reportes allegados a la Comisión.

En ese contexto, resulta clave que la medida tenga un alcance operativo claro: solicitamos que la suspensión temporal del tráfico asociado al código corto vinculado en la actuación administrativa sea obligatoria y exigible para todos los actores de la cadena, desde el PCA, su Integrador Tecnológico en caso de tenerlo, y demás intermediarios que participen en el encaminamiento del tráfico, hasta el PRST, de

manera que se eviten vacíos de implementación o interpretaciones fragmentadas que permitan que el tráfico continúe cursándose por algún eslabón.

Para que esta medida sea efectiva, es necesario que la CRC establezca un tiempo máximo de atención a la denuncia o reporte hecho ante un posible fraude que no supere las 24 horas para el acto de apertura de la actuación administrativa que permita realizar la suspensión del código corto y del tráfico que está cursando por dicho código, de forma preventiva hasta tanto se resuelva por completo la misma.

2.4.4. **TEMÁTICA 4: Condiciones asociadas a la vigencia y obligaciones de actualización de la asignación de recursos de identificación**

2.4.4.1. Alternativa 1: Statu quo

RTA. Conforme al problema identificado, es necesario establecer medidas regulatorias que permitan mitigar los fraudes que se cometen a través del servicio de mensajería de texto corto SMS, por tanto, se descarta esta alternativa.

2.4.4.2. Alternativa 2: Vigencias y actualización de la asignación del código corto

RTA. La medida de imponer la obligación de renovar periódicamente la asignación de los códigos cortos, una vez transcurrido un plazo determinado, contribuiría a fortalecer el control sobre la asignación y a promover el uso eficiente de estos recursos, evitando que permanezcan indefinidamente en cabeza de un asignatario sin una validación actualizada de su necesidad y operación real.

Adicionalmente, aunque no se propone expresamente, consideramos indispensable que la renovación esté acompañada de una **verificación del nivel de utilización efectiva del recurso**. En la práctica, se han identificado casos en los que una misma empresa mantiene múltiples códigos cortos asignados y, en algunos de ellos, cursa un volumen mínimo de mensajes únicamente para evitar la pérdida del recurso, sin que ello responda a un tráfico genuino derivado de una relación contractual vigente con una marca.

Esta situación genera dos efectos negativos: (i) distorsiona la disponibilidad del recurso al mantenerlo “ocupado” sin una demanda real, y (ii) dificulta la supervisión y trazabilidad, en tanto el uso marginal puede utilizarse como apariencia de operación para conservar la asignación.

Por ello, resulta pertinente que el proceso de renovación incluya criterios objetivos de utilización (por ejemplo, umbrales mínimos sostenidos, consistencia del tráfico, evidencia de la marca asociada y del modelo de operación), de manera que la asignación se mantenga únicamente cuando exista un uso real, verificable y acorde con la finalidad del código corto.

3. CONSULTA PÚBLICA

3.1. Preguntas generales

- Considerando que la atención coordinada del fraude mediante una estrategia nacional es una necesidad urgente para el país y los usuarios, y que este proyecto regulatorio será un paso de varios en la lucha contra un fenómeno tan dinámico, ¿qué tiempos de implementación estima necesarios para cada una de las medidas propuestas, teniendo en cuenta los desarrollos y capacidades actuales de los PRST y agregadores? ¿Qué retos técnicos, operativos o regulatorios podrían influir en esos plazos? ¿Qué esquemas de transición o fases intermedias propondría para garantizar una metodología ágil con victorias tempranas que permita atender oportunamente la creciente oleada de comunicaciones fraudulentas en el país?

  RTA. Los tiempos de implementación dependerán del tipo y alcance de las medidas que finalmente se adopten. En la temática de fraude a través de SMS, estimamos que la alternativa 4 de la sub temática 2 podría contribuir de forma relevante a la trazabilidad de las campañas comerciales que se emitan por este servicio, al establecer un único código corto o numeración E.164 por marca, además reduce la complejidad operativa frente a otras alternativas que exigirían mayores inversiones y coordinaciones.

  Por su parte, en la temática de fraude a través del servicio de voz, consideramos que, en términos generales, las medidas planteadas deben recaer en los Carrier internacionales, por ser quienes se encuentran en una posición técnica y operativa determinante para contener el ingreso de tráfico irregular. Por otra parte, la alternativa 2 de la subtemática 3 sería la única que, al establecer rangos de numeración específicos para la originación de llamadas comerciales y publicitarias, permitiría plantear controles para mecanismos de fraudes como el Robocall.

  Ahora bien, implementar todos los desarrollos propuestos en las alternativas regulatorias, implica necesariamente un horizonte de ejecución amplio y que razonablemente podría ser en mínimo 12 meses. En este punto, resulta importante destacar que, conforme a lo expuesto en los comentarios previos, varias de las alternativas en discusión no se traducen en una reducción directa e inmediata de los casos de fraude actualmente observados en el país.

  Por tanto, consideramos que una victoria temprana sería permitirle al operador realizar la suspensión temporal preventiva de cualquier código corto que esté cursando tráfico con indicios de fraude, acompañado de una debida denuncia que soporte la suspensión temporal hecha por el operador. Esto acompañado de las acciones que también podría implementar la CRC de manera inmediata frente a las condiciones en que realiza la entrega de los códigos cortos o recursos de numeración.

- ¿Qué ventajas, desventajas, retos y oportunidades identifica en la implementación por parte de la CRC de mecanismos de evaluación periódica de las medidas adoptadas para mitigar el fraude mediante servicios móviles tradicionales de voz y SMS? ¿Qué criterios, metodologías o frecuencias de evaluación considera más adecuados para asegurar la efectividad y actualización continua de estas medidas?

  RTA. Es importante que la CRC lidere y articule mesas de trabajo multisectoriales que permitan evaluar si estas medidas son realmente eficientes y, con base en ese análisis, pueda replantear la estrategia.

  Como lo hemos mencionado en los comentarios previos, las estrategias usadas por los ciberdelincuentes se adaptan de manera ágil al entorno cambiante que se presenta en la actualidad. Por ende, resulta necesario que la CRC establezca una metodología de evaluación y ajuste continuo que pueda implementarse con una velocidad similar, de modo que la respuesta regulatoria mantenga su efectividad.

  Por este motivo, las medidas que eventualmente se adopten deberían privilegiar un enfoque costo-eficiente, procurando que mantengan su efectividad en el tiempo y evitando escenarios de obsolescencia temprana ante la evolución de las estrategias delictivas. En esa línea, exigir a los PRST inversiones significativas en desarrollos sobre sus sistemas de información o en la red podría no resultar coherente ni proporcional, considerando los plazos de implementación y el retorno esperado en términos de mitigación del fraude.

- ¿Cuáles considera que son los principales aciertos y limitaciones de las alternativas propuestas para mitigar el contacto fraudulento a través de servicios tradicionales de voz y mensajes de texto? ¿Qué elementos adicionales o diferentes propondría para mejorar la eficacia de estas medidas?

  RTA. Uno de los principales aciertos relacionados con los contactos fraudulentos mediante mensajes de texto es la formulación de medidas específicas aplicables a los PCA. En esa misma línea, resulta necesario extender el análisis e incorporar medidas dirigidas también a los IT quienes deben tener las mismas cargas y responsabilidades frente a la prevención del fraude, que los PCA para quienes actúan como sus integradores, dado que a hoy esa responsabilidad entre ellos está diluida y es aprovechada para cometer los ilícitos, , así como prever consecuencias aplicables a los representantes legales cuando se evidencie un uso indebido de los recursos de numeración.

  Asimismo, esperamos que la CRC, con un enfoque equivalente, contemple medidas aplicables a los Carrier internacionales, considerando que, en la actualidad, estas empresas no cuentan con un régimen específico que regule de manera integral su actividad ni con obligaciones explícitas en materia de prevención y mitigación del fraude.

Ahora bien, frente a las limitaciones identificadas en algunas alternativas, medidas como el validador externo con asignación de Sender ID o STIR/SHAKEN implican desafíos relevantes, tanto presupuestales como técnicos, para su implementación. Adicionalmente, dada la capacidad de adaptación de los defraudadores, existe el riesgo de que su efectividad se reduzca en el corto plazo. Por lo anterior, consideramos que las medidas a priorizar deberían ser de implementación sencilla, rápidamente ajustables y costo-eficientes, de manera que permitan una respuesta oportuna y sostenible frente a la evolución de las modalidades de fraude.

- ¿Qué métricas, indicadores o criterios considera que deberían establecerse en la industria para evaluar de manera efectiva la reducción del fraude y el impacto de las alternativas regulatorias propuestas en este documento? ¿Qué variables cuantitativas o cualitativas serían más útiles para medir la evolución del fraude, la protección al usuario y la eficacia de las medidas implementadas, y cómo podrían ser recolectadas y/o reportadas de forma coordinada entre los diferentes actores del sector?

  RTA. En relación con las métricas, indicadores y criterios para evaluar la reducción del fraude y el impacto de las alternativas regulatorias, es importante precisar que, desde un enfoque metodológico, no resulta viable definir indicadores que permitan atribuir de manera directa la no materialización de un fraude específico a una medida aislada (p. ej., una campaña pedagógica particular) o a un actor específico. Esto se debe a que el fraude es un fenómeno multicausal, dinámico y adaptativo, y los insumos disponibles suelen provenir de reportes ex post (denuncias, PQR, quejas ante autoridades, reportes de entidades financieras), los cuales no permiten establecer con certeza una relación causal directa entre una intervención y la ausencia del evento.

