Bogotá, enero 15 de 2026

Señores
CRC
Equipo Diseño Regulatorio

Ref: Comentarios al Documento de Alternativas Regulatoria - Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles

En Inalambria agradecemos el trabajo adelantado por la Comisión de Regulación de Comunicaciones en el análisis del fenómeno de fraude cibernético a través de servicios móviles, así como la apertura del proceso de consulta pública para recoger las visiones de los distintos actores del ecosistema.

También reconocemos que el fraude vía SMS es un problema creciente, complejo y dinámico, cuya mitigación exige una aproximación integral, técnica y coordinada entre regulador, operadores, agregadores, integradores tecnológicos, sector financiero y entidades de control.

A través de este documento buscamos:

1. Compartir nuestra visión sobre el canal SMS y el problema en discusión.
2. Formular una propuesta concreta de mitigación basada en nuestra experiencia práctica trabajando activamente en la prevención de fraude.
3. Responder a las preguntas formuladas por la CRC en el documento original.

reiterando nuestra intención de colaborar activamente en los espacios que la CRC designe para continuar en la búsqueda de las soluciones más efectivas para mitigar y erradicar el problema del fraude cibernético a través de SMS.

1. La visión de Inalambria sobre el canal de mensajes de texto SMS.

SMS como tecnología habilitadora. El SMS ha sido, y continúa siendo, una tecnología habilitadora fundamental para el desarrollo económico y social en Colombia. Nuestra experiencia de más de 20 años operando el canal, trabajando con empresas de todos los tamaños, desde las entidades financieras más grandes del país hasta microempresas y consultorios médicos en municipios rurales,lo c onfirma.

En el contexto colombiano los mensajes de texto son el canal más universal, accesible incluso en zonas con baja penetración de datos móviles; son un canal inclusivo, clave para pequeñas y medianas empresas, servicios públicos, salud, educación y banca, y finalmente se han

convertido en parte crítica de la infraestructura digital del país para generar notificaciones, autenticaciones, alertas y comunicaciones transaccionales. Por estas razones, cualquier medida regulatoria debe, por tanto, proteger al canal sin debilitar su accesibilidad, competitividad y capacidad de inclusión económica.

El fraude como problema sistémico, no aislado. El fraude vía SMS no es atribuible a un único actor. Es un fenómeno producto de la interacción entre incentivos económicos, asimetrías de información, falta de trazabilidad de origen y las capacidades técnicas desiguales entre actores. Por esta razón, consideramos fundamental que los esfuerzos regulatorios se enfoquen en los puntos del ecosistema con mayor capacidad real de prevención, distribuyan responsabilidades de forma proporcional al nivel de control, visibilidad e impacto y por último eviten trasladar de manera exclusiva la carga de contención a un solo eslabón de la cadena.

También resulta importante reconocer que en Colombia el SMS es un canal excepcionalmente costo-efectivo para cometer fraude por varias razones puesto que las tarifas de mercado son de las más bajas a nivel mundial, lo cual reduce drásticamente el costo de intentos masivos de fraude y hace de éste un negocio extremadamente rentable. Actualmente, la responsabilidad operativa y reputacional de “contener” dicho fraude recae exclusivamente en agregadores e integradores tecnológicos, incluso cuando no controlan la red de acceso y no tienen visibilidad completa del destino final generando un desequilibrio que trae: riesgos operativos, incentivos mal alineados, barreras de entrada para nuevos participantes formales

Consideramos que la propuesta regulatoria debe evolucionar hacia un modelo de responsabilidad compartida y coordinada, recordando que las medidas que se adopten en el corto plazo deberán contribuir también a la mitigación del riesgo presente en las nuevas modalidades de fraude y delitos digitales: empresas ilegales que promueven apuestas, juegos en línea y préstamos digitales fuera de la ley; en adición a que se convertirán en un precedente regulatorio importante ante la adopción de tecnologías emergentes como RCS que gradualmente reemplazarán a los mensajes de texto.

Por último, en Inalambria creemos que un marco regulatorio demasiado restrictivo, técnicamente rígido o poco inclusivo podría repetir los mismos problemas en nuevos canales, afectando su adopción y escalabilidad.

2. Nuestra propuesta.

La propuesta de Inalambria se basa en dos principios: 1) la redistribución de responsabilidades entre los actores del ecosistema, acorde con su rol, capacidades y nivel de control y 2) la adopción de mecanismos técnicos proactivos, automatizados y colaborativos, que permitan anticipar y bloquear el fraude antes de que impacte al usuario final; privilegiando la prevención proactiva sobre los esquemas exclusivamente sancionatorios o reactivos frente a reincidencias.

