

Bogotá D.C., 4 de agosto de 2025

CECO: C030
AC-GAPRS-233-2026

Doctora
CLAUDIA XIMENA BUSTAMANTE OSORIO
Directora Ejecutiva
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Calle 59A BIS No. 5-53 - Edificio Link Siete Sesenta - Piso 9
medidasantifraude@crcom.gov.co

Asunto: Comentarios y respuesta a consulta de ETB al documento formulación del problema dentro del proyecto *"Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles"*

Respetada doctora Bustamante,

En atención al proyecto regulatorio mencionado en el asunto, la Empresa de Telecomunicaciones de Bogotá S.A. E.S.P., en adelante ETB, presenta de manera atenta, oportuna y respetuosa sus comentarios y observaciones sobre el documento de formulación del problema y da respuesta a la consulta sectorial planteada en el mismo.

I. Comentarios Generales

El documento de formulación del problema publicado por la Comisión de Regulación de Comunicaciones (CRC) menciona las barreras existentes para mitigar el fraude cibernético cometido a través de los servicios de voz móvil y mensajes cortos (SMS), análisis que se enmarca en la creciente preocupación por la seguridad digital y la protección del usuario final en el ecosistema de telecomunicaciones.

En ese contexto, ETB reconoce la importancia de abordar el fraude cibernético como una amenaza creciente para la confianza digital y la protección del usuario. Sin embargo, observamos con preocupación que el enfoque planteado en el documento concentra su análisis desde la perspectiva de los PRST, omitiendo actores clave del ecosistema digital que tienen un rol determinante en la génesis y proliferación del fraude, lo que incrementa la asimetría regulatoria entre los PRST y estos actores.

En efecto, la problemática se examina desde la perspectiva de los PRST, quienes ya operamos bajo una alta carga regulatoria y una estricta supervisión, pero omite a los actores clave como los Proveedores de Contenidos y Aplicaciones (PCA), plataformas Over-The-Top (OTT) y carriers internacionales, entre otros, quienes operan sin cargas regulatorias y sin control por parte de MINTIC, lo que limita desde ya la eficacia de las posibles medidas que surjan de las posibles alternativas de intervención del análisis de impacto normativo (AIN) del proyecto.

En este punto, es importante que la Comisión tenga en cuenta que la experiencia internacional demuestra que las estrategias más exitosas en la lucha contra el fraude cibernético son aquellas que adoptan enfoques integrales, abordando todos los eslabones de la cadena de

valor y estableciendo responsabilidades compartidas proporcionales al nivel de participación de cada actor en el ecosistema digital.

Así las cosas, el problema central definido como “ausencia de herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto” podría ampliarse en la medida que el servicio de voz móvil y los SMS no son en la mayoría de los casos las únicas herramientas utilizadas en el fraude. De hecho, tiene mayor preponderancia al canal final de entrega de las campañas fraudulentas, que en la mayoría de los casos se originan y gestionan en plataformas digitales no reguladas.

La evidencia disponible indica que una proporción sustancial del fraude cibernético actual se origina en aplicaciones de mensajería instantánea, redes sociales, plataformas de comercio electrónico y otros servicios over-the-top (OTT) que operan sin marcos regulatorios. Estos actores utilizan posteriormente los servicios de telecomunicaciones tradicionales como mero vehículo de entrega, aprovechando la confianza que los usuarios depositan en canales formales como SMS bancarios o llamadas que aparentan provenir de entidades reconocidas.

En este contexto, la focalización exclusiva en regular más intensivamente a los PRST, que ya operamos bajo marcos normativos robustos, mientras se permite que los verdaderos originadores del fraude continúen operando sin restricciones, constituye una estrategia de eficacia limitada.

Por otro lado, hay otros actores clave como los Proveedores de Contenidos y Aplicaciones (PCA), frente a los cuales se ha interpretado que no son PRST, pero sí son asignatarios de numeración, al tráfico que generan les aplica los cargos de acceso regulados, entre otros, pero no tienen Registro TIC, no le aplican las obligaciones establecidas para PRST, como las de ciberseguridad y, por ende, no son objeto de control de MINTIC.

Sin embargo, el artículo 6 de la Ley 1341 de 2009 define las TIC de manera amplia como “el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios” que permiten diversos procesos de información y comunicación. Bajo esta definición, los PCA, al proveer aplicaciones y contenidos que utilizan recursos de identificación administrados por la CRC y al formar parte integral de la cadena de valor de las comunicaciones, se encuentran claramente dentro del ámbito de aplicación de la ley, por lo que deberían hacerse las precisiones pertinentes, en especial, las establecidas en la Resolución 3501 de 2011 frente a su definición y registro.