3.2. Frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

- ¿Qué retos y beneficios identifica en la implementación de un proceso obligatorio de conocimiento del cliente (KYC) para agregadores de SMS? ¿Qué criterios mínimos considera indispensables para que este proceso sea efectivo y no excluyente?

  RTA. Esta medida debe articularse con las entidades de vigilancia y control para hacer efectivo su cumplimiento. De lo contrario, perdería la rigurosidad que debe emplear el agregador en su ejecución.

  Dentro de los criterios mínimos este proceso debe contener:

- ✓ Verificación de identidad. Validar la identificación del cliente, ya sea persona natural o jurídica. Cuando se trate de persona jurídica, deberá verificarse además la identidad y legitimación de sus representantes legales y/o apoderados.
- ✓ Perfilamiento y evaluación del riesgo. Evaluar antecedentes relacionados con el uso adecuado de recursos de numeración. Adicionalmente, resulta pertinente descartar estructuras sin actividad real ("empresas de papel"), corroborando elementos objetivos como la existencia de operación y un historial contable y tributario verificable.
- ✓ Monitoreo continuo. La validación no debe limitarse al inicio de la relación contractual. Se requiere un seguimiento periódico que permita confirmar que las condiciones verificadas al momento de la asignación y habilitación del código se mantienen vigentes, e identificar oportunamente cambios de comportamiento o señales de alerta.

- Teniendo en cuenta que los agregadores pueden actuar tanto en acuerdos directos (normalmente clientes nacionales como bancos, comercios, entidades de salud o aerolíneas, etc.), como en esquemas donde funcionan como parte de una cadena para terminar tráfico de otros agregadores (normalmente tráfico internacional). ¿Qué diferencias, riesgos u oportunidades identifica entre estos dos tipos de tráfico en cuanto al establecimiento de medidas regulatorias para la prevención del fraude? ¿Considera pertinente establecer medidas diferenciadas para cada caso? ¿Qué criterios o mecanismos recomendaría para gestionar de manera más efectiva el tráfico proveniente de cadenas internacionales, especialmente en lo relacionado con la trazabilidad, el monitoreo y la validación de los originadores de contenido?

  RTA. Para el tráfico internacional, también podría contemplarse la asignación de un código corto único por cliente, de modo que se facilite la identificación del origen del tráfico y se reduzcan zonas grises operativas. Es decir, en la resolución de asignación de un código corto la Comisión debería designar si el código fue asignado para uso de un cliente local o si es para el uso de un cliente internacional. Con esta caracterización se podría validar el establecimiento de reglas diferenciales que debe implementar el Asignatario del código corto como la validación mencionada de URLs para el tráfico local. En el tráfico internacional no es posible determinar cuál es el cliente que origina el mensaje, debido a que un mensaje puede tener varios saltos antes de llegar al proveedor en Colombia (Asignatario de código corto) para su distribución.

  Adicionalmente, cuando se detecten patrones o señales objetivas compatibles con campañas asociadas a fraude, debería preverse un marco que habilite, la suspensión temporal y preventiva de la numeración asociada con dicho tráfico, tanto por parte del agregador como del PRST, como medida de contención.

- ¿Considera pertinente la implementación de un proceso centralizado o distribuido para la validación de agregadores, marcas y campañas antes de cursar tráfico A2P?

  RTA. Consideramos que esta alternativa podría implicar costos elevados de implementación y sostenimiento, tanto por los desarrollos requeridos como por la operación y el monitoreo permanente que demanda. Adicionalmente, dado el carácter dinámico del fraude, existe un riesgo significativo de que los actores fraudulentos adapten rápidamente sus tácticas, reduciendo la efectividad de la medida en el corto plazo y obligando a incurrir en nuevas inversiones para mantener su utilidad.

  En ese contexto, estimamos más pertinente priorizar la asignación única por marca de códigos cortos o numeración E.164, en la medida en que simplifica el ecosistema de envío, facilita la trazabilidad y el control, y permite una implementación más directa y costo-eficiente, sin depender de soluciones complejas que pueden perder vigencia ante la evolución de las modalidades de fraude.

- ¿Cuáles serían, a su juicio, los principales desafíos técnicos, económicos, operativos y de gobernanza para un sistema centralizado de validación de remitentes y campañas? ¿Qué mecanismos de transparencia y auditoría considera necesarios?

  RTA. En los mismos términos de la respuesta anterior.

- ¿Qué ventajas y desafíos técnicos, económicos, operativos o de gobernanza identifica en un modelo distribuido de validación basado en DLT? ¿Qué elementos deberían definirse para asegurar la interoperabilidad y la confianza entre los distintos actores?

  RTA. En los mismos términos de la respuesta anterior.

- ¿Qué requerimientos funcionales considera que una solución tecnológica debe tener en cuenta para llevar a cabo de manera efectiva la validación de autenticidad de las URL en el evento que el mensaje corto de texto las contenga?

  RTA. Con la asignación de un único código corto o numeración E.164 por marca, se refuerza la trazabilidad del tráfico y la asociación unívoca entre el identificador utilizado para el envío y el titular responsable del contenido. Bajo este esquema, el agregador contaría con un parámetro objetivo para la debida diligencia de sus clientes, al exigir y mantener actualizada la(s) URL(s) oficial(es) asociadas a la marca con la que tiene su relación contractual para fines de comunicación A2P.

  En consecuencia, el agregador podría incorporar reglas de validación y gestión del tráfico (firewalls) en sus plataformas para detectar y bloquear mensajes que incluyan enlaces

distintos a los previamente registrados y autorizados por el titular de la marca, en tanto tales desviaciones constituyen un indicador de riesgo de suplantación o de campañas de smishing.

- ¿Qué impactos positivos y negativos prevé en la obligación de bloquear o marcar mensajes que no cuenten con identificadores validados? ¿Cómo se podría garantizar que no se afecte la entrega de mensajes legítimos?

  RTA. Conforme lo expuesto previamente, la alternativa más pertinente de implementación es la asignación de un único código corto o numeración E.164 por marca. Con este mecanismo no se materializaría el riesgo asociado a la no entrega de mensajes legítimos que no cuenten con identificadores validados.

- ¿Qué ventajas y riesgos observa en la clasificación obligatoria de los mensajes por tipo de contenido y la articulación con el consentimiento del usuario mediante el RNE? ¿Cómo podría mejorarse la protección de los derechos del usuario a decidir el tipo de contenido que desea recibir? ¿Considera pertinente una clasificación de tipos de contenido distinta a la propuesta?

  RTA. Sobre este punto, resulta pertinente recordar que recientemente se adelantó la implementación de la Resolución CRC 7356 de 2024 *"Por la cual se modifican disposiciones sobre el Registro de Números Excluidos contenidas el Capítulo 1 del Título II de la Resolución CRC número 5050 de 2016 y se dictan otras disposiciones."*, cambio motivado por las disposiciones contenidas en la Ley 2300 de 2023 conocida como la Ley *"Dejen de fregar"*. En consecuencia, introducir nuevas obligaciones regulatorias sobre consentimiento y categorización, podría desbordar el alcance del proyecto, generar solapamientos normativos y elevar la complejidad de articulación con una norma de jerarquía superior ya vigente e implementada, sin aportar una solución real y proporcional al núcleo del problema: la prevención y mitigación del fraude cibernético materializado mediante SMS.

- ¿Qué capacidades o características mínimas debería tener el sistema de monitoreo de tráfico por parte de los agregadores para detectar patrones anómalos o sospechosos? ¿Qué salvaguardas deberían definirse para evitar bloqueos injustificados?

  RTA. Se reitera lo señalado anteriormente respecto del bloqueo del tráfico que incorpore URLs distintas a las previamente reportadas y autorizadas por las marcas. En todo caso, resulta pertinente precisar que la materialización del fraude suele ocurrir una vez el usuario hace clic sobre el enlace incluido en el mensaje, siendo redirigido a una página que no corresponde al dominio oficial de la empresa que aparentemente origina la comunicación, con el propósito de inducir la entrega de información o credenciales.

  Bajo el control propuesto, el agregador podría detectar y prevenir el envío de mensajes que incluyan enlaces no registrados, reduciendo de forma significativa la probabilidad de

redireccionamientos a sitios apócrifos y, en consecuencia, mitigando la efectividad de campañas de suplantación y smishing.

- ¿Qué beneficios y limitaciones identifica en la alternativa de asignación de códigos alfanuméricos, códigos cortos o números E.164 exclusivos para cada marca? ¿Cómo podría impactar esto en la trazabilidad y la experiencia del usuario?

  RTA. Consideramos que esta alternativa es la más propicia para mitigar el fraude a través de mensajes de texto. Permite tener trazabilidad de inicio a fin del recorrido de los mensajes, así como, implementar controles que podrían tener un impacto positivo en la reducción de actividades fraudulentas.