Específicamente, sugerimos:

a. *Propuesta 1: La implementación de un mecanismo técnico de prevención proactiva y colaborativa contra el fraude*.

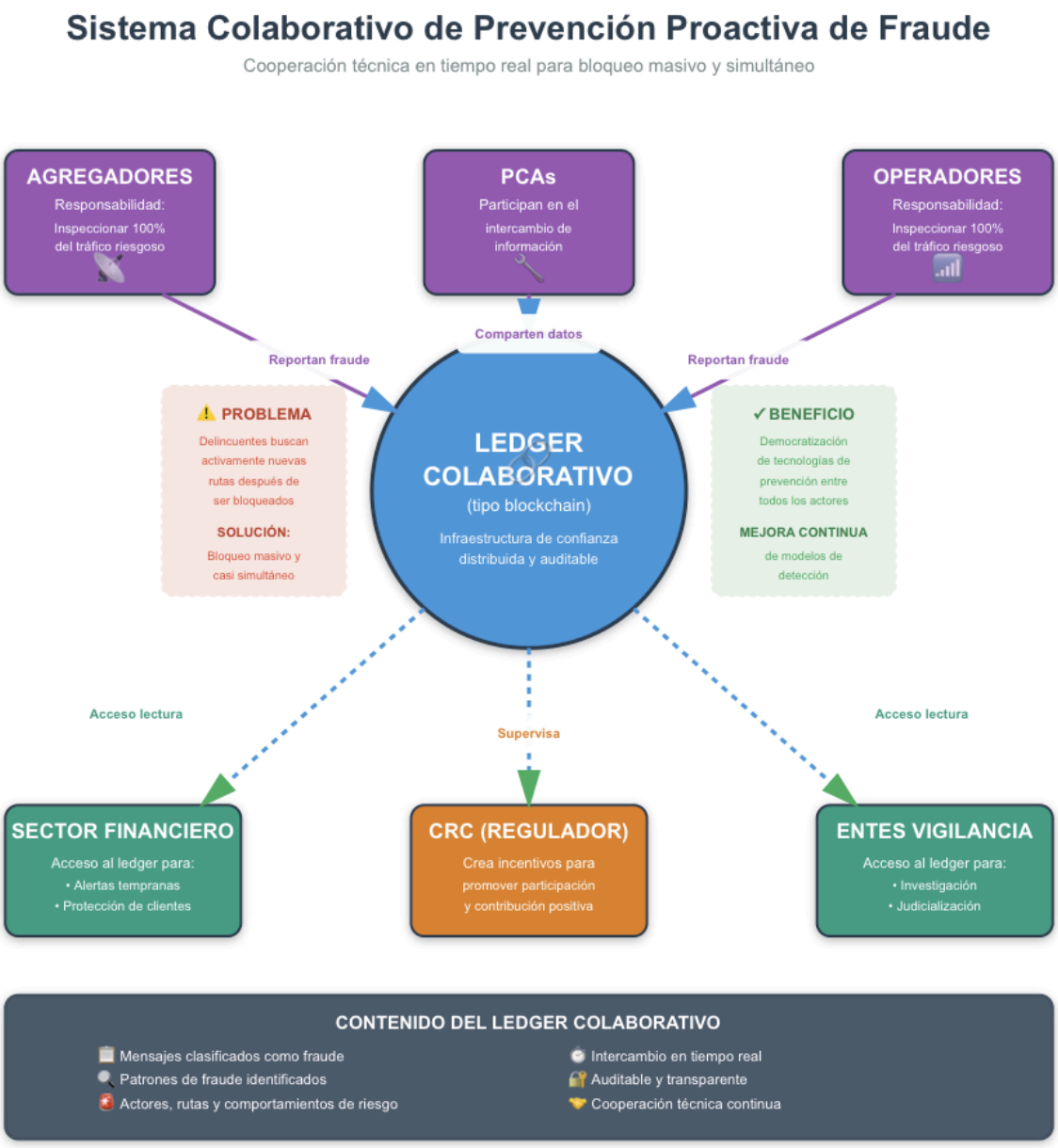
En una estrategia de lucha frontal basada en la cooperación técnica entre los actores, proponemos la creación de un sistema en línea de intercambio seguro de eventos de riesgo (mensajes de fraude identificados por operadores y agregadores) con el fin de que una vez un fraude sea detectado por alguno de los actores, éste pueda ser reportado de inmediato al sistema y el resto de actores pueda incorporarlo en casi tiempo-real en sus sistemas propios de detección evitando que el mismo fraude pueda llegar a destinatarios a través de otros nodos con acceso a la red de mensajes de texto.