Lo mismo ocurre con los carriers internacionales, que en muchos casos se constituyen en los principales facilitadores del spoofing, no solo en la suplantación de identidad, sino también en la manipulación de numeración, al reescribir o enmascarar llamadas internacionales con numeración local y alterar la información de identificación de las mismas. Mientras que en países como Estados Unidos se han implementado sistemas de registro obligatorio con requisitos como garantías financieras y representación legal local para estos actores, así como la obligatoriedad de diligenciar el registro nacional Do Not Call Registry. En Colombia se permite el tráfico internacional sin ningún tipo de registro o restricciones significativas, lo que facilita la operación de redes criminales transnacionales.

Adicionalmente, la proliferación de agregadores internacionales de SMS, proveedores de servicios en la nube que alojan infraestructura fraudulenta, y plataformas digitales que operan sin una supervisión adecuada, completan un ecosistema en el que los únicos actores efectivamente regulados son, paradójicamente, aquellos sobre los cuales se pretende aumentar las cargas regulatorias.

En ese sentido, ETB considera que es fundamental ampliar la mirada regulatoria más allá de los PRST, para que las medidas regulatorias que se adopten reconozcan la complejidad del fenómeno e integren actores relevantes de la cadena de valor —incluidos los Proveedores de Contenidos y Aplicaciones (PCA), las plataformas Over-The-Top (OTT), los carriers internacionales, los agregadores y los proveedores de servicios en la nube—, y distribuyan las responsabilidades de forma proporcional al impacto y rol que cada uno desempeña en la generación, facilitación o contención del fraude.

Por lo anterior, confiamos en que proyecto sea una oportunidad para avanzar hacia un modelo de gobernanza digital más equilibrado y colaborativo y, con ello, fortalecer la cooperación entre los distintos agentes del ecosistema digital, promover soluciones sostenibles y diseñar intervenciones normativas que no solo mitiguen el fraude, sino que también fortalezcan la equidad competitiva, la innovación responsable y la protección del usuario.

I. Respuesta a la consulta

A continuación, damos respuesta a las preguntas planteadas por la Comisión en el documento de formulación del problema, con el ánimo de aportar al análisis que sustentará el desarrollo del AIN

1. Sobre el problema planteado

a) *¿El problema definido involucra todos los elementos que evidencian las dificultades generadas por el fraude cibernético mediante llamadas de voz y SMS?*

Respuesta:

La definición del problema como “ausencia de herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto” no incorpora todos los elementos necesarios para comprender plenamente las dificultades generadas por el fraude cibernético.

Esta formulación presenta limitaciones conceptuales que reducen su capacidad para orientar soluciones regulatorias eficaces y sostenibles. Si bien identifica correctamente el uso indebido de recursos de identificación —como números telefónicos y códigos cortos— por parte de actores malintencionados, restringe el análisis al canal de transmisión (voz y SMS), sin considerar las múltiples capas tecnológicas y la diversidad de actores involucrados en la gestación y ejecución de estos esquemas fraudulentos.

Como se ha señalado, esta definición omite elementos fundamentales que condicionan la eficacia de cualquier respuesta regulatoria, en particular al no contemplar:

- **Ecosistema multiplataforma:** El fraude cibernético actual no se limita a los servicios tradicionales de telecomunicaciones; más bien, estos suelen ser el canal final por el cual se materializan campañas fraudulentas que se gestan en plataformas digitales no reguladas. Aplicaciones OTT, redes sociales, plataformas de comercio electrónico y servicios de mensajería instantánea son entornos donde se origina una proporción sustancial de estos delitos.
 - **Proveedores de Contenidos y Aplicaciones (PCA):** Aunque son actores TIC conforme a la Ley 1341 de 2009, actualmente no están sujetos a mecanismos de vigilancia ni control. Esta omisión, resultado de una interpretación restrictiva, los ha eximido del registro TIC, del pago de contraprestaciones y de obligaciones frente a los usuarios, generando espacios de opacidad y facilitando escenarios de suplantación. Incluir a los PCA como sujetos del análisis permitiría avanzar en la construcción de un sistema más robusto de trazabilidad y control, conforme a su definición como actores TIC.
 - **Plataformas OTT:** A pesar de prestar servicios funcionalmente equivalentes a los tradicionales, operan fuera del ámbito regulatorio sectorial. En estos entornos digitales se originan campañas de fraude, incluyendo ingeniería social, envío de enlaces maliciosos y suplantación de entidades legítimas, sin mecanismos efectivos de trazabilidad o sanción. Incorporarlas en esquemas de colaboración sectorial podría permitir una detección más temprana de campañas y el desarrollo de mecanismos compartidos de alerta y respuesta.
- Tráfico internacional:** El tráfico entrante, especialmente el proveniente de carriers internacionales, representa una vulnerabilidad crítica, particularmente en casos de **spoofing** (suplantación de numeración). A diferencia de otros países como Estados Unidos, donde existen esquemas obligatorios de autenticación como **STIR/SHAKEN**, en Colombia no se ha implementado un sistema de registro y autenticación para estos carriers, lo que dificulta la identificación y el control de este riesgo.