  Beneficios:

  - ✓ Permite identificar claramente el agregador (asignatario del código) y la marca que está lanzando cada campaña.
  - ✓ El agregador podría implementar firewall para bloquear tráfico que no corresponda con la URL reportada por la marca a la que le pertenecería el código corto o numeración E.164.
  - ✓ Se puede implementar la obligación KYC a los agregadores.
  - ✓ No requiere establecer un acuerdo contractual con un tercero para la validación de los mensajes, evitando costos por este concepto.
  - ✓ Como se daría continuidad a la metodología de configuración de recursos de red actual, su implementación no sugiere complejidades técnicas.
  - ✓ Este tipo de numeración permite configurar texto para que el usuario pueda identificar su remitente.
  - ✓ Se podría habilitar a los PRST la suspensión temporal del código corto con tráfico sospechoso.

- ¿Qué efectividad considera que tendría la obligatoriedad de usar identificadores alfanuméricos únicos (Sender ID) en todos los mensajes de texto que reciban los usuarios, de cara a la confianza en el canal y la prevención del fraude?

  RTA. La identificación de la marca que envía el mensaje también se puede implementar con códigos cortos y numeración E.164. Esta identificación del remitente si bien puede generar confianza en el usuario, también se corre el riesgo de una falsa sensación de legitimidad. Por ello, se sugiere que esta medida este acompañada de la medida de asignación de un único código corto o numeración E.164 por marca para que pueda tener efectos positivos en la prevención del fraude.

- ¿Considera que una eventual limitación del uso de Sender ID alfanumérico a mensajes transaccionales reduciría costos de implementación, o por el contrario contribuiría a

desaprovechar la posibilidad de poder generar un mecanismo en el que los usuarios puedan identificar a todos los originadores de contenidos de manera clara?

RTA. En concordancia con la respuesta anterior, la implementación de un identificador del mensaje se puede realizar con los códigos cortos y la numeración E.164. Se sugiere no implementar desarrollos para la inclusión de los mecanismos de validación por el uso de un Sender ID.

- ¿Qué criterios considera relevantes para definir patrones atípicos en el tráfico SMS P2P? ¿Cómo se podría evitar afectar a usuarios legítimos?

  RTA. Los criterios atípicos a un uso habitual de una persona podrían tipificarse en estas dos modalidades:

  - ✓ Criterio por dispersión: se presenta cuando un mismo usuario origina una cantidad inusualmente alta de mensajes dirigidos a múltiples destinatarios distintos. Este patrón es característico de campañas masivas y, por ende, resulta indicativo de posibles prácticas abusivas o fraudulentas.

  - ✓ Criterio por ventana de tiempo: se configura cuando se registran volúmenes elevados de envíos concentrados en una ventana temporal corta (alta frecuencia), lo cual excede el comportamiento esperado de un usuario humano y es consistente con el uso de herramientas automatizadas.

- ¿Qué ventajas y desventajas identifica en la imposición de un límite máximo de SMS P2P por usuario? ¿Qué umbrales serían razonables?

  RTA. La regulación vigente ya habilita a los PRST para implementar herramientas tecnológicas orientadas a la prevención del fraude. En ese sentido, consideramos que la medida debería propender por reconocer de manera expresa en el marco regulatorio la facultad de bloquear numeración que evidencie patrones de uso compatibles con conductas asociadas a actividades fraudulentas.

- ¿Qué mecanismos de colaboración entre agregadores, operadores y autoridades considera que pueden implementarse para que la detección, prevención y judicialización de fraudes sea más efectiva?

  RTA. Dada la constante adaptación de los actores fraudulentos frente a las estrategias de prevención y control implementadas por los distintos grupos de interés, resulta especialmente pertinente priorizar la educación y sensibilización de la ciudadanía, de manera que los usuarios cuenten con criterios claros para identificar y evitar campañas de smishing.

Adicionalmente, se considera necesario que, a partir de las denuncias y reportes, incluidos aquellos presentados por los PRST, las autoridades competentes y, en el marco de sus funciones, la CRC, promuevan procedimientos más expeditos y coordinados que permitan adelantar las investigaciones y adoptar medidas oportunas en los menores tiempos posibles.

3.3. Frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

- En el servicio de llamadas de voz, los operadores pueden gestionar tanto tráfico originado por acuerdos directos con clientes nacionales (por ejemplo, bancos, comercios, entidades de salud, aerolíneas), como tráfico internacional que llega a través de cadenas de intermediarios, donde el originador de la llamada no siempre es certificado o plenamente identificable. ¿Qué diferencias, riesgos y oportunidades observa entre estos dos tipos de tráfico en relación con la prevención y mitigación del fraude? ¿Qué criterios, mecanismos o medidas considera relevantes para gestionar de manera diferenciada el tráfico directo y el tráfico en cadena, especialmente en lo relacionado con la trazabilidad, autenticación, control de llamadas sospechosas y judicialización?

  RTA. En el caso del tráfico originado a través de acuerdos directos existe un escenario de mayor control, que permite la identificación de alguna debilidad y su mitigación.

  Por otra parte, para el tráfico internacional que llega a través de cadenas de intermediarios; si el origen no cuenta con firmas certificadas, el control y la identificación de los eventos de fraude resulta complejo y altamente costoso.

  Es evidente para TIGO que la obligación de control no puede recargarse en el último eslabón de la cadena, principalmente en los PRST's, y además las acciones de control no pueden limitarse a la detección, o prevención, adicionalmente deben articularse mecanismos de sanción lo suficientemente justos y robustos que desincentiven la generación de eventos de fraude.

- ¿Qué mecanismos, herramientas o procedimientos tiene actualmente implementados su organización para detectar, prevenir y controlar el spoofing en llamadas de voz? ¿Qué nivel de efectividad han observado en estas medidas y qué retos técnicos y operativos han enfrentado en su aplicación?

  RTA. No hay implementadas herramientas antispoofing; se realizan controles offline para identificar posibles enmascaramientos del tráfico originado desde la red de TIGO; Se tienen líneas de comunicación para compartir los hallazgos y aplicar las medidas pertinentes en cada red.

Como se ha indicado es muy complejo identificar el enmascaramiento de las llamadas de origen internacional, dado que la cabecera de los registros de llamada puede ser modificada en el origen, y es técnicamente imposible detectar esta manipulación.

- ¿Qué efectos positivos y negativos prevé en la prohibición de llamadas internacionales con identidad de línea llamante CLI nacional? ¿Qué excepciones o consideraciones deberían contemplarse para no afectar la prestación de servicios legítimos?

  RTA. Efectos positivos:

  - ✓ El bloqueo de llamadas internacionales con identidad de linealínea llamante CLI nacional, podría implicar un desincentivo al enmascaramiento de llamadas.

  Efectos negativos:

  - ✓ No se prevé sanción u obligación de los carrier nacionales o internacionales, o del originador, o intermediarios de las llamadas. La responsabilidad se sobrecarga en el agente terminante de la comunicación.
  - ✓ En este sentido la CRC podría más bien implementar una medida prohibitiva de la práctica de enmascaramiento, estableciendo que, en caso de que esta práctica sea detectada se establezcan multas para quien la promueva o permita.
  - ✓ Es una alternativa que técnicamente demanda costos muy altos sólo para el proceso de detección, y no garantiza la eliminación de la generación de fraudes con origen internacional.
  - ✓ En los casos, en los que el enmascaramiento es aplicado como medida de seguridad para protección del llamante, así como, llamadas de emergencia o denuncias anónimas que requieren protección de los usuarios, tendrán que disponerse medidas excepcionales. Y en muchos casos este tipo de llamadas serán restringidas.
  - ✓ Los bloqueos de llamada podrían potencialmente causar perjuicios a los usuarios.

- ¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema que permita el enmascaramiento de la identidad de la línea llamante CLI en llamadas internacionales, siempre que estas sean etiquetadas en el dispositivo del usuario como “No verificada” o “Probable fraude”? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la prevención del fraude, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

  RTA. Ventajas:

  - El etiquetado de la llamada ofrece la posibilidad al usuario de identificar un riesgo potencial de acuerdo con sus necesidades y criterios; y en todo caso tener referencia

de aquellos eventos potencialmente peligrosos para que puedan iniciarse denuncias o investigaciones.

Retos:

- 1. Técnicos
  - Actualización del Core y coordinación con redes internacionales para implementar la infraestructura de autenticación STIR/SHAKEN.
  - Interoperabilidad global, para que el sistema funcione. Todos los países deben soportar los mecanismos de autenticación.
  - Evitar la restricción de las llamadas en las que se practica enmascaramiento es 'legal', bien por necesidad de protección al usuario, o por condiciones técnicas.

  2. Operativos
  - Coordinación entre operadores para acordar formatos y mecanismos de clasificación.
  - Necesidad de capacitación al usuario para evitar confusiones con el etiquetado y las reglas de bloqueo.
  - La CRC debe establecer una normatividad clara sobre el uso, exclusiones y sanciones relacionadas con los mecanismos de clasificación.

Posibles Impactos:

- Los costos de implementación son altos y no garantizan la eliminación del fraude en llamadas de voz de origen internacional.
- Las prácticas de suplantación también se ejecutan a través de numeración internacional, por lo que al restringir la práctica de enmascaramiento, se podría incrementar el fraude practicado con numeración internacional "no enmascarada", y aunque de esta forma los agentes de fraude no evitarían los cargos por roaming, si mantendrían la alternativa de fraude de origen internacional. Y en estas condiciones serían desperdiciados los recursos en los que se incurra para la aplicación de la medida.