¿Por qué? Porque en nuestra experiencia combatiendo el fraude hemos visto cómo los delincuentes buscan activamente nuevas rutas para entregar mensajes de fraude después de que son bloqueados en su primer intento y creemos que una estrategia articulada de bloqueo masivo y casi simultáneo les impediría lograr sus objetivos. Además, entendemos que no todos los actores del ecosistema tienen acceso a las mismas tecnologías de prevención de fraude y éste sería un mecanismo para democratizar la prevención entre quienes pueden contenerla: operadores y agregadores.

El componente central del mecanismo propuesto es un ledger colaborativo de prevención (modelo tipo “blockchain”) auditable que le permita a agregadores y operadores y demás actores, compartir mensajes clasificados como fraude y patrones de fraude, identificar actores, rutas y comportamientos de riesgo y permita mejorar continuamente los modelos de detección. Este ledger no debe entenderse como una criptomoneda, sino como una infraestructura de confianza distribuida con el fin de detectar proactivamente el fraude y asegurar que cada actor toma las medidas necesarias para bloquear el tráfico en su red. Correspondería a la CRC crear incentivos que promuevan la participación de todos los actores, con el fin de premiar a quienes contribuyan constructivamente al ledger.

En este nuevo esquema tanto agregadores como operadores tendrían la responsabilidad de inspeccionar el 100% de su “tráfico riesgoso”, definiéndose como tráfico riesgoso para agregadores todo aquel que provenga de clientes nacionales o internacionales cuyo responsable de originación de mensajes no sea fácilmente identificable; y para operadores todo aquel tráfico que provenga de códigos cortos activados a PCAs con “tráfico riesgoso” o activados a agregadores que reportan cuáles de sus códigos cortos podrían ser usados para cometer fraude.

Los demás actores como el sector financiero y entes de vigilancia también tendrían acceso al ledger con el fin de activar alertas tempranas a sus clientes finales e iniciar tareas de investigación y judicialización de delincuentes cuando sea posible.



Este modelo prepara al ecosistema SMS Colombiano para el control proactivo frente a la siguiente generación de modalidades de fraude que estamos empezando a combatir: mensajes de empresas de apuestas no autorizadas que operan en el país y compañías de préstamos digitales “gota-gota”, ambas utilizando el canal SMS para adquirir a sus clientes; puesto que trataría de una nueva modalidad de mensajes que se clasificarían como riesgosos y se distribuirían instantáneamente al ecosistema a través del ledger, con participación activa en este caso de entidades de control como Coljuegos y la Superfinanciera.

b. *Propuesta 2: La definición de un esquema de identificación de recursos escalonado e inclusivo*.

La regulación de precios del mercado SMS ha logrado que el uso de mensajes de texto A2P per cápita en Colombia sea diez veces superior al de nuestros países vecinos. Lograr que este avance beneficie no sólo a las empresas más grandes del país sino a pequeñas y medianas empresas debe ser el siguiente objetivo.

Por lo tanto exigir que todos los mensajes deben originarse a través de SenderIDs alfanuméricos impone limitaciones técnicas (puesto que según el protocolo sólo es posible utilizar 11 caracteres para incluir a los cientos de miles de empresas que querrían usar este recurso) y operativas (pues se vuelve impráctico y confuso que la carnicería Don Andrés de la esquina -SenderID: “AndresCarne” compita con el SenderID de “AndresCarne” del famoso restaurante Colombiano).

Nuestra propuesta plantea el diseño de un esquema de identificación de originadores con tres categorías:

1.1. Códigos Cortos Compartidos para individuos, pequeños empresarios o comerciantes y PYMES que están dispuestos a reutilizar el mismo recurso de numeración siempre y cuando el agregador o PCA que los representa pueda garantizar el control de fraude.

Este esquema garantiza que las empresas más pequeñas del país puedan utilizar de manera costo eficiente el canal a través de alternativas de compra de mensajes vía e-commerce y similares.