En consecuencia, una reformulación más amplia y sistémica del problema contribuiría a orientar de manera más efectiva las medidas regulatorias, fortaleciendo la capacidad institucional para anticipar, prevenir y sancionar el fraude cibernético en todas sus dimensiones.

Por lo anterior, se propone esta reformulación del problema:

Ausencia de un marco regulatorio integral y de mecanismos de control efectivos sobre actores clave del ecosistema TIC, lo que impide abordar de manera sistémica la cadena del fraude cibernético. Esta situación limita la capacidad de prevenir eficazmente el contacto fraudulento a los usuarios a través de servicios de telecomunicaciones y mantiene vigentes vacíos normativos en materia de originación, trazabilidad y autenticación de las comunicaciones fraudulentas.

b) ¿Las causas presentadas son las que generan el problema definido?

Respuesta:

El documento identifica causas relacionadas con la trazabilidad limitada, la reutilización no controlada de recursos numéricos y la falta de educación del usuario. No obstante, desde una perspectiva más amplia, **se omiten las siguientes causas estructurales:**

- Ausencia de obligaciones regulatorias para PCA, pese a que utilizan recursos del sistema de numeración para contactar usuarios.
- Desregulación de los carriers internacionales que ingresan tráfico a Colombia sin ningún tipo de autenticación, control o responsabilidad.
- Inexistencia de una estrategia de trazabilidad y monitoreo integral, basada en inteligencia artificial y colaboración intersectorial.
- Omisión del rol de las OTT como canal principal de fraude y su falta de cooperación efectiva con autoridades y operadores.
- Ausencia de control por parte de MINTIC a actores como los PCA y otros, a pesar de estar inmersos en la definición del artículo 6° de la Ley 1341.

c) *¿Las consecuencias expuestas se relacionan con el problema?*

Respuesta:

Aunque las consecuencias expuestas en el documento se relacionan directamente con el problema identificado, **son insuficientes para reflejar la verdadera magnitud y complejidad de los impactos generados por el actual enfoque regulatorio fragmentado.** Dicho enfoque provoca efectos como:

- **La imposición de nuevas obligaciones a los PRST**, lo que eleva significativamente sus costos operativos.
- **El incentivo a la migración de actividades ilícitas hacia plataformas no reguladas** (PCA, OTT, carriers internacionales, etc.), debido a la ausencia de medidas de control equivalentes para estos actores.
- **El deterioro de la confianza del usuario en todo el sector de telecomunicaciones**, trasladando la carga reputacional negativa exclusivamente al PRST, al ser este el único actor visible y fiscalizado.

Ahora bien, como consecuencias adicionales se proponen:

- **Crecimiento sostenido del ecosistema del fraude**, que se adapta rápidamente a vacíos regulatorios y tecnológicos.
- **Sobrecarga de responsabilidad sobre los PRST**, que deben asumir los costos operativos, reputacionales y regulatorios sin tener control sobre el origen de muchas prácticas fraudulentas.
- **Debilitamiento de la seguridad digital nacional**, al carecer de trazabilidad y mecanismos de respuesta articulada frente al fraude transfronterizo.
- **Erosión de la confianza en el entorno digital en su conjunto**, que afecta no solo a las telecomunicaciones, sino también a servicios financieros, estatales y de comercio electrónico.

2. Respeto de los grupos de valor

a) *¿Por qué considera que existen otros grupos de valor que deben tenerse en cuenta en el desarrollo del presente proyecto regulatorio?*

Respuesta:

El enfoque adoptado en el documento de la CRC identifica adecuadamente algunos grupos de valor, como los PRST y los usuarios, **pero omite actores esenciales que no solo participan activamente en el ecosistema, sino que también son responsables, directa o indirectamente, de la gestación de escenarios de fraude.** Entre estos actores se destacan:

- **Proveedores de Contenidos y Aplicaciones (PCA)**
- **Carriers internacionales**
- **Plataformas OTT**
- **Autoridades judiciales y de protección del consumidor**, como la Fiscalía General de la Nación y la Superintendencia de Industria y Comercio (SIC), la Superintendencia Financiera, que deben integrarse activamente en un modelo de gobernanza para combatir el fraude con eficacia interinstitucional.
- **Proveedores de servicios en la nube:** AWS, Google Cloud, Microsoft Azure y similares frecuentemente alojan infraestructura técnica que soporta operaciones fraudulentas, incluyendo servidores de phishing, sistemas de gestión de campañas masivas y plataformas de procesamiento de datos robados. Su relevancia en el ecosistema del fraude es creciente y requiere atención regulatoria específica.
- **Agregadores internacionales de SMS:** Operan frecuentemente sin registro local ni supervisión efectiva, facilitando el envío masivo de mensajes fraudulentos a través de conexiones internacionales que evaden controles domésticos. Su inclusión es esencial para cerrar brechas regulatorias que facilitan operaciones irregulares transfronterizas.
- **Autoridades regulatorias internacionales:** FCC, CRTC, OFCOM y otros reguladores internacionales deben incluirse como grupos de valor para facilitar coordinación transfronteriza, intercambio de información y implementación de medidas recíprocas que aborden la naturaleza global del fraude cibernético