- ¿Qué oportunidades y retos identifica en la adopción de protocolos de autenticación como STIR/SHAKEN/RCD? ¿Qué condiciones técnicas y regulatorias serían necesarias para su implementación efectiva? ¿Considera que, con la implementación de este protocolo de autenticación, no resulta necesaria la implementación de medidas de filtrado de tráfico o listas de no originación (DNO)?

  RTA. Antes de listar las oportunidades y retos que supone la implementación de los protocolos de autenticación, enfatizamos el hecho que la autenticación de las llamadas de

origen internacional depende de la gestión y certificación de los originadores, lo cual no es gestionable por los PRSTs locales en Colombia principalmente porque los protocolos STIR/SHAKEN no corresponden a estándares de implementación global y adicionalmente al no establecerse en todos los acuerdos internacionales con conexiones directas pueden involucrarse intermediarios que hagan tránsito de las llamadas que no aplican estos protocolos, y rompen la cadena de autenticación.

De acuerdo con lo anterior las obligaciones que se establezcan deben asignarse también a los Carrier internacionales y a las entidades originadoras de tráfico y no puede recargarse a los PRSTs, pues no es un proceso que dependa completamente de su gestión propia.

Oportunidades

- Con el uso de estos mecanismos, los usuarios contarían con una herramienta que les puede ayudar a distinguir mejor las llamadas legítimas de las sospechosas.

Retos:

- El protocolo STIR/SHAKEN no es un protocolo que por ahora tenga utilización global, esto implica que un gran porcentaje de llamadas no puede ser verificado.
- Los PRST's en Colombia no tienen gestión directa sobre la certificación de las llamadas de origen internacional, en razón a la falta de globalidad del protocolo. Y no es conveniente para el servicio prestado a los usuarios restringir los acuerdos internacionales a la entrega de llamadas con el protocolo STIR/SHAKEN.
- El entorno tecnológico está fragmentado, y STIR/SHAKEN fue diseñado para redes SIP/IP (VoIP, VoLTE) y no es compatible con redes tradicionales (PSTN/SS7) sin el uso de adaptadores.
- Para que el protocolo sea efectivo en las llamadas que cursan a través de una cadena de intermediarios, cada participante de la cadena debe efectuar la certificación de la llamada y no se puede garantizar este proceso completo.

Condiciones técnicas necesarias para la implementación efectiva:

- Las redes deben operar en IP para que puedan soportar el protocolo STIR/SHAKEN
- Es necesario implementar la infraestructura de autenticación, lo que implica crear un ecosistema de certificado digitales; en el que tienen que integrarse nuevos participantes como por ejemplo las entidades encargadas de gestionar los certificados digitales.
- Todos los operadores que originan, transitan y terminan llamadas deben cooperar y acordar políticas de firma, verificación y tratamiento de la información, definiendo adecuadamente los niveles de servicio.

- Se deben actualizar los dispositivos de software, pues estos deben ser capaces de interpretar y mostrar los resultados de la autenticación.

Finalmente, sobre la última consulta, las listas de no originación DNO son un mecanismo ineficiente en el control de fraude que no debería ser implementado.

- ¿Qué parámetros y tecnologías considera más adecuados para estandarizar los modelos de monitoreo y filtrado de tráfico de voz? ¿Cómo garantizar que no se generen falsos positivos (que terminen afectando el tráfico legítimo), así como la protección de la privacidad de las comunicaciones y la proporcionalidad de las medidas?

  RTA. Los parámetros definidos para este tipo de control podrían ser:

  Volumen de llamadas: Llamadas por segundo/minuto/hora por CLI o rango, Duración promedio: Llamadas extremadamente cortas o repetitivas, Tasa de establecimiento fallido: Alto número de intentos no contestados o rechazados, Patrones temporales: Picos en horarios atípicos, Relación origen–destino: Un CLI llamando a miles de números distintos Cambios abruptos de comportamiento: Variaciones repentinas respecto a su histórico.

  Estos parámetros definen un marco para desarrollar no en tiempo real una analítica basada en el comportamiento.

  La única forma de prevenir los falsos positivos es NO aplicar las medidas antifraude en tiempo real, sino luego del análisis y verificación comprobada de la información (**Las medidas que afectan el tráfico** deben ser: Posteriores, Confirmadas, Reversibles.) para garantizar el debido proceso y la continuidad del servicio. Esto también permite proteger la privacidad de las comunicaciones, pues no se interfiere la comunicación del usuario en el momento de su establecimiento, sino posterior a él.

- ¿Qué actores deberían participar en una plataforma nacional de intercambio de alertas sobre fraudes en llamadas? ¿Qué mecanismos de gobernanza y protección de datos serían necesarios? ¿Cuáles considera que serían los retos técnicos y económicos de construir y operar la plataforma de alertas bajo un modelo centralizado vs un modelo distribuido? ¿Qué mecanismos considera deben ser adoptados y estandarizados para validar la veracidad de una alerta antes de su distribución mediante la plataforma de intercambio?

  RTA. Una plataforma nacional de intercambio de alertas sobre fraudes en llamadas debe considerar la participación de:

  - ✓ Entidades Públicas: CRC, MinTIC, SIC, Autoridades de seguridad.
  - ✓ Todos los proveedores del ecosistema de VOZ: Carriers, PRSTs, Agregadores y proveedores de Call Center, Fabricantes de software y dispositivos.

- ✓ Gestores de información de Fraude: Entidades que pueden gestionar listas de numeración restringida, claves de autenticación, certificados de registro.
- ✓ Usuarios: Personas y entidades.

Respecto de la gobernanza es importante que las entidades públicas asuman las siguientes responsabilidades clave:

1. Definir las obligaciones, responsabilidades y sanciones respecto de la lucha antifraude para todos los actores del sistema digital, y no enfocar las responsabilidades sólo en algunos participantes.
2. Participar activa y efectivamente en la investigación e identificación de los participantes o responsables de la promoción o ejecución de actividades fraudulentas
3. La articulación de un sistema sancionatorio justo, que no enfoque las sanciones a las limitaciones en la detección, sino más bien orientado a la penalización de quienes participan, promocionan o ejecutan premeditadamente acciones fraudulentas.

El sistema sancionatorio para los asignatarios de recursos de identificación y Carrier internacional es clave en la lucha antifraude, pues es una herramienta de desincentivo real del fraude; enfocar los esfuerzos sólo en la detección del fraude, sin que las autoridades investiguen e identifiquen los responsables es una estrategia costosa que sólo promueve el cambio de modalidades de los agentes delictivos.

- ¿Qué ventajas y desafíos observa en la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias? ¿Considera que esta medida podría ser efectiva para facilitar la identificación y denuncia de fraudes por parte de los usuarios?

  RTA. Ventajas:

  - Los usuarios podrían reconocer las llamadas que tienen un propósito comercial o publicitario.
  - Se reduce para el usuario la confusión para aceptar llamadas personales, institucionales y comerciales.
  - Se otorga la facilidad al usuario de tomar una decisión informada: Aceptar, declinar, o bloquear llamadas.
  - Facilita para el usuario el reconocimiento y la interposición de denuncias por fraude.
  - A nivel general esta medida limita el uso de la numeración móvil o fija normal para fines comerciales y dificulta que los actores fraudulentos se oculten en numeración asignada para usos personales o locales.
  - A nivel institucional la medida permitiría el reconocimiento a través de los rangos de proveedores y campañas específicas.

Desafíos:

- La definición y asignación correcta de los rangos de numeración.
- La definición precisa del alcance respecto al uso de la numeración comercial.
- La adaptación en las redes de la señalización, el enrutamiento y la facturación de las llamadas.
- Los controles requeridos para que sólo actores pertinentes y autorizados accedan a esos rangos.
- El establecimiento de un método sancionatorio efectivo para aquellos actores que hagan uso indebido de la numeración.
- El establecimiento de obligaciones de identificación y registro para quienes utilicen esos rangos.
- La migración de las entidades de sus servicios actuales a los nuevos rangos de numeración.

- ¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la transparencia en las comunicaciones, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

  RTA. Ventajas:

  - Las etiquetas brindan al usuario una identificación inmediata y práctica del llamante, que no implica para él un reconocimiento de la numeración.
  - Obliga al originador a declarar el propósito de la llamada.
  - Facilita el proceso de denuncia.

  Retos:

  - Requiere mecanismos confiables para etiquetar la señalización IP; para redes tradicionales (PSTN/SS7) esta opción no es viable sin adaptadores.
  - No hay un entorno homogéneo para la presentación y gestión de las etiquetas.
  - Los agentes de fraude podrían omitir el uso de las etiquetas, o utilizar etiquetas falsas para engañar al usuario.
  - Requiere implementar procesos de registro y auditoría de las etiquetas.
  - La saturación en el uso de las etiquetas puede ocasionar la omisión de su revisión por parte de los usuarios.
  - La definición precisa del uso de las etiquetas y las sanciones que conlleva su mala utilización.

- El etiquetado no reemplaza la autenticación STIR/SHAKEN, ni sustituye el filtrado o listas DNO, aunque podría complementar este tipo de medidas.

- ¿Qué beneficios y riesgos identifica en la creación de un registro nacional único de números DNO? ¿Qué criterios deberían regir su actualización y acceso?

