

Bogotá D.C., 28 de julio de 2025

Doctora

CLAUDIA XIMENA BUSTAMANTE

Directora Ejecutiva

Comisión de Regulación de Comunicaciones

Correos: atencioncliente@crcom.gov.co; medidasantifraude@crcom.gov.co

Bogotá, D.C

Asunto: Respuesta a la Consulta Pública realizada por la CRC en el marco del proyecto regulatorio denominado *“Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles”*

Respetada Doctora Bustamante:

DIEGO DAMIAN VALDIVIESO PIFNILLA mayor de edad, identificado con la cédula de ciudadanía **80.876.160** expedida en Bogotá, obrando en calidad de Apoderado General de **HABLAME COLOMBIA S.A. E.S.P.** sociedad identificada con NIT 900.994.857-4, me permito dar respuesta a la CONSULTA PÚBLICA socializada por la CRC en el marco del proyecto regulatorio denominado *“Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles”*.

Desde HABLAME COLOMBIA S.A. ESP valoramos este tipo de iniciativas regulatorias que promueven la construcción conjunta de soluciones orientadas a enfrentar el creciente impacto del fraude cibernético, el cual está generando importantes pérdidas financieras y afectaciones reputacionales a quienes trabajamos con transparencia, dentro del marco legal y en pro del desarrollo del país.

Desde HABLAME hemos propuesto ante la comisión de regulación de Comunicaciones –CRC (Sandbox Regulatorio) el proyecto “Modernización y Regulación de los Códigos Alfanuméricos: Propuesta de Seguridad y Administración Centralizada para Colombia”, una iniciativa innovadora que busca implementar un sistema de autenticación y trazabilidad para mensajes SMS mediante el uso de códigos alfanuméricos verificados, como “BANCOCO123” o “HBLMOVIL333”. Esta solución surge ante la creciente problemática del smishing y el uso fraudulento de códigos cortos, especialmente en sectores como la banca, salud y servicios públicos. El proyecto plantea crear un Registro Nacional de Códigos Alfanuméricos,

administrado inicialmente por la CRC, con validación técnica previa, interoperabilidad entre operadores y acceso público a través de plataformas web y API. Esto permitiría a los usuarios identificar claramente al remitente de cada mensaje y la campaña asociada, reduciendo la suplantación y aumentando la confianza en el canal SMS.

La propuesta se desarrolla en el marco del Sandbox Regulatorio de la CRC, La propuesta *“Modernización y Regulación de los Códigos Alfanuméricos: Propuesta de Seguridad y Administración Centralizada para Colombia”* también promueve la inclusión digital en zonas rurales, donde los usuarios dependen del SMS como principal canal de interacción con bancos y entidades del Estado. Con esta iniciativa, en HABLAME buscamos transformar estructuralmente la gestión de la numeración alfanumérica, modernizar el ecosistema de mensajería y aportar una solución escalable y regulada que proteja los derechos de los usuarios, fortalezca la seguridad digital y optimice la supervisión del canal por parte de la CRC.

PREGUNTAS Y RESPUESTAS DOCUMENTO DE IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES

“1. Sobre el problema planteado

a) ¿Por qué considera que el problema definido en este documento involucra todos los elementos que evidencian las dificultades generadas por la comisión de fraude cibernético mediante la provisión de los servicios tradicionales de llamadas de voz y SMS? Dado el caso que considere que el problema definido no involucra todos los elementos necesarios, por favor justifique sus motivos, aporte evidencia al respecto y proponga un problema alternativo con sus respectivas causas y consecuencias.”

RESPUESTA:

Consideramos que el problema definido por la CRC *“Ausencia de herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto”* recoge adecuadamente los elementos esenciales que evidencian las dificultades actuales. No obstante, desde HABLAME sugerimos profundizar en dos aspectos adicionales críticos que aún no se tuvieron en cuenta dentro del árbol del problema.

1. Uso de rutas entre los PRSTM y los PCA e IT inseguras vía VPN que se anuncian en internet público, por lo que proponemos que se incluya dentro de las causas del problema la falta de exigencia de enlaces dedicados punto a punto entre los PCA e IT y los PRTSM, que permitan auditar la trazabilidad y garanticen la seguridad

extremo a extremo, tal como lo presentamos en el documento presentado ante la CRC con fecha 3 de julio de 2025 y radicado 2025814725, el cual se adjunta a la presente.