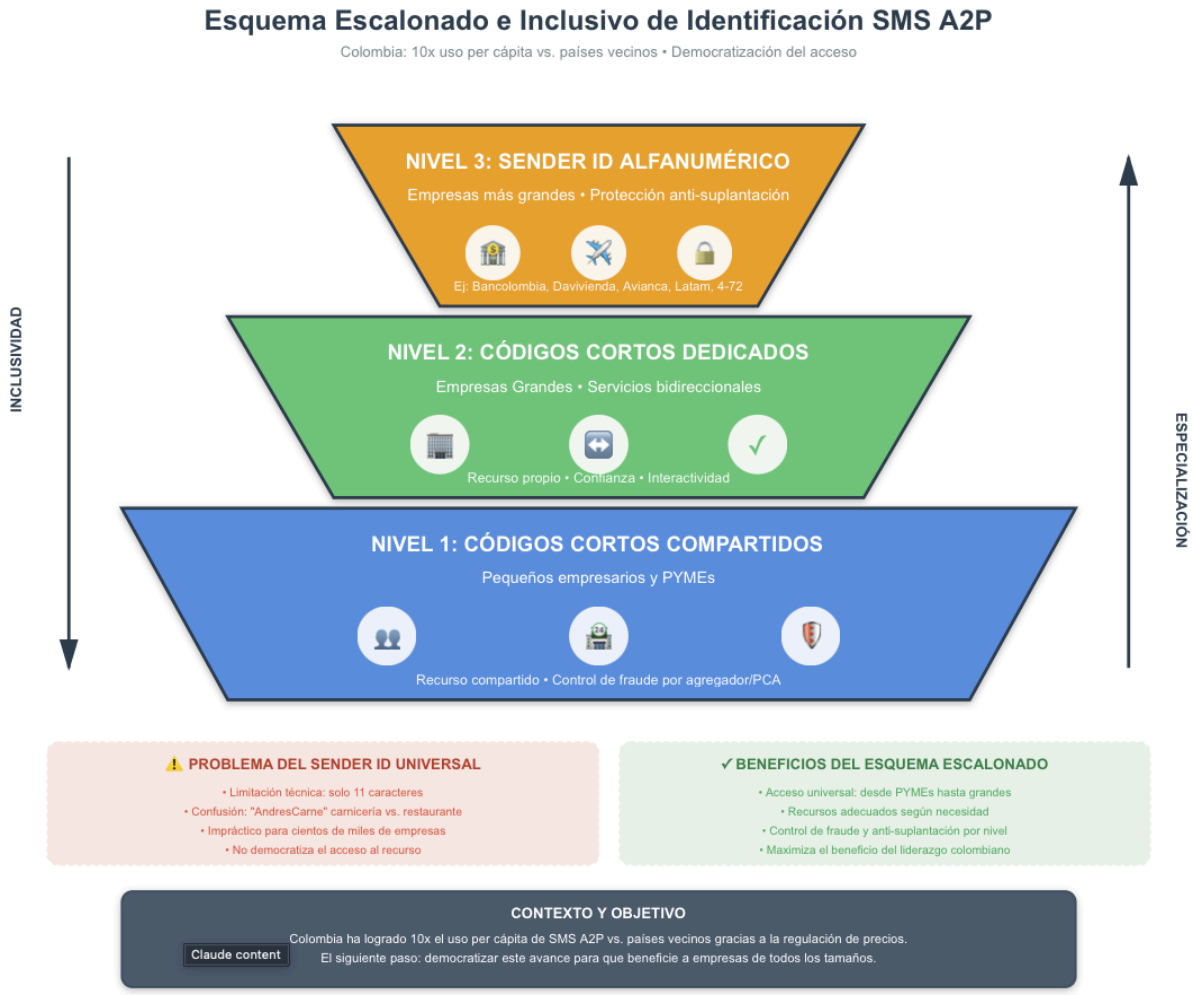
1.2. Códigos Cortos Dedicados para Grandes Empresas y aplicaciones de doble-vía puesto que resulta de vital importancia contar con recursos propios para transmitir confianza y soportar servicios interactivos a través de mensajes.

Como funciona en la actualidad, este esquema permite que las empresas puedan asumir la responsabilidad directa por los mensajes que envían, transmitiendo mayor tranquilidad a sus usuarios a través de los códigos cortos que tienen asignados en adición a permitir la implementación de servicios de doble vía para aplicación que así lo requieran (confirmaciones de transacciones, de citas, entre otros).

1.3. Sender ID alfanumérico para Empresas Grandes que lo requieran por ser los principales sujetos de suplantación. Este avance le ayudaría a las empresas consumidoras de mensajería SMS A2P más grandes del país (ej: Bancolombia,

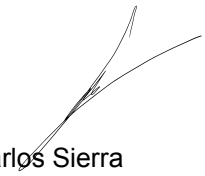
Davivienda, Avianca, Latam, 4-72) y que están sujetas a los mayores riesgos de suplantación, a proteger a sus usuarios de mensajes informativos que pretenden engañarlos puesto que sólo ellas, a través de sus agregadores y la coordinación directa con los operadores, estarían en capacidad de generar mensajes con dichos SenderIDs.