  RTA. Beneficios:

  - Consideramos que esta opción es ineficiente para la prevención del fraude, por cuanto progresivamente limita el uso de la numeración (que es un recurso escaso), e incrementa el ritmo de sustitución de la numeración utilizada para efectuar fraudes.

  Riesgos:

  - No facilita el uso eficiente de los recursos de numeración.
  - Acelera el ritmo de sustitución de la numeración que es utilizada para realizar fraude.

- ¿Qué ventajas, retos y posibles impactos identifica en la adopción de un esquema en el que cada PRST mantenga su propia lista de no originación (DNO), bajo un estándar mínimo obligatorio definido por la CRC? ¿De qué manera considera que esta medida podría contribuir a la protección contra el fraude y la suplantación en llamadas de voz, y qué desafíos técnicos, operativos o de coordinación deberían ser tenidos en cuenta para asegurar su efectividad y coherencia en Colombia?

  RTA. Ventajas:

  - Los operadores pueden reaccionar de manera más rápida y adaptable al fraude, respecto de un sistema centralizado
  - Los PRST pueden adaptar sus listas DNO a su topología de red, su perfil de tráfico, y su base de clientes.

  Retos:

  - Definir un estándar mínimo que mitigue las diferencias en los criterios de inclusión y los niveles de protección en las redes.
  - La complejidad técnica que imposibilita integrar en tiempo real la consulta de las listas con sistemas de enrutamiento y rastreo.
  - La coordinación entre redes para asegurar la interoperabilidad entre listas y el intercambio de información relevante. DE tal manera que se presenten casos en que se bloquea un número en una red y no en otra
  - Evitar el bloqueo de llamadas legítimas.

3.4. Frente a las temáticas enfocadas en la educación de la ciudadanía

- ¿Qué acciones voluntarias (no regulatorias) adelanta actualmente su organización o conoce usted en el mercado para informar a los usuarios sobre riesgos de fraude? ¿Son efectivas? ¿Tienen métricas de impacto?

  RTA. Como se describió en la alternativa 1, Status quo, actualmente se realizan campañas de educación a los usuarios con el ánimo de prevenir el fraude cibernético.

  En cuanto a las métricas de impacto, desde un punto de vista metodológico no es posible implementar indicadores que permitan atribuir de manera directa la prevención de un fraude específico a una campaña determinada. Ello obedece a que las campañas de divulgación tienen un carácter masivo y preventivo, y no existe un mecanismo que permita identificar con certeza qué usuarios, habiendo estado expuestos a una campaña concreta, evitaron ser víctimas de una modalidad particular de fraude como resultado de dicha intervención. Adicionalmente, la información disponible sobre eventos de fraude suele provenir de denuncias o reportes posteriores, los cuales no permiten establecer una relación causal directa entre la acción pedagógica y la no ocurrencia del fraude. En este contexto, cualquier intento de medición directa del impacto podría conducir a conclusiones imprecisas o sesgadas.

- ¿Qué cargas técnicas y económicas representaría para los PRST, los IT y los PCA implementar obligaciones de divulgación pedagógica frente al fraude cibernético?

  RTA. La implementación de acciones de divulgación pedagógica frente al fraude cibernético no constituye una actividad marginal, sino una función estructural que requiere una **capacidad instalada permanente**, con costos reales para los diferentes agentes.

  Para implementar obligaciones de divulgación pedagógica frente al fraude cibernético se requiere una capacidad instalada consistente en: un proceso definido para la realización de las campañas de divulgación, un equipo de comunicadores y diseñadores encargados del diseño de la comunicación y una infraestructura tecnológica para comunicar, es decir las plataformas según el caso, sms, whatsapp, Push, etc.

  Dada la dinámica del fraude, consideramos pertinente que los diferentes agentes interesados cuenten con autonomía en el diseño de sus estrategias y campañas, apoyados en las diferentes herramientas existentes y que por supuesto hagan parte de su capacidad.

  De ser seleccionada la alternativa 2 *"Pedagogía y lista de campañas más denunciadas"* se contará con un insumo estratégico de gran importancia, que es la lista de campañas más denunciadas; este insumo facilitará la focalización de las acciones pedagógicas y

preventivas, en la medida en que los agentes del sector podrán orientar sus esfuerzos de divulgación hacia los riesgos reales y vigentes; asimismo, permitirá optimizar el uso de recursos técnicos y económicos, al priorizar contenidos y mensajes asociados a las tipologías de fraude que presentan mayor incidencia, en lugar de imponer obligaciones uniformes y permanentes.

En este sentido, la alternativa 2 se perfila como una medida costo-eficiente y flexible, que contribuye a la prevención y mitigación del fraude, al tiempo que respeta la diversidad de modelos operativos y capacidades de los agentes regulados.

- Frente a la alternativa de divulgación pedagógica por parte de PRST, PCA e IT ¿Qué tipo de contenidos deberían ser obligatorios? (ejemplos reales, guías de prevención, alertas recientes, recomendaciones prácticas, etc.)

  RTA. Consideramos que, más allá de la definición de contenidos rígidos u obligatorios, resulta más efectivo contar con un conjunto flexible de herramientas y recursos pedagógicos tales como: guías de prevención, ejemplos basados en casos reales debidamente anonimizados, alertas sobre modalidades emergentes, recomendaciones prácticas y mensajes de autocuidado digital que puedan ser utilizados de manera dinámica según la situación y el riesgo identificado en cada momento. Este enfoque permite adaptar la divulgación pedagógica a la evolución constante de las modalidades de fraude, evitando esquemas estáticos que rápidamente pueden quedar desactualizados.

  Por ejemplo, ante la identificación de una nueva modalidad de fraude, y con el fin de socializar oportunamente esta información y atender la necesidad de conocimiento de los usuarios, el equipo de profesionales encargado del proceso podrá seleccionar y combinar los recursos pedagógicos que resulten más efectivos en función del público objetivo, el nivel de urgencia y el canal de divulgación. De esta manera, se promueve una solución basada en el análisis del problema concreto, apoyada en distintos recursos pedagógicos, que fortalece la capacidad de prevención de los usuarios y maximiza el impacto de las acciones de divulgación, sin limitar la innovación ni la adaptación a contextos cambiantes.

- Frente a la alternativa de divulgación pedagógica por parte de PRST, PCA e IT ¿Cuál considera es el canal más apropiado para esta divulgación? (ejemplo: SMS masivos, mensajes en facturas, Landing pages, Push notifications en apps, etc.)

  RTA. No existe un único canal óptimo, sino que la efectividad de la divulgación depende del uso complementario de los canales disponibles, en función del tipo de mensaje, el nivel de urgencia y el perfil del usuario objetivo. Una alternativa es utilizar de manera articulada los distintos canales disponibles, definiendo en cada estrategia cuáles son los más apropiados según el contexto y el riesgo que se busca mitigar. Canales directos como los SMS masivos, los mensajes en facturas físicas o digitales y las notificaciones push en aplicaciones móviles

resultan especialmente útiles para alertas inmediatas y de alto impacto, mientras que herramientas como landing pages permiten ampliar la información, profundizar en explicaciones pedagógicas y centralizar recomendaciones actualizadas. Adicionalmente, las redes sociales forman parte activa de la estrategia de divulgación, al permitir un mayor alcance y segmentación. Este enfoque multicanal permite reforzar los mensajes, adaptarlos a los hábitos de consumo de información de los usuarios y maximizar la efectividad de las acciones pedagógicas, sin depender de un único medio de comunicación.

- Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, ¿Qué nivel de detalle debería tener la información publicada para ser útil sin generar nuevas vulnerabilidades? (ejemplo: números reportados, patrones o modus operandi, ejemplos de mensajes fraudulentos, etc.)

  RTA. Frente a la implementación de un Portal con las campañas más denunciadas, el nivel de detalle de la información publicada debe ser suficiente para alertar y educar a los usuarios, así como para servir de insumo a los agentes del sector, sin exponer elementos que puedan ser reutilizados o perfeccionados por actores fraudulentos. En ese sentido, el portal debería incluir, de manera agregada y dinámica, los códigos cortos, numeraciones o rangos desde los cuales se están originando mensajes o llamadas fraudulentas, así como una descripción general del modus operandi de cada campaña, explicando cómo funciona la estafa sin detallar procedimientos técnicos sensibles. Adicionalmente, resulta útil incorporar ejemplos ilustrativos de los mensajes o llamadas fraudulentas, debidamente anonimizados y despersonalizados, junto con recomendaciones claras y accionables para que los usuarios identifiquen señales de alerta y eviten caer en esa modalidad específica de fraude. De esta forma, el portal cumple una función pedagógica y preventiva, fortaleciendo la capacidad de respuesta de los usuarios y del sector, sin generar nuevos riesgos ni facilitar la replicación de las campañas fraudulentas.

- Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, ¿Qué beneficios concretos considera que traería este portal para los usuarios y agentes del sector?

  RTA. Los beneficios para los agentes del sector incluidos los PRST, los PCA y los IT de contar con un portal que consolide las campañas de fraude más denunciadas radica en la disponibilidad de un insumo estratégico y actualizado para el diseño de acciones de divulgación y prevención. Este repositorio permitiría identificar de manera oportuna las modalidades de fraude que se encuentran en mayor circulación en un momento determinado, facilitando la construcción de mensajes pedagógicos pertinentes y focalizados que alerten efectivamente a los usuarios. De esta forma, los esfuerzos de comunicación y sensibilización de los distintos actores del ecosistema se encontrarían alineados, y sustentados en una fuente de información común, real, confiable y basada en denuncias

efectivas, lo que incrementa la coherencia, la eficiencia y el impacto de las campañas de prevención del fraude.