2. Se propone establecer un marco regulatorio que obligue a la cooperación activa, continua, transparente y eficiente entre los actores del ecosistema y evitar fomentar la desvinculación entre PRSTM e Integradores Tecnológicos, esto con el objetivo de construir una capacidad institucional y técnica coordinada para enfrentar los desafíos del fraude digital. Situación que están aprovechando los cibernautas quienes cada día están más fortalecidos mientras los PRSTM y las entidades de vigilancia y control atacan a los PCA e IT.

En resumen, consideramos que el problema central está bien enfocado, pero podría fortalecerse si incluye de forma explícita:

- La falta de obligatoriedad de enlaces dedicados punto a punto entre PCA y PRSTM, lo que expone al ecosistema a rutas no auditables y vulnerables.
- La falta de Cooperación entre los diferentes actores de los contratos de acceso, quienes asumen una posición desafiante y estigmatizante contra los PCA e IT, en lugar de asumir una posición de trabajo mancomunado en beneficio de los usuarios.

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

RESPUESTA:

Consideramos que las causas identificadas por la CRC en el documento son pertinentes y reflejan adecuadamente varias de las fallas estructurales que facilitan la comisión del fraude cibernético mediante los servicios de llamadas de voz y SMS. En especial, compartimos el diagnóstico que vincula la falta de trazabilidad, la deficiente gestión de recursos de identificación, y la ausencia de medidas de control y supervisión técnica efectiva, como causas directas del problema.

Sobre la primera causa:

No estamos de acuerdo con la causa que indica que "las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso", como si esto fuera el origen del problema. Por el contrario, consideramos que la raíz del problema es que la CRC no tiene un entendimiento actualizado y profundo del funcionamiento real del mercado de mensajería A2P ni de la cadena de valor involucrada en los servicios de SMS, particularmente en lo relacionado con los roles de los Proveedores de Contenidos y Aplicaciones (PCA), los Integradores Tecnológicos y los operadores internacionales.

El enfoque regulatorio actual desconoce dinámicas clave del ecosistema, como:

- La participación de múltiples actores fuera del control directo del asignatario del recurso.
- La complejidad de la trazabilidad cuando intervienen integradores internacionales o rutas de tránsito.
- La necesidad de establecer estándares técnicos y contractuales que protejan el recurso en toda la cadena.

Mientras la CRC no evolucione su comprensión del mercado y no se actualice en línea con las tendencias globales en trazabilidad, autenticación, enrutamiento responsable y filtrado de tráfico, no será posible garantizar un uso eficiente del recurso ni generar condiciones adecuadas que respalden a los actores responsables como los PCA e integradores serios.

En ese sentido, más que un problema de "uso eficiente", lo que se requiere es una regulación alineada con la realidad operativa, tecnológica y comercial actual del ecosistema de SMS, que permita implementar mecanismos efectivos de seguridad, control y prevención, sin castigar o entorpecer la operación de quienes sí cumplen.

Sobre la segunda causa:

No estamos de acuerdo con la afirmación según la cual "las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes", ya que desconoce que actualmente tanto los Proveedores de Redes y Servicios de Telecomunicaciones (PRST), como los Proveedores de Contenidos y Aplicaciones (PCA) e Integradores Tecnológicos, cuentan con diversas herramientas técnicas, contractuales y operativas para mitigar el fraude en el ecosistema de mensajería.

Los actores responsables implementan controles de acceso, validaciones de origen, filtros de contenido, trazabilidad, monitoreo automatizado, protocolos de reporte, auditorías periódicas y mecanismos de bloqueo preventivo. Sin embargo, es importante entender que el fraude, particularmente el asociado a ingeniería social mediante SMS, es un fenómeno que evoluciona constantemente, adaptándose a nuevas medidas de defensa y explotando cualquier vulnerabilidad en la cadena, incluyendo incluso al propio usuario.

Pretender que los agentes del mercado puedan eliminar por completo un delito global, que existe desde antes de la telefonía móvil y que ha mutado desde el correo electrónico hasta el canal SMS, resulta ingenuo e irrealista. El fraude no se erradica, se administra, se reduce, se contiene. Ninguna regulación en el mundo ha podido erradicarlo por completo, ni siquiera en los entornos más controlados.

Por lo tanto, la CRC no puede formular un diagnóstico que parte de una expectativa desproporcionada, como si fuera posible construir un entorno libre de fraude. La regulación debe enfocarse en fortalecer capacidades, fomentar la colaboración entre actores, incentivar buenas prácticas, y permitir la innovación en esquemas de defensa, pero con los pies en la tierra: el fraude muta y seguirá existiendo. Lo razonable es minimizar su impacto.

Sobre la tercera causa:

Estamos completamente de acuerdo con la causa “Desconocimiento de los usuarios sobre privacidad de la información y la obtención de datos personales con fines fraudulentos”. De hecho, consideramos que esta es la causa más relevante y estructural del problema.