En la práctica este mecanismo, aunque es opcional, sería altamente deseado por los grandes consumidores de SMS del país y resultaría fácil de implementar puesto que sólo requiere que, al momento en el que un operador activa un código corto para un agregador o PCA, se solicite la activación del SenderID alfanumérico previa validación de los documentos que demuestran la relación comercial entre el agregador solicitante la empresa o marca detrás del nuevo recurso identificación. Los operadores en este caso tendrían la responsabilidad de administrar este componente adicional al proceso actual de aprovisionamiento de códigos cortos y configuración en su red.



Con la implementación de estas dos acciones específicas, el ledger para distribuir los eventos de fraude y el sistema de identificación escalonado, en Inalambria creemos que el país daría un salto importante en la dirección correcta, dándole continuidad a las políticas de la CRC que pretenden llevar el uso de los mensajes de texto a más sectores de la economía y avanzando simultáneamente de manera firme en la lucha contra el crímen organizado de delincuentes cibernéticos que usan SMS para promover el fraude actual y del futuro.

Cordiamente,



Carlos Sierra
Director General
Equipo Inalambria
carlos.sierra@inalambria.com
www.inalambria.com

3. Respuestas a Preguntas formuladas por la CRC

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?

    - Agregadores como Inalambria están preparados para la implementación de las medidas que sean necesarias. Por ejemplo, el soporte para la configuración de SenderIDs está disponible en nuestras plataformas y realizar las adecuaciones a clientes existentes, podrías ser implementable en menos de 3 meses con todos nuestros clientes más importantes.
    - La participación en el sistema compartido de alertas de fraude, usando tecnologías blockchain, podría tomar entre 3 y 4 meses debido a la curva de aprendizaje en el uso de este tipo de tecnologías
    - Nuestra propuesta escalonada de implementación:

Fase	Medida	Importancia Estratégica
1	Creación y puesta en marcha del proceso configuración de SenderIDs controlado directamente por los operadores móviles.	Permite que las empresas más grandes de Colombia que hoy están expuestas a suplantaciones puedan empezar a enviar mensajes de texto desde un identificador único (Bancolombia, Davivienda, LATAM, Avianca, 4-72, Servientrega, entre otras empresas que hoy son sujetas a suplantación), algo imposible para los delincuentes. Esta medida debería ser adoptada de manera voluntaria por quienes crean que se benefician -> Aumento en la confianza de los usuarios finales, logrando que se identifiquen genuinamente los mensajes originados por empresas sujetas a suplantación.
2	Creación y puesta en marcha del sistema de detección proactiva y distribución en línea de mensajes de fraude, adopción por parte de todos los agentes de la cadena (agregadores, operadores y sector financiero y otros)	Permite que los mensajes de fraude puedan ser bloqueados de manera simultánea por agregadores y operadores. -> Se cierran las puertas a los mensajes de fraude de manera simultánea.
3	Implementación de actividades de divulgación	Aumentar el conocimiento del problema por parte de usuarios finales y enviar mensajes ejemplificantes sobre las consecuencias del uso de mensajes de texto para cometer delitos cibernéticos.

- ¿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?

  Creemos que de manera simultánea debe evaluarse (por lo menos trimestralmente):

  1. El número de incidentes de fraude reportados por la ciudadanía
  2. El número de mensajes de fraude bloqueados proactivamente tanto por agregadores como por operadores.

  Una tendencia decreciente en 1 y creciente en 2, debería ser el objetivo.

- ¿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?

  La implementación de un sistema de validación distribuido (DLT) de originadores de contenido (y no del contenido como tal) no necesariamente contribuye a bloquear la fuente principal de tráfico fraudulento del país: Delincuentes que contratan a agregadores internacionales, que a su vez contratan a agregadores nacionales para entregar su tráfico (“tráfico problema”). Si bien la medida puede verse como la evolución del sistema actual de control y administración de códigos, se queda corta a la hora de identificar quienes son los verdaderos originadores de tráfico SMS puesto que

para el sistema de validación de originadores un agregador internacional estaría plenamente identificado, sin embargo sus miles de clientes no.

Aquí un sistema incluyente (las 3 categorías de identificación de originadores mencionadas anteriormente en nuestra propuesta) y un sistema distribuido para colaborar en la identificación proactiva de tráfico de fraude, creemos que pueden generar una disminución contundente en el corto plazo del fenómeno 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 y 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?

  Mensajes de fraude bloqueados, reportes de la ciudadanía, como se mencionó anteriormente.

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?

  Hoy todos los agregadores realizan verificaciones KYC de alguna manera, inclusive los que le vendemos a todos los espectros de la economía (desde PYMES hasta Grandes Corporaciones), sin embargo en la práctica y para los casos en donde resulta imposible identificar el último eslabón de la cadena de fraude (empresas que contratan agregadores internacionales, que a su vez contratan a agregadores nacionales para entregar su tráfico), esta medida no resolvería del todo el problema.