Por su parte, los beneficios para los usuarios de contar con un portal que consolide las campañas de fraude más denunciadas radican en el acceso oportuno a información clara, confiable y actualizada sobre las modalidades de estafa que se encuentran circulando en un momento determinado. Este portal permitiría a los usuarios reconocer patrones recurrentes, identificar señales de alerta en mensajes, llamadas o comunicaciones digitales y adoptar medidas preventivas antes de verse afectados.

Al basarse en reportes y denuncias reales, la información publicada se convierte en una fuente fidedigna que reduce la desinformación, fortalece la cultura de autoprotección y genera mayor confianza en las acciones de prevención del fraude. De esta manera, los esfuerzos de sensibilización y alerta hacia los usuarios se encuentran alineados con una misma fuente oficial, lo que incrementa la efectividad de los mensajes y contribuye a disminuir la probabilidad de que los usuarios sean víctimas de modalidades de fraude "de moda" o emergentes.

- Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, en caso de que aplique, ¿qué cargas técnicas y económicas representaría para su organización implementar estas obligaciones?

  RTA. Teniendo en cuenta que el proyecto regulatorio en lo que concierne a la temática "Acciones educativas que aumenten el conocimiento de los usuarios", en la alternativa 2, propone que la CRC creará y administrará un portal que incluya la lista con las campañas más denunciadas ante esta entidad los agentes del sector incluidos los PRST, los PCA y los IT tendrían como única responsabilidad la consulta de dicho portal, sin contar con injerencia alguna en su diseño, operación o implementación técnica.

- ¿Considera viable técnica y operativamente crear un sistema de trazabilidad centralizado de PQR relacionadas con fraude por mensajes de texto o llamadas? Justifique su respuesta.

  RTA. El sistema de trazabilidad de PQR relacionadas con fraude a través de mensajes de texto o llamadas de voz que propone el proyecto regulatorio, según lo descrito en la alternativa 3, pretende publicar información correspondiente únicamente a las temáticas relacionadas con el intento o comisión de fraudes a través de llamadas de voz y mensajes de texto con el fin último que los agentes interesados conozcan las modalidades empleadas por los delincuentes, constituyendo este sistema en una herramienta de divulgación, prevención y mitigación de este tipo de conductas.

  No obstante, el fin último de esta herramienta puede alcanzarse mediante mecanismos alternativos menos complejos y más costo-eficientes, como la implementación del portal

que consolide las campañas más denunciadas, contemplado en la alternativa 2. Este último permitiría centralizar y difundir información relevante y agregada sobre las modalidades de fraude vigentes, sin requerir la construcción, integración y mantenimiento de un sistema de trazabilidad de PQR que implicaría altos costos técnicos, operativos y económicos, así como desafíos asociados a la interoperabilidad entre sistemas de los distintos agentes, la estandarización de datos y la protección de información sensible de los usuarios.

En este contexto, la alternativa de un portal informativo con campañas más denunciadas resulta más viable técnica y operativamente, al cumplir el mismo propósito de divulgación y prevención, reduciendo cargas regulatorias y evitando la duplicación de esfuerzos, sin introducir complejidades adicionales que podrían afectar la eficiencia del ecosistema.

- ¿Qué variables o campos considera debería contener este sistema de trazabilidad para permitir análisis útiles?

  RTA. En línea con la anterior respuesta, no consideramos variables o campos para ese sistema.

- ¿Qué riesgos de seguridad o privacidad considera deben ser tenidos en cuenta al centralizar la información de PQR relacionadas con fraude?

  RTA. La centralización de la información de PQR relacionadas con fraude conlleva diversos riesgos de seguridad y privacidad que deben ser cuidadosamente evaluados y mitigados. En primer lugar, este tipo de información puede contener datos personales y sensibles de los usuarios, tales como números telefónicos, registros de contacto, descripciones de los hechos y, en algunos casos, información financiera o de comportamiento, lo que incrementa el riesgo de accesos no autorizados, filtraciones de datos o usos indebidos de la información.

  Adicionalmente, se presentan riesgos asociados a la integridad y calidad de la información, en la medida en que errores en la carga, clasificación o actualización de las PQR podrían generar alertas imprecisas, afectar la confianza en el sistema o derivar en decisiones operativas incorrectas por parte de los agentes del sector. Finalmente, la interoperabilidad entre los sistemas de los distintos agentes y el sistema centralizado plantea desafíos en materia de estándares de seguridad, trazabilidad de accesos y responsabilidades frente a eventuales incidentes de seguridad de la información.

- ¿Qué componentes debería incluir estrategia educativa conjunta entre la CRC, los agentes regulados y otras entidades competentes? (por ejemplo: campañas nacionales, identificación de patrones emergentes, material didáctico para usuarios, indicadores de éxito, etc.)

RTA. Una estrategia educativa conjunta entre la CRC, los agentes regulados y otras entidades competentes debería estructurarse a partir de un esquema de coordinación centralizado, liderado por la CRC, que permita maximizar el impacto de las acciones pedagógicas y, al mismo tiempo, minimizar las cargas técnicas, operativas y económicas para los PRST toda vez que nuestro rol responde a un mero transportador de tráfico. En este sentido, la estrategia debería incluir, como componente principal, campañas nacionales de alcance general diseñadas y coordinadas por la CRC, con el apoyo de otras autoridades competentes, tales como la Policía, la Fiscalía entre otras, a partir de información agregada y validada sobre las modalidades de fraude más recurrentes.

Adicionalmente, la identificación y análisis de patrones emergentes de fraude debería realizarse de manera centralizada, utilizando insumos provenientes de denuncias, reportes institucionales y otras fuentes oficiales. Como resultado de este ejercicio, la CRC podría poner a disposición de los agentes regulados un repositorio común de material didáctico estandarizado tales como guías, alertas, mensajes tipo y piezas comunicacionales que pueda ser reutilizado y adaptado por los diferentes agentes (PRST, PCA, IT) a través de sus canales habituales de comunicación, sin requerir desarrollos adicionales significativos.

Finalmente, los indicadores de éxito de la estrategia deberían enfocarse en métricas agregadas de alcance, difusión y actualización de contenidos, definidas y monitoreadas de manera centralizada. Este enfoque permite una estrategia educativa coherente, costo-eficiente y basada en la colaboración interinstitucional, en la que los PRST actúan principalmente como canales de difusión, reduciendo cargas regulatorias y promoviendo una protección efectiva de los usuarios.

3.5. Frente a las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación

A partir de las temáticas identificadas en el presente documento, y en el marco del proceso de revisión del Régimen de Administración de Recursos de Identificación bajo un enfoque de simplificación regulatoria, resulta pertinente evaluar la pertinencia de ajustes adicionales. En este sentido, se plantean las siguientes preguntas orientadoras:

Reincidencia en el uso indebido de recursos de identificación para el envío de SMS.

- Desde la perspectiva de prevención de contactos fraudulentos a los usuarios, ¿qué elementos del régimen de administración de recursos de identificación para el envío de SMS deberían ser revisados o simplificados para prevenir su uso indebido? Explique detalladamente las razones que justifican dicha revisión.

  RTA. Conforme a lo mencionado en los comentarios relacionados con el envío de SMS, entre otras cosas, se debe:

- ✓ Asignación de un único código corto o numeración E.164 por marca.
- ✓ Prohibir expresamente prácticas de préstamo o uso por terceros de los códigos cortos y si aplica de la numeración E.164 para SMS ya que estos son de uso exclusivo del asignatario. Dado que la trazabilidad es el eje del proyecto, cualquier figura que separe asignación formal de uso efectivo resulta incompatible con el objetivo regulatorio.
- ✓ Establecer obligaciones de acceso y consecuencias por el uso indebido de los recursos de identificación tanto para PCA como para IT en su calidad de Asignatarios de estos recursos.
- ✓ Establecer obligaciones especificas relacionadas con controles de fraude para los asignatarios de los códigos cortos, como la implementación de firewalls, medidas de KYC y bloqueo de tráfico presuntamente fraudulento.
- ✓ Establecer consecuencias claras frente a la reincidencia y deben ser aplicadas no solo a la persona jurídica sino también a los representantes legales que hagan uso indebido de los recursos de identificación.

- En relación con la detección de uso indebido del recurso de identificación, ¿qué criterios adicionales a los expuestos considera necesarios para determinar que un asignatario está haciendo un uso indebido del recurso de identificación? Describa y fundamente cada criterio propuesto.