La inclusión de estos actores es indispensable si se pretende un abordaje comprehensivo y balanceado de la problemática, evitando que la carga de las soluciones recaiga exclusivamente sobre los PRST.

3. Sobre posibles alternativas de solución

a) *En relación con el uso indebido de la numeración de códigos cortos:*

a.1) *¿Cuáles beneficios o desafíos cree que podría tener la implementación de un registro de remitentes de mensajes cortos de texto, que haga uso de códigos alfanuméricos para su identificación por parte de los usuarios, así como de la identificación de la campaña de comercialización o publicidad que se va a adelantar por parte del remitente?*

Respuesta:

Beneficios: La implementación de la medida podría **ofrecer mejoras teóricas en la trazabilidad de las comunicaciones y la claridad para el usuario final**, facilitando la validación de campañas legítimas.

Sin embargo, estos beneficios son **marginales y condicionados**. Su efectividad depende de la adopción simultánea de un marco regulatorio integral que aborde las causas raíz del fraude, en lugar de tratar únicamente sus síntomas.

Desafíos: Los desafíos asociados a esta medida superan ampliamente sus beneficios potenciales, introduciendo riesgos significativos:

- **Asimetría de Cargas y Costos:** La propuesta concentra todas las responsabilidades de implementación, costo y supervisión en los PRST. Mientras tanto, otros actores del ecosistema quedan exentos de obligaciones, generando una distorsión de mercado y costos operativos insostenibles para los operadores.
- **Vulnerabilidad ante la Evasión:** La efectividad de la medida es inherentemente limitada, ya que el fraude puede migrar fácilmente a través de actores no regulados, como carriers internacionales y agregadores que operan fuera de la supervisión local.
- **Falla en el Marco de Verificación:** La integridad del sistema propuesto se ve comprometida desde su origen por la ausencia de un marco de verificación efectivo por parte del MINTIC para actores diferentes a los PRST. Esto crea una brecha que permitiría a actores no supervisados registrar identificadores fraudulentos sin control.
- **Creación de una Falsa Sensación de Seguridad:** En su conjunto, la medida amenaza con generar una fachada de seguridad que oculta las vulnerabilidades estructurales del sistema. Esto no solo no resuelve el problema, sino que podría agravarse al desviar la atención de las reformas integrales que sí son necesarias.
- **Implementación y Operación:** La ejecución práctica de la medida impone obstáculos técnicos y de gestión significativos, entre ellos:
 - Garantizar la **interoperabilidad técnica** entre las plataformas de múltiples actores.
 - La complejidad de crear y **gestionar un registro centralizado** de forma segura y eficiente.
 - La necesidad de una **supervisión tecnológica constante** y proactiva para detectar y prevenir la suplantación de identificadores legítimos.

a.2) ¿Cómo valora la creación de un registro de remitentes que utilice tanto numeración de códigos cortos como numeración no geográfica de servicios (Numeración E.164 del NDC 940), teniendo en cuenta la actualización de las categorías de atribución como requisito para su asignación? ¿Considera viable esta alternativa? ¿Qué pros y contras podría identificar?

Respuesta:

La propuesta es técnicamente viable. Sin embargo, su efectividad está condicionada a la **implementación simultánea de reformas regulatorias** que garanticen una aplicación equitativa y universal a TODOS los actores del ecosistema.

Ventajas Potenciales

- **Modernización y Capacidad Numérica:** La migración a la numeración E.164 con el NDC 940 ofrece una mayor disponibilidad numérica y facilita la integración con estándares internacionales de autenticación.
- **Supervisión y Trazabilidad:** Un registro centralizado y obligatorio mejoraría drásticamente la capacidad de supervisión, permitiendo auditar el uso de la numeración y trazar el origen de las comunicaciones de manera precisa.
- **Segmentación de Servicios:** Permitiría una mejor organización y clasificación de los remitentes según el tipo de servicio que prestan.