  KYC para pequeñas las empresas más pequeñas no resulta ser práctico, pues muchas de ellas no son formales y son difícilmente identificables más allá de un un email y un teléfono móvil de contacto. Para estos casos y para evitar la exclusión, se requieren plataformas que estén en capacidad de detectar fraude proactivo usando los avances más recientes de inteligencia artificial y otras tecnologías disponibles. (Ver. https://www.inalambria.express/post/ia-avanzada-inalambria-express-fraudes-sms)

- 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?

Nuestra propuesta es que todos los agregadores nacionales que permitan la terminación de tráfico internacional deben implementar, para dichas conexiones, estrictas medidas de inspección proactiva de tráfico apoyados en el sistema de distribución de mensajes fraudulentos propuesto.

En adición a esto, todos los operadores móviles deben implementar medidas de control similares (inspección de tráfico) para aquellas conexiones que puedan contener “tráfico problema”, obligando a los agregadores o PCAs a compartir información de cuáles de sus clientes (o qué códigos cortos) generan dicho tráfico.

Estas dos medidas generaría un bloqueo efectivo a los agentes generadores de fraude.

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

  No. Agregaría fricción al proceso de activación de nuevos clientes (limitando el acceso especialmente en empresas pequeñas) y no contribuiría al objetivo de identificar quienes cometen fraude hoy (delincuentes que contratan a agregadores internacionales que a su vez contratan a agregadores nacionales) debido a la longitud en la cadena.

- ¿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?

  Un sistema centralizado podría tornarse burocrático, ineficiente e impráctico. La administración de SenderIDs alfanuméricos no requiere un sistema complejo, simplemente la posibilidad de que operadores puedan activar el servicio previa verificación de la relación que existe entre agregadores y empresas que solicitan el SenderID. En la actualidad, este proceso podría tomar algunos minutos más en los procesos de aprovisionamiento de códigos cortos que los operadores ya realizan con integradores o PCAs.

- ¿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?

  El modelo distribuido para prevención proactiva de fraude resulta ser la aplicación ideal para distribuir hallazgos de tráfico y transmitirlos en casi-tiempo-real a todos los jugadores del ecosistema con el ánimo de que puedan bloquearse aquellos mensajes, antes de que lleguen a sus destinatarios.

El uso de un modelo distribuido para validación de identificadores (códigos cortos y SenderIDs) como se propone en el documento de alternativas regulatorias, creemos que es innecesario y no resuelve el problema fundamental.

- ¿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?

  Los avances tecnológicos recientes permiten inspeccionar mensajes de texto con URLs y determinar, con un nivel muy alto de precisión, cuáles son mensajes con contenido fraudulento y cuáles no. Nuestra experiencia de los últimos 12 meses usando una combinación de técnicas de “embeddings”, “deep-learning” y “IA agéntica” nos permiten con seguridad afirmar que el fraude sí se puede contener proactivamente.

- ¿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?

  Es una medida que infortunadamente distorsiona el valor utilitario de los mensajes de texto, especialmente cuando la longitud de los mensajes está limitada a tan sólo 160 caracteres; y no necesariamente combate el problema de raíz.

  Gracias a la CRC, Colombia es el país con el consumo per cápita de SMS A2P más alto del mundo. Controlar la legitimidad de cada empresa originadora de mensajes no necesariamente va a mitigar el problema. En Inalambria creemos que los esfuerzos regulatorios deben estar enfocados en aquellos agentes de la cadena que tienen la capacidad operativa de prevenir el problema sin agregar artificios que operativamente costosos.

- ¿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?

  La clasificación obligatoria de los mensajes por tipo de contenido va en línea con los planes de evolución de producto que tenemos agregadores como Inalambria, sin embargo requiere un esfuerzo logístico importante pre-envío por parte de las empresas generadoras de mensajes y los agregadores que contratan, teniendo que adecuar su infraestructura ó un esfuerzo técnico importante para agregadores que requieran clasificar automáticamente su tráfico (usando modelos predictivos). Sin embargo, hasta que el RNE no sea un mecanismo maduro de control, es difícil garantizar la efectividad de un nuevo modelo en donde el bloqueo para usuarios finales se haga a partir de estos sistemas de clasificaicón.ó

- ¿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?
    - Capacidades de detección a partir de heurísticas de fraude (“embeddings”)
    - Capacidades de detección a partir de inspección profunda de mensajes que contengan URLs
    - Capacidades que puedan demostrar el uso práctico de AI para combatir el problema.

- ¿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?