  RTA. Criterios para determinar que un asignatario está haciendo uso indebido del recurso de identificación:

  - ✓ Desviación del propósito autorizado del código corto. Se considera que existe un uso indebido cuando el código corto es utilizado para fines distintos a aquellos declarados y aprobados en el proceso de asignación a través del acto administrativo correspondiente, tales como emplearlo para campañas comerciales, promocionales o de captación de información cuando fue autorizado exclusivamente para notificaciones transaccionales, informativas o de seguridad. Este criterio se fundamenta en la necesidad de preservar la trazabilidad, confianza y finalidad específica del recurso de numeración.
  - ✓ Asociación recurrente del código corto con PQR o denuncias por fraude. Cuando un código corto registra un volumen significativo y recurrente de PQR relacionadas con intentos o comisión de fraude, suplantación o engaño, puede considerarse que existe un uso indebido o, al menos, una falla en los controles del asignatario.
  - ✓ Que el código corto o la numeración E.164 para SMS que está utilizando el agente en cuestión en sus comunicaciones no le fueron asignados por la CRC si no que están bajo la responsabilidad de otro agente.
  - ✓ Falta de mecanismos de control, trazabilidad y atención de incidentes por parte del asignatario. La ausencia de controles internos mínimos para supervisar el uso del

código corto, gestionar incidentes de seguridad o atender oportunamente reportes de abuso puede constituir un uso indebido por omisión. Este criterio se fundamenta en la responsabilidad del asignatario de administrar adecuadamente el recurso asignado

- ✓ Reasignación, subarriendo o cesión no autorizada del código corto. Se considera uso indebido cuando el asignatario permite que terceros utilicen el código corto sin la autorización correspondiente o sin cumplir las condiciones regulatorias aplicables. Este criterio se fundamenta en la necesidad de mantener claridad sobre la titularidad y responsabilidad en el uso del recurso.
- ✓ En la práctica, se han identificado casos en los que una misma empresa mantiene múltiples códigos cortos asignados y, en algunos de ellos, cursa un volumen mínimo de mensajes únicamente para evitar la pérdida del recurso, sin que ello responda a un tráfico genuino derivado de una relación contractual vigente con una marca, por lo que esta práctica se considera un uso indebido del recurso.

- Respecto a las medidas correctivas, ¿qué restricciones adicionales a las previstas actualmente, considera pertinente aplicar a los asignatarios que incurren en uso indebido del recurso de identificación para SMS? Explique en detalle las razones de cada restricción sugerida.

  RTA. De habilitarse el código corto único por marca, se le facilitaría al PRST la identificación de la marca y agregador involucrados en eventos de presuntas campañas fraudulentas, con lo cual debería facultarse a los PRST para realizar una suspensión temporal del tráfico generado a través del recurso de identificación utilizado en dicha campaña, mientras se verifica con el agregador los motivos y contenidos de la presunta campaña fraudulenta.

  Además, cuando se determine que un agregador es reincidente en conductas fraudulentas, bajo los criterios que defina la CRC, debería vetarse la personería jurídica, así como sus representantes legales para la asignación de nuevos recursos de identificación.

- Con base en su experiencia, ¿cuáles de las medidas actualmente contempladas en la regulación sobre la recuperación de códigos cortos considera efectivas y cuáles no? Por favor sustente su respuesta indicando, cuando sea posible, ejemplos o casos que respalden su argumento.

  RTA. Respecto al criterio de uso eficiente: *"Los códigos cortos implementados no deberán reportar ausencia de tráfico en periodos consecutivos iguales o superiores a doce (12) meses",* hemos evidenciado en la práctica, casos en los que una misma empresa mantiene múltiples códigos cortos asignados y, en algunos de ellos, cursa un volumen mínimo de mensajes únicamente para evitar la pérdida del recurso, sin que ello responda a un tráfico genuino derivado de una relación contractual vigente con una marca, por lo que se debe replantear este criterio.

De habilitarse el código corto único por marca, el agregador deberá garantizar un tráfico mínimo de dicha marca durante la vigencia específica declarada en la asignación del código corto.

Respecto al criterio de uso eficiente: "Los códigos cortos implementados no deberán reportar tráfico para un único usuario por un periodo superior a tres (3) meses"; de habilitarse el código corto único por marca, este criterio debe desaparecer.

Ahora bien, respecto a las causales de recuperación de códigos cortos, la siguiente medida consideramos no ha sido efectiva:

> *"Cuando los códigos cortos asignados presenten un uso diferente a aquél para el que fueron asignados."* Frente a esta causal hemos evidenciado ausencia de supervisión por parte del administrador de los recursos de identificación, al no existir mecanismos de auditoría y control a los PCAs e IT, de manera preventiva, el riesgo de uso de los códigos cortos para un propósito diferente a la asignación definida a través de la resolución correspondiente, aumenta.

Cesión o transferencia de recursos

- En relación con la cesión o transferencia de recursos de identificación, ¿considera que deberían mantenerse las condiciones iniciales de asignación cuando un recurso de identificación sea cedido o transferido? Por favor, explique las razones que fundamentan su respuesta.

  RTA. Desde una perspectiva jurídica y conforme a las normas que regulan la cesión y transferencia de recursos de identificación, consideramos que las condiciones iniciales de asignación deben mantenerse cuando un recurso sea cedido o transferido a un nuevo titular. Ello en la medida en que dichas condiciones constituyen parte integral del acto administrativo de asignación y definen el alcance, finalidad y límites del uso autorizado del recurso. La continuidad de estas condiciones garantiza la estabilidad del régimen jurídico aplicable, evita vacíos regulatorios y previene usos distintos a los originalmente autorizados que podrían afectar la confianza de los usuarios y la integridad del sistema de identificación.

  No obstante, la permanencia de las condiciones iniciales no obsta para que la autoridad competente, en ejercicio de sus funciones de control y supervisión, verifique que el cesionario cumpla con los requisitos técnicos, operativos y jurídicos exigidos para el uso adecuado del recurso, ni para que, de manera excepcional y debidamente motivada, pueda ajustar o actualizar dichas condiciones cuando existan cambios normativos, tecnológicos o de interés público que así lo justifiquen. En todo caso, cualquier modificación posterior debería sujetarse a los principios de legalidad, proporcionalidad, debido proceso y seguridad jurídica.

- Para autorizar la cesión de un código corto, ¿qué tipo de documentación, validación previa o requisitos formales adicionales deberían exigirse a la persona jurídica que recibirá el código corto? Detalle y explique cada elemento propuesto.

  RTA. Adicional a los elementos exigidos en el artículo 6.4.2.2 "Procedimiento de asignación de la numeración de códigos cortos para SMS y USSD" es importante validar que el cesionario, tanto la persona jurídica como el representante legal, en el momento de la solicitud de la cesión del código corto no estén involucrados en una investigación administrativa que aún no haya concluido; de ser el caso no se le debería permitir el trámite de cesión del código corto.

- Con base en su experiencia, ¿considera que para códigos cortos debería prohibirse la cesión de estos recursos? ¿Qué aspectos considera que la regulación debe priorizar para mitigar estos riesgos? Justifique su respuesta.

  RTA. Conforme a lo señalado en los comentarios generales, no se evidencia que la problemática esté asociada a la cesión o transferencia formal de la numeración. El riesgo se origina, más bien, cuando el asignatario de un código corto autoriza su uso a un tercero sin que medie una cesión debidamente registrada por la CRC ni un cambio formal de titularidad.

  Este tipo de "préstamo" o habilitación informal, sumado a la utilización de un mismo código para múltiples marcas o clientes, termina por diluir la trazabilidad y la atribución de responsabilidades frente al contenido, el origen del tráfico y la atención de reclamaciones. En la práctica, se generan zonas grises que dificultan la supervisión, la investigación de incidentes y la adopción de medidas correctivas oportunas.

  Es por esto por lo que es imperativo prohibir expresamente dichas prácticas de préstamo o uso por terceros. En ese sentido, se recomienda que la regulación delimite de forma explícita que el uso de códigos cortos y, si aplica, de numeración E.164 para SMS, debe realizarse exclusivamente por el asignatario, evitando esquemas informales que habiliten su uso. En caso de configurarse el escenario para una cesión de estos recursos, se debe cumplir el procedimiento que defina la CRC para tal fin y el cumplimiento de los requisitos correspondientes.

- Respecto a la cesión o transferencia de recursos de identificación, ¿considera que la CRC debe imponer condiciones para mantener la asignación de un código corto, tal como validar el estado vigencia de la matrícula mercantil de la razón social que solicita un código corto? Por favor, sustente su respuesta.

  RTA. En relación con la cesión o transferencia de recursos de identificación, consideramos que la CRC sí puede imponer condiciones orientadas a verificar la capacidad jurídica del

solicitante para mantener la asignación de un código corto, en la medida en que dichas condiciones se encuentren directamente relacionadas con la correcta administración del recurso y con la responsabilidad asociada a su uso. En este sentido, validar la vigencia de la matrícula mercantil de la razón social que solicita la cesión o transferencia resulta jurídicamente razonable, toda vez que permite confirmar la existencia legal y la capacidad para asumir las obligaciones derivadas del acto administrativo de asignación.

Además de la validación de la vigencia de la matrícula mercantil, la CRC podría incluir otras condiciones adicionales razonables y jurídicamente sustentables, coherentes con su rol de administrador del recurso de identificación tales como:

- ✓ Verificar que la persona que actúa en nombre de la razón social cuente con representación legal vigente y facultades suficientes para solicitar la cesión o transferencia.
- ✓ Exigir una declaración formal mediante la cual el cesionario acepte íntegramente las condiciones regulatorias vigentes asociadas al uso del código corto.
- ✓ Verificar que el objeto social o la actividad económica declarada tenga relación directa con el uso que se pretende dar al código corto.
- ✓ Revisar si el solicitante ha sido objeto de medidas correctivas o sanciones previas relacionadas con el uso indebido del recurso objeto de la cesión
- ✓ Exigir que se informe si el código corto será utilizado por terceros (integradores tecnológicos).