Desafíos y Limitaciones Críticas

- **Requisito de Aplicación Universal (Limitación Crítica):** La principal vulnerabilidad de la propuesta es la evasión. Si la obligación de registro no se extiende a otros actores diferentes a los PRST, los actores irregulares simplemente migrarán a estos canales no supervisados, anulando el beneficio de la medida.
- **Riesgo de Inequidad Regulatoria:** Concentrar las responsabilidades y los **altos costos de implementación** únicamente en los PRST mantiene la distribución inequitativa de cargas que define al marco regulatorio actual.
- **Complejidad Técnica y Operativa:** La implementación requiere superar desafíos de interoperabilidad, gestionar la actualización de plataformas y sistemas de entrega en todo el ecosistema y manejar la complejidad que una nueva numeración puede suponer para el usuario final.

a.3) *¿Qué efectos cree que tendría una medida regulatoria que prohíba la inclusión de enlaces o URL de cualquier tipo en el contenido de los mensajes cortos de texto? ¿Esta restricción podría mitigar riesgos de fraude? ¿Qué efectos tendría sobre el mercado de envío de SMS?*

Respuesta:

Consideramos que una prohibición total de enlaces o URLs en mensajes de texto sería una **medida contraproducente con impactos negativos desproporcionados** sobre la economía digital del país.

Si bien la intención de mitigar el *smishing* es válida, esta acción afectaría gravemente a servicios legítimos de alto valor social que son fundamentales para millones de colombianos. Sectores como la **banca digital, los trámites gubernamentales, el comercio electrónico, los servicios de salud y la logística** dependen del uso de enlaces seguros para operar de manera eficiente.

Adicionalmente, la experiencia internacional demuestra que este tipo de prohibiciones no elimina el fraude, sino que simplemente lo **desplaza hacia otros canales** menos regulados,. El fraude se adaptaría rápidamente, mientras que los servicios legítimos nacionales perderían competitividad frente a alternativas internacionales no sujetas a esta restricción.

a.4. *¿Qué implicaciones considera que tendría la prohibición de la intermediación o reventa del uso de numeración de códigos cortos por parte de los asignatarios, estableciendo la*

07-07.7-F-020-v.8

"Una vez impreso este documento, se considerará **documento no controlado**".

13/06/2023

Pág. 8

identificación exclusiva de remitentes de mensajes de texto (SMS) a través de un único código corto atribuido a una modalidad y rango numérico exclusivo? Es decir, un código corto como canal dedicado de comunicación entre un originador de mensajes de texto y sus destinatarios, atribuido en la modalidad de servicios financieros. Ejemplo: código corto: 86000; modalidad: servicios financieros; uso: parauso exclusivo por parte de la entidad financiera: Banco X

¿Considera que la cantidad disponible de numeración de códigos cortos sería suficiente para atender la demanda de estos servicios, o sería necesario migrar a otro tipo de numeración con mayor disponibilidad de números?

Respuesta:

La medida tiene una **intención positiva pero con efecto limitado**, pues busca mejorar la **trazabilidad y la responsabilidad**, al vincular inequívocamente un remitente con un número. Esto, en teoría, facilitaría la identificación de campañas fraudulentas y fortalecería la confianza del usuario en ese canal exclusivo.

Sin embargo, tiene como restricción **la insuficiencia del recurso numérico**, pues una prohibición total de la intermediación tiene como consecuencia el agotamiento inmediato del recurso, por lo que sería una medida inviable en la práctica y económicamente perjudicial.

No existen suficientes códigos cortos para asignar uno exclusivo a cada entidad que lo requiere. Por lo tanto, una prohibición generaría de inmediato un agotamiento del recurso y forzaría una **migración masiva y costosa hacia numeración E.164 (NDC 940)**. Esta migración implicaría **altos costos de actualización de sistemas y procesos operativos que afectarían desproporcionadamente a pequeñas y medianas empresas**, quienes dependen de los intermediarios para acceder a estos servicios de forma asequible.

En efecto, la medida crearía barreras de entrada significativas y reduciría la competitividad del mercado, perjudicando a los actores más pequeños.

En lugar de prohibir, proponemos **regular la intermediación bajo un modelo de corresponsabilidad**, que garantice la trazabilidad sin desarticular el ecosistema digital, es decir, se debe permitir que agregadores y otros terceros ofrezcan estos servicios, siempre y cuando cumplan con:

1. Un **registro obligatorio** ante el regulador.
2. Reglas claras que garanticen la **trazabilidad completa** de cada mensaje.
3. La **identificación inequívoca del originador** final de la campaña.

Este modelo de corresponsabilidad logra el objetivo de mejorar el control y la seguridad sin desarticular el mercado ni imponer costos prohibitivos.

a.5. ¿Qué beneficios o desafíos considera que podría tener la migración del uso de la numeración de códigos cortos a numeración E.164 no geográfica de servicios atribuida en el NDC 940 para acceder a contenidos y aplicaciones soportados en SMS y USSD, con reglas estrictas sobre exclusividad de uso y prohibición de compartición o tercerización del recurso?