  La propuesta incluyente y escalonada puede ser una solución práctica al problema de identificación responsable de agentes y empresas.

  Obligar a que todas las empresas o marcas de Colombia tengan un código alfa o corto representa un reto logístico importante y haría dispendioso, especialmente para empresas pequeñas, el uso del canal.

- ¿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?

  La obligatoriedad en el uso de SenderIDs alfanumericos resulta impráctica para empresas que quieren usar mensajes de texto para aplicaciones interactivas.

  Sugerimos que sea opcional y recomendable para empresas grandes sujetas a suplantación, pues hay numerosos casos de uso en donde los mensajes de texto originados desde códigos cortos numéricos son útiles:
    - Pequeñas y medianas empresas que reutilizan un código corto de un agregador para mantener sus costos de comunicación bajos.
    - Grandes empresas que requieren usar mensajes de texto para implementar servicios interactivos.

- ¿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?

  Es el mecanismo ideal para identificar confiablemente a los originadores de mensajes, especialmente grandes empresas sujetas a suplantación.

Creemos que la limitación no debería hacerse por el tipo de mensajes (transaccionales), sino por el tipo de empresa, siendo un mecanismo opcional pero sugerido.

En nuestras conversaciones recientes con el sector financiero, el uso de SenderIDs alfanuméricos genera una alta receptividad e interés de adopción.

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

  Los firewalls SMS de operadores tienen esto resuelto. Si bien el fraude originado desde conexiones P2P es importante, éste representa un porcentaje marginal del total de mensajes de fraude, los cuales son generalmente enviados a través de conexiones A2P de alto rendimiento (procesando cientos o miles de mensajes por segundo).

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

  Dicho umbral debería ser definido por cada operador. Como referencia, Meta/Whatsapp sólo permite el envío de 250 en “business accounts” no verificadas.

- ¿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?

  En adición al contenido del fraude, utilizando el sistema distribuido, resultaría extremadamente útil compartir en tiempo real la meta-data (IPs, emails registrados, documentar uso de VPNs, entre otros) correspondiente a cada mensaje de fraude identificado.

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

No aplica para nuestro negocio.

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?

  Como agregadores, nuestra función es la de informar a nuestros clientes sobre las medidas que tomamos para prevenir fraude, especialmente a agregadores internacionales, con quienes trabajamos de la mano en la detección proactiva.

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

  Como la divulgación es para nuestros clientes empresariales, no debería representar una carga, pues se incluye en nuestras comunicaciones periódicas.

- 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.)

  - Guías de prevención
  - Ejemplos reales de fraudes
  - Recomendaciones prácticas
  - Y especialmente comunicaciones que logren disuadir a delincuentes al mostrar las implicaciones de sus actos (cárcel, multas, entre otros).

- 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.)

  Facturas, landing pages en operadores móviles y entidades con riesgo de suplantación.

- 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.)

  Todas las anteriores.

- 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?

  Hay mayor concientización sobre el problema. Si los datos se exponen públicamente, esta se convierte en una fuente de información importante para entrenar modelos.

  Conectar este portal con el sistema propuesto de intercambio de información de fraude a partir de blockchain permitiría darle mayor visibilidad a los mensajes de texto de fraude que intenten llegar al país, creando incentivos para que otro tipo de agentes (startups, entidades académicas, entre) la usen y la exploten para efectos de prevención.

- 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?

Una carga adicional, sin embargo creemos que vale la pena, pues conectada con el sistema distribuido para la detección proactiva, generaría impacto inmediato.

- ¿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.

  Si, pues permite conocer la efectividad de las medidas de control que está tomando el ecosistema, como se planteó en puntos anteriores.

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

  Código corto, texto de mensaje, modalidad de fraude, categoría de fraude, impacto y riesgo; entre otros.

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

  No vemos riesgos, siempre y cuando no se compartan datos que identifiquen a los usuarios afectados.

- ¿Qué componentes debería incluir una 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.)

  Principalmente campañas ejemplificantes que le muestren a los delincuentes que el delito del fraude cibernético tiene consecuencias serias (cárcel, entre otras).

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.

- El instrumento utilizado en la actualidad para prevenir contactos fraudulentos no es del todo efectivo. Hace que paguen “justos por pecadores”. El papel que juega la CRC como “juez” y “parte” genera un incentivo perverso para que cualquier reclamación, fundamentada o no, genere una acción administrativa de recuperación de códigos.
- Consideramos importante que exista un mecanismo que permita que agregadores nacionales representen a empresas internacionales que no tienen representación legal o domicilio en Colombia. Muchos de estas empresas tienen negocios o operaciones legítimas en el país, sin embargo no tienen ningún incentivo para registrarse oficialmente en el sistema de administración de recursos del país.