Suspensión preventiva del tráfico

- En relación con la suspensión preventiva del tráfico asociado a un código corto, ¿qué condiciones o supuestos deberían considerarse para habilitar la aplicación de esta medida durante el desarrollo o inicio de la actuación administrativa para la eventual recuperación del recurso? Por favor, explique su respuesta.

  RTA. Se considera pertinente incorporar de forma expresa una causal de recuperación del recurso de identificación asociada a actividades fraudulentas cuando existan presuntos indicios de uso indebido del recurso soportados en las quejas o reportes allegados a la Comisión.

  Importante que la suspensión temporal del tráfico asociado al código corto vinculado en la actuación administrativa sea obligatoria y exigible para todos los actores de la cadena, desde el PCA (y demás intermediarios que participen en el encaminamiento del tráfico) hasta el PRST, de manera que se eviten vacíos de implementación o interpretaciones fragmentadas que permitan que el tráfico continúe cursándose por algún eslabón.

Para que esta medida sea efectiva, es necesario que la CRC establezca un tiempo máximo de atención a la denuncia o reporte hecho ante un posible fraude que no supere los 3 días hábiles para iniciar la actuación administrativa y que permita realizar la suspensión del código corto y del tráfico que está cursando por dicho código.

- Desde su experiencia, ¿cuáles serían los principales beneficios de aplicar una suspensión preventiva del tráfico en casos de presunto uso indebido vinculados a un código corto? Explique sus razones.

  RTA. La aplicación de una suspensión preventiva del tráfico asociada a un código corto frente a indicios razonables de presunto uso indebido genera beneficios relevantes tanto para la protección de los usuarios como para la gestión eficiente del riesgo. En primer lugar, esta medida permite mitigar de manera inmediata el potencial daño a los usuarios, evitando la continuidad de mensajes o comunicaciones que podrían inducir a error, fraude o afectaciones económicas, mientras se adelanta la verificación correspondiente. La posibilidad de actuar de forma temprana resulta especialmente relevante en contextos de fraude, donde la velocidad de propagación es un factor crítico.

  En segundo lugar, la suspensión preventiva constituye una herramienta operativa eficaz para contener el impacto reputacional y de confianza en los servicios de mensajería, tanto para los usuarios como para el ecosistema de telecomunicaciones en general.

  La suspensión preventiva, al ser temporal, focalizada y sujeta a criterios objetivos, no implica un prejuzgamiento sobre el asignatario, sino que se configura como una acción de gestión del riesgo, compatible con el respeto al debido proceso y con la posibilidad de restablecer el servicio una vez aclarada la situación.

- En cuanto a los posibles impactos, ¿qué riesgos, limitaciones o efectos no deseados podrían derivarse de la aplicación de una suspensión preventiva del tráfico durante el desarrollo o inicio de la actuación administrativa? Detalle y explique los elementos que considere relevantes.

  RTA. Es fundamental que se fijen criterios objetivos claros que llevan a una suspensión preventiva, por ejemplo, si se tienen evidencias de que un código corto asignado presenta un uso diferente a aquel para el que fue asignado y bajo el entendido que esta es una causal de recuperación de la numeración de códigos cortos, procede la suspensión preventiva como mecanismo de gestión de un riesgo identificado.

  Así mismo, la CRC debe precisar en el proceso de suspensión preventiva, la duración de esta y los tiempos que tomará iniciar la investigación administrativa correspondiente.

- Sobre las garantías del debido proceso, ¿qué elementos considera adicionales para establecer la medida de suspensión del tráfico durante el desarrollo o inicio de la actuación administrativa en casos de presunto uso indebido del código corto? Describa y explique los pasos que considere adecuados.

  RTA. La CRC debe establecer de manera expresa las circunstancias que habilitan la suspensión preventiva, tales como volúmenes atípicos de PQR, evidencia técnica de suplantación o reiteración de conductas asociadas a fraude, evitando criterios indeterminados o discrecionales.

  La suspensión debe formalizarse mediante un acto administrativo debidamente motivado, en el que se indiquen los hechos, las razones técnicas y jurídicas, el alcance de la medida (código corto específico), su duración y las condiciones para su levantamiento.

  Ahora bien, el PRST quien actúa como ejecutor operativo de la suspensión, requiere de un marco claro que le permita actuar con agilidad sin comprometer las garantías del debido proceso.

Actualización y trazabilidad de información

- Sobre la actualización de información, ¿considera que debe incluirse como causal de recuperación de los recursos asignados el incumplimiento en la actualización de los datos en las bases de la CRC, como el RPCAI, conforme al Registro Único Empresarial y Social (RUES) de la sociedad asignataria? Por favor, justifique su respuesta.

  RTA. Consideramos pertinente que el incumplimiento en la actualización de los datos en las bases de la CRC, como el RPCAI, conforme a la información reportada en el Registro Único Empresarial y Social (RUES), pueda incluirse como causal de recuperación de los recursos de identificación asignados. Esta medida contribuye directamente a garantizar la legitimidad, trazabilidad y responsabilidad del PCA como titular del recurso, en tanto permite a la autoridad verificar de manera permanente la existencia jurídica, representación legal y capacidad operativa del asignatario.

  Desde una perspectiva jurídica, la administración de los recursos de identificación exige que estos se encuentren asignados a sujetos plenamente identificables y jurídicamente vigentes, condición que se ve comprometida cuando la información registrada ante la CRC no se encuentra actualizada o no coincide con los datos oficiales del RUES. La falta de actualización impide el ejercicio efectivo de las funciones de control y supervisión, debilita la exigibilidad de responsabilidades frente a eventuales usos indebidos y puede facilitar escenarios de anonimato o intermediación irregular en la utilización del recurso.

- ¿Considera que la CRC debería incorporar una causal específica de recuperación de códigos cortos que permita suspender de manera preventiva la autorización de uso cuando el asignatario no actualice la información conforme con el Registro Único Empresarial Social (RUES)? Por favor, justifique su respuesta.

  RTA. Consideramos pertinente que la CRC incorpore una causal específica de recuperación de códigos cortos que permita suspender de manera preventiva la autorización de uso cuando el asignatario no mantenga actualizada su información conforme al Registro Único Empresarial y Social (RUES). Esta medida fortalece la legitimidad y trazabilidad del titular del recurso, elementos esenciales para la gestión operativa y la prevención de usos indebidos asociados a fraudes a través de mensajes de texto.

  La falta de actualización de los datos dificulta la identificación del responsable del código corto, limita la capacidad de reacción frente a reportes de abuso y aumenta el riesgo de que el recurso sea utilizado por terceros no autorizados o en contextos irregulares. En este sentido, la suspensión preventiva de la autorización de uso se configura como una medida razonable de gestión del riesgo, orientada a proteger a los usuarios y al ecosistema de mensajería, más que como una sanción.

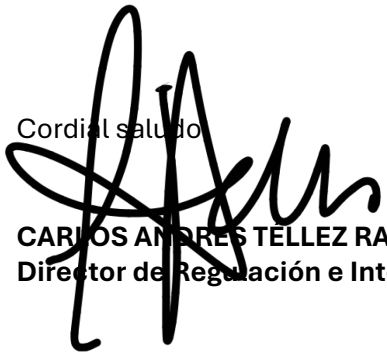
- ¿Considera que la CRC debería establecer alguna medida regulatoria adicional en los eventos en los que exista conducta reincidente ante el uso indebido de códigos cortos? Por favor, justifique su respuesta.

  RTA. Consideramos pertinente que la CRC establezca medidas regulatorias adicionales en los casos en que se configure una conducta reincidente en el uso indebido de códigos cortos. La reincidencia evidencia un incumplimiento sistemático de las condiciones de uso del recurso de identificación y una gestión inadecuada de los riesgos asociados, lo que justifica la adopción de medidas diferenciadas y de mayor intensidad frente a los mecanismos correctivos ordinarios.

  En este contexto, una medida razonable y proporcional consiste en la inhabilitación temporal del representante legal responsable del recurso para solicitar la asignación de nuevos códigos cortos, por un período determinado. Esta medida no tiene un carácter meramente sancionatorio, sino preventivo y disuasivo, en la medida en que incentiva una gestión responsable del recurso y refuerza la obligación de supervisión efectiva por parte del titular. Asimismo, al focalizarse en el responsable del uso del código corto y no de manera indiscriminada sobre la totalidad de la empresa o del servicio, se evita afectar de forma desproporcionada operaciones legítimas.

- ¿Qué consecuencias regulatorias adicionales considera adecuadas en caso de que los asignatarios no actualicen su información según lo estipulado? Por favor, justifique su respuesta.

RTA. Como lo mencionamos anteriormente, consideramos pertinente que la CRC incorpore una causal específica de recuperación de códigos cortos que permita suspender de manera preventiva la autorización de uso cuando el asignatario no mantenga actualizada su información conforme al Registro Único Empresarial y Social (RUES). Esta medida fortalece la legitimidad y trazabilidad del titular del recurso, elementos esenciales para la gestión operativa y la prevención de usos indebidos asociados a fraudes a través de mensajes de texto.



Cordial saludo,

CARLOS ANDRES TELLEZ RAMIREZ.
Director de Regulación e Interconexión