Respuesta:

La solución recomendada no es la prohibición, sino **la regulación de la intermediación bajo un modelo de corresponsabilidad**, que garantice la trazabilidad sin desarticular el ecosistema digital.

Sin embargo, si la prohibición de intermediación de códigos cortos es inviable por la escasez, la migración a numeración E.164 se convierte en una consecuencia inevitable pero altamente costosa y con desafíos críticos:

- **Actualizaciones en el Core de Red:** Los operadores móviles tendrán que adaptar sus plataformas de enrutamiento, tarificación y facturación.
- **Adaptación del Ecosistema Empresarial:** Todas las empresas (bancos, comercios, etc.) tendrían que modificar sus sistemas (CRMs, plataformas de marketing, aplicaciones) para integrarse con la nueva numeración.
- **Comunicación y Educación al Usuario Final:** Acostumbrar a millones de usuarios a reconocer e interactuar con números largos (de 10 dígitos o más) en lugar de códigos cortos memorables de 5 dígitos es un reto de comunicación masiva.
- **Persistencia de la Ineficiencia del Mercado:** Si la regla de prohibición de intermediación se mantiene, el problema de fondo no se soluciona. Aunque haya números para todos, se obliga a cada empresa, sin importar su tamaño, a gestionar un recurso de telecomunicaciones directamente, perdiendo las eficiencias y la especialización que ofrecen los intermediarios.
- **Riesgo de una Implementación Disruptiva:** Una migración forzosa y rápida, producto de una prohibición mal planificada, podría causar interrupciones en servicios críticos que dependen hoy de los códigos cortos, como los servicios bancarios.

a.6. Por favor describa de manera detallada cualquier otra alternativa regulatoria que considere podría contribuir a prevenir el uso indebido de la numeración de códigos cortos y el contacto a usuarios con fines presuntamente fraudulentos mediante el envío de mensajes cortos de texto.

Respuesta:

Para abordar de manera efectiva el uso indebido de la numeración y el contacto fraudulento a través de mensajes de texto (SMS), se requiere una **estrategia regulatoria multifactorial que combine innovación tecnológica, fortalecimiento de la supervisión y corresponsabilidad de todos los actores del ecosistema**.

Podría explorarse la posibilidad de implementar firmas digitales en los SMS, sobre todo en los mensajes de texto de alta sensibilidad como transacciones bancarias, notificaciones de autoridades, para garantizar la integridad y el no repudio del mensaje de extremo a extremo. Sin embargo, esto implica altos costos de implementación y procesamiento para PCA y PRST.

b) Sobre el uso inadecuado de la numeración E.164:

b.1. ¿Qué beneficios y retos identifica en la implementación de un registro de originadores de llamadas comerciales y publicitarias, que permita su identificación por parte del usuario final mediante códigos alfanuméricos, y que se complemente con medidas como el uso exclusivo de rangos de numeración dedicadas, bloqueo de numeración no válida o extranjera sospechosa y el registro de campañas que se van a realizar por medio de llamadas de voz?

Respuesta:

Crear un registro de originadores de llamadas comerciales podría presentar beneficios significativos para el ecosistema nacional:

- **Transparencia y Empoderamiento del Usuario:** La identificación clara de la llamada mediante códigos alfanuméricos permitiría al usuario tomar decisiones informadas sobre si contestar o no, y facilitaría el bloqueo selectivo.
- **Control Regulatorio y Trazabilidad:** La asignación de rangos numéricos exclusivos para fines comerciales y el registro previo de campañas ante la CRC proporcionarían a la autoridad una alta visibilidad del uso de la numeración, facilitando una rápida identificación de irregularidades.
- **Disuasión para Actores Locales:** La simple existencia de un registro estricto disuadiría a muchas empresas locales de realizar prácticas abusivas o fraudulentas.

Sin embargo, la implementación presenta grandes retos y limitaciones que compromete su viabilidad:

- **Costos de Adaptación Tecnológica:** Los operadores y los originadores de llamadas deberán realizar grandes inversiones para adaptar sus plataformas, sistemas de marcación y redes para soportar la identificación alfanumérica y la gestión de los nuevos rangos.
- **Resistencia al Cambio:** Es previsible que algunos sectores empresariales muestren resistencia a la adopción de nuevas obligaciones de registro y reporte, lo que requerirá una gestión del cambio y una comunicación regulatoria efectiva, de esto depende la efectividad de la medida.
- **Vulnerabilidad ante el Tráfico Internacional:** La experiencia demuestra que parte del tráfico de llamadas fraudulentas con suplantación de identidad se pueden originar a través de carriers internacionales que operan con laxa o nula supervisión en Colombia. Sin un sistema robusto que obligue a estos carriers a registrarse, certificarse y responder por el tráfico que cursan, un registro nacional será fácilmente burlado.