- 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.

  - El uso indebido es un concepto relativo, puesto que agregadores pueden hacer esfuerzos continuos de detección de fraude sin embargo la naturaleza cambiante de las modalidades de fraude hace que exista una venta de afectación mientras se incorporan las medidas de contención. A primera vista los agregadores pueden verse como quienes están haciendo uso indebido del recurso cuando en realidad son sus clientes en la parte final de la cadena que están buscando nuevas formas de delinquir.
  - El uso indebido realmente se da cuando después de un proceso de investigación imparcial, la CRC logra demostrar que el asignatario no está realizando el mayor de los esfuerzos para prevenir fraude y existen casos reiterados de fraude de la misma naturaleza.

Reincidencias

- 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.

  Ambos operadores móviles y agregadores deben ser los responsables por la prevención proactiva de fraude. El nivel de responsabilidad es el mismo y definir responsabilidades a ambos niveles aumenta la capacidad de contención.

- 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.

La recuperación de códigos cortos como medida de prevención no es efectiva mientras la CRC actúe como juez y parte dentro de un proceso de investigación.

Esta medida, sin investigaciones rigurosas, desconoce los esfuerzos que hacen los agregadores para prevenir el fraude y genera perjuicios económicos importantes p disminuyendo su capacidad operativa.

- 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.

  Si.

- 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.

  Los contratos que validen las relaciones comerciales que justifican el cambio.

- 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.

  No. La cesión de códigos es un mecanismo útil que hoy le brinda opciones a las empresas que contratan servicios de interconexión SMS con agregadores.

- 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 o vigencia de la matrícula mercantil de la razón social que solicita un código corto? Por favor, sustente su respuesta.

  Si, esto le agrega formalidad al proceso y permite que las empresas contratantes puedan entender la importancia del proceso de asignación de recursos.

- 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.

Un código corto puede operar como un activo compartido por múltiples marcas y destinado a tipos de contenido específicos. Por lo tanto, antes de aplicar una suspensión preventiva, debe considerarse que el bloqueo del código no solo afecta al presunto infractor, sino que impacta operaciones legítimas de otros clientes que cursan tráfico por el mismo código, incluyendo notificaciones de alto valor para los usuarios móviles.

- 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.

  En la práctica, la suspensión preventiva no representa beneficios claros cuando se aplica de forma general al código. Las marcas realizan esfuerzos importantes para comunicar y posicionar el uso de un código corto ante su base de usuarios con el fin de generar confianza. Si el código se bloquea, se obliga a un cambio de numeración, lo cual implica nuevos esfuerzos de comunicación y, adicionalmente, puede degradar la confianza previamente construida con los usuarios.

- 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.

  La aplicación de esta medida puede generar impactos relevantes, entre ellos:

  - Impactos operativos: necesidad de ejecutar cambios y ajustes en la operación para migrar tráfico o modificar configuraciones, incluyendo esfuerzos asociados a cambios de código corto.
  - Impacto sobre usuarios móviles: si el bloqueo se origina en uno o pocos casos reportados y aún no se ha demostrado que el contenido corresponde a fraude o riesgo real, se termina afectando a millones de usuarios que reciben notificaciones legítimas de diversas marcas a través del mismo código corto.
  - Impactos financieros para el IT adjudicatario del código: el bloqueo eleva el riesgo de retiro de clientes que cursan notificaciones por el código, afectando la continuidad del servicio y los ingresos asociados.

- 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.

  Para asegurar proporcionalidad y debido proceso, la medida debería ser quirúrgica y focalizada, evitando afectar a toda la base de usuarios y a marcas legítimas. En ese sentido, se propone:

- Bloqueo únicamente a los usuarios que interpusieron la reclamación, y solo respecto del tipo de contenido específico asociado al reporte.
- En la experiencia del integrador, se ha identificado que la mayoría de usuarios que reclaman no están inscritos en el RNE. La inscripción en el RNE reduce de manera importante la exposición a ciertos contenidos, dado que una proporción relevante del tráfico indebido suele circular por categorías asociadas a marketing. Por ello, si se aplica una medida preventiva, debería concentrarse en los usuarios reclamantes, en lugar de suspender de forma general el código corto completo.

- 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.

  Si. Esto crea un incentivo importante para que los asignatarios mantengan su información actualizada.

- ¿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.

  Si.

- ¿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.

  Los asignatarios que no implementen medidas de prevención de fraude, alineadas con las propuestas, deberán perder su licencia pues la prevención de fraude se convierte en un requisito obligatorio para operar.

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

  Ninguna.

—-------- FIN DE DOCUMENTO —--------