El registro podría ser una herramienta valiosa, pero solo si se construye sobre una base sólida e involucra a los diversos actores del ecosistema.

b.2. ¿Qué percepción tiene sobre la adopción de técnicas tecnológicas de filtrado (screening) para identificar y bloquear llamadas o mensajes sospechosos? ¿Considera que esta medida debe ser complementada con acciones regulatorias sobre el uso de numeración?

Respuesta:

El enfoque regulatorio para combatir el fraude no debe centrarse en las técnicas de filtrado de contenido a cargo de los PRST. Consideramos que **el filtrado es una medida reactiva, imprecisa y con un alto potencial de efectos adversos**, por lo que debe ser considerada únicamente como una opción de último recurso y de uso limitado.

La estrategia prioritaria debe ser la **prevención en el origen**. El fraude debe ser contrarrestado antes de que el mensaje o la llamada ingrese a la red, no mientras está en tránsito. Esto se logra con un marco regulatorio robusto que garantice la identidad y la responsabilidad de quien origina la comunicación y generando la responsabilidad de todos los actores del ecosistema, a través de:

1. **Autenticación de Origen:** Asegurar criptográficamente que el remitente es quien dice ser.
2. **Registro y Supervisión de Toda la Cadena:** Incluir de manera obligatoria a PCA y carriers internacionales, eliminando el anonimato.

Recurrir al filtrado como solución principal es admitir una falla en el diseño del sistema e implica una práctica deficiente y riesgosa por las siguientes razones:

- **Alto riesgo de Falsos Positivos:** Los sistemas de filtrado, incluso los basados en IA, cometen errores. El bloqueo de comunicaciones legítimas puede interrumpir servicios esenciales como códigos de autenticación bancaria, notificaciones médicas o alertas de emergencia, generando un daño social y económico mayor al que se busca prevenir.
- **Ineficacia a Largo Plazo:** El filtrado induce a una carrera de técnicas de evasión sin fin, ya que los defraudadores adaptan rápidamente sus métodos para evadir los filtros, lo que exige una inversión continua y creciente en tecnología de monitoreo, con resultados decrecientes.
- **Potencial de Censura y Abuso:** Otorgar a los operadores o a una autoridad la capacidad de bloquear comunicaciones basándose en análisis de patrones o contenido abre la puerta a posibles abusos o a una censura gradual, erosionando la neutralidad de la red.

Entonces, el filtrado no debe ser una herramienta de uso generalizado. Su aplicación debe ser considerada únicamente **bajo circunstancias extraordinarias**, como un ataque masivo y comprobado de una fuente específica, y de manera temporal mientras se aplican soluciones en el origen, por lo que la regulación no debe promover su uso, sino **establecer barreras altas para su aplicación**, garantizando que sea siempre la última opción.

b.3. Por favor describa de manera detallada cualquier otra alternativa regulatoria que considere podría contribuir a prevenir el uso indebido de la numeración E.164 y el contacto usuarios con fines presuntamente fraudulentos mediante llamadas de voz.

Respuesta: No hay sugerencias adicionales.

c) Sobre el desconocimiento del usuario sobre privacidad y técnicas de ingeniería social:

c.1. ¿Cuál es su opinión sobre establecer obligaciones de divulgación pedagógica y de prevención en cabeza de los operadores móviles, PCA e integradores tecnológicos, complementadas con un portal de la CRC con información sobre remitentes denunciados?

Respuesta:

La divulgación pedagógica siempre es necesaria. Sin embargo, debe ser una **responsabilidad compartida y proporcional de todos los actores del ecosistema**, pues concentrar esta carga solo en algunos sería inequitativo e ineficaz.

Ahora, hay que tener en cuenta que el deber de educar y proteger al usuario no es exclusivo del sector de las telecomunicaciones. Es una responsabilidad de todo el ecosistema digital que se beneficia de la confianza del usuario. Por tanto, las **obligaciones deben ser vinculantes y extenderse a todos los actores clave**, esto es, todos los actores TIC, las entidades del sector financiero, plataformas de comercio electrónico, servicios OTT, etc.

La CRC puede dirigir las campañas frente al contenido y la periodicidad, con un enfoque especial en las poblaciones más vulnerables, como adultos mayores y comunidades en zonas rurales, donde el analfabetismo digital representa el mayor desafío.

En ese sentido, el portal de la CRC, es un complemento útil, pero su éxito depende de la alimentación de información oportuna por parte de todos los actores mencionados y de una fuerte coordinación intersectorial. Sin esta colaboración, corre el riesgo de ser un repositorio de información desactualizado e incompleto.

c.2) ¿Qué efectos cree que tendría la creación de un portal que incluya una lista negra con los recursos de identificación más denunciados ante la CRC, e identificados de oficio por esta autoridad, que sean utilizados para contactar usuarios con fines presuntamente fraudulentos?

Respuesta:

La creación de un portal que publique una “lista negra” de recursos de identificación, aunque bien intencionada, **es una medida ineficaz frente a las dinámicas actuales del fraude cibernético y riesgosa para los derechos de ciudadanos y empresas legítimas**. La experiencia ha demostrado que este tipo de mecanismos resultan operativamente complejos, fácilmente eludibles por los defraudadores y propensos a generar falsos positivos que afectan a actores legítimos.

En efecto, este tipo de mecanismo presenta tres problemas fundamentales:

1. **Ineficacia operativa:** Los defraudadores cambian constantemente los números y utilizan suplantación de identidad (spoofing), por lo que los números listados rara vez les pertenecen. El resultado sería una lista desactualizada que castiga a víctimas

inocentes, no a los criminales.

2. **Vulneración de derechos fundamentales:** Publicar números con base en denuncias, sin proceso judicial, viola el debido proceso, la presunción de inocencia, el buen nombre o habeas data y la libertad económica, afectando gravemente a personas y empresas legítimas.
3. **Falsa sensación de seguridad:** La ausencia de un número en la lista podría interpretarse erróneamente como garantía de confiabilidad, reduciendo la alerta de los usuarios y facilitando nuevos fraudes.

Por lo anterior, el enfoque regulatorio debe centrarse en **soluciones preventivas y estructurales, como la autenticación de origen, que enfrentan el problema en su raíz, en lugar de medidas reactivas y contraproducentes.**

c.3) ¿Cómo valoraría la creación de un sistema intersectorial de trazabilidad de recursos de identificación, administrado por la CRC, que centralice las PQRD9s presentadas por los usuarios y se complemente con campañas educativas conjuntas?

Respuesta:

Coincidimos en que **las campañas educativas deben fundamentarse en evidencia real sobre las modalidades de fraude.** No obstante, centralizar todas las PQR del país en una única plataforma administrada por la CRC, si su único propósito es orientar dichas campañas, resulta una medida desproporcionada, costosa y operativamente innecesaria.

Para fines pedagógicos, resulta más eficiente y proporcional un modelo de inteligencia agregada, basado en el análisis descentralizado por parte de cada sector (financiero, PCA, entre otros), con reportes periódicos a la CRC. Este enfoque permite obtener información relevante sin incurrir en los costos y riesgos de una centralización masiva de quejas individuales.

c.4) Por favor describa de manera detallada cualquier otra alternativa que considere útil para aumentar el conocimiento y empoderamiento de los usuarios frente a los riesgos del fraude cibernético por medio de servicios móviles.

Respuesta: No tenemos sugerencias adicionales.

4. Revisión del régimen de recursos de identificación

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

Respuesta:

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

Respuesta:

La gestión eficiente de los recursos de identificación exige un sistema automatizado y confiable por parte de la CRC. No obstante, el mapa de numeración (SIGRI) presenta actualmente múltiples inconsistencias que dificultan la trazabilidad y el control.

Debe tenerse en cuenta que los PRST no gestionan ni controlan el contenido transmitido a través de los recursos de identificación asignados. El uso indebido de la numeración —como ocurre en casos de fraude por suplantación o mediante intermediarios no autorizados— suele ser cometido por terceros y escapa tanto al control de los operadores como al del propio regulador.

Por tanto, para mejorar la administración de estos recursos, sugerimos:

1. **Automatización del proceso de asignación y recuperación:** Incluir validaciones automáticas del uso previsto, trazabilidad de los bloques.
2. **Fortalecimiento del control regulatorio sobre terceros:** Las medidas de supervisión y depuración deben orientarse hacia los usuarios finales, intermediarios no autorizados o quienes realmente incurren en usos indebidos, sin trasladar dicha responsabilidad a los PRST, que no tienen injerencia sobre esos comportamientos.

Estas acciones permitirían optimizar los procedimientos sin trasladar cargas indebidas a los operadores y atendiendo la verdadera raíz del problema: el uso fraudulento por parte de actores externos al ecosistema regulado.

Confiamos en que los comentarios presentados en este documento constituyan un aporte valioso para el fortalecimiento del proyecto regulatorio. Agradecemos la oportunidad de participar en esta consulta y reiteramos nuestra disposición para seguir colaborando en las siguientes etapas del proceso.

Cordialmente,



LUDWIG CHRISTIAN CLAUSEN NAVARRO
Gerente Asuntos Públicos, Regulación y Sostenibilidad

Elaboró: Tatiana Sedano Cardozo – Gerencia Asuntos Públicos, Regulación y Sostenibilidad