La mayoría de los fraudes que se cometen a través de SMS no ocurren por fallas técnicas en las redes ni por negligencia de los operadores o asignatarios, sino porque el usuario final aún no está suficientemente formado para identificar mensajes maliciosos o sospechosos, ni comprende los riesgos de entregar su información personal a través de este canal.

Así como en su momento los usuarios de correo electrónico aprendieron a través de campañas de concientización, experiencia y repetición a reconocer correos fraudulentos, enlaces engañosos y remitentes sospechosos, lo mismo debe ocurrir en el entorno móvil. Los usuarios deben evolucionar su conocimiento y desarrollar criterios para identificar mensajes que no provienen de fuentes confiables, que contienen solicitudes inusuales o enlaces acortados sin contexto.

Mientras el usuario no sea un actor activo en la protección de su información, cualquier medida técnica será siempre parcial. No es viable construir un ecosistema seguro si el eslabón más importante, el destinatario, no tiene herramientas para interpretar y filtrar lo que recibe.

Por tanto, más que enfocarse únicamente en endurecer la regulación sobre los actores del mercado, la CRC debe liderar, impulsar y coordinar campañas nacionales de educación digital y alfabetización en ciberseguridad orientadas al usuario final, que incluyan a operadores, entidades financieras, comercios y sector público. Sin usuarios informados, no hay ecosistema seguro posible.

“c. Frente al problema planteado, ¿por qué considera que las consecuencias expuestas en el presente documento tienen relación directa con la materialización del problema? En caso de considerar lo contrario, indicar las razones por las cuales no está de acuerdo con la relación que se establece entre el problema definido y las consecuencias descritas, y proponga las consecuencias que considere pertinentes.”

RESPUESTA:

Consideramos que las consecuencias descritas en el documento tienen una relación directa, clara y bien sustentada con el problema identificado por la CRC

“2. Respecto de los grupos de valor:

a. ¿Por qué considera que existen otros grupos de valor que deben tenerse en cuenta en el desarrollo del presente proyecto regulatorio? Por favor indíquelos, justificando la razón que tendría para incluirlos. En caso de considerar que se encuentran incluidos todos los grupos de valor, justifique también su respuesta.”

RESPUESTA:

Consideramos que deben incluirse expresamente como grupo de valor a los Proveedores de Servicios de Internet (ISP), dado que tienen una responsabilidad directa en la prevención del acceso a contenidos maliciosos, ya que es a través de su infraestructura que se materializa el ingreso de los usuarios a enlaces fraudulentos asociados a campañas de phishing, smishing o suplantación de identidad. Su rol es crucial, pues tienen la capacidad técnica y legal para bloquear de forma oportuna y efectiva las URLs identificadas como maliciosas, mitigando así los efectos de mensajes SMS que redirigen a sitios inseguros. Esta obligación se fundamenta no solo en su deber de diligencia frente a la prestación del servicio, sino también en el principio de corresponsabilidad en el ecosistema digital, donde todos los actores, incluidos los ISP deben adoptar medidas concretas para proteger la seguridad y confianza de los usuarios. Incluir a los ISP en el diseño regulatorio permite cerrar el ciclo técnico-preventivo y fortalecer la capacidad de respuesta frente a amenazas digitales que circulan mediante el canal SMS.

Policía Nacional y Fiscalía General de la Nación: Estas autoridades deben ser actores estratégicos en la identificación, investigación y judicialización de estructuras criminales que operan a través de servicios móviles. La experiencia acumulada por sus unidades especializadas en cibercrimen y delitos económicos es clave para alimentar el diseño regulatorio con evidencia, alertas tempranas y mecanismos de respuesta ante nuevas modalidades de fraude.

Instituto Nacional Penitenciario y Carcelario – INPEC: La evidencia señala que muchas llamadas extorsivas y mensajes de texto fraudulentos se originan desde centros carcelarios, haciendo uso de equipos y líneas móviles ilegales. La inclusión del INPEC como actor regulatorio permitirá articular medidas como el uso de inhibidores de señal, el control y bloqueo selectivo de dispositivos, y la identificación de patrones de actividad sospechosa.

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

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

El uso de identificadores alfanuméricos puede generar una mayor percepción de confianza en el usuario final, especialmente cuando el nombre visible del remitente coincide con una entidad reconocida como un banco, una entidad gubernamental o una marca de alto reconocimiento. En ese contexto, el usuario podría interpretar que el mensaje proviene de una fuente legítima y tomarlo con mayor seriedad.

Sin embargo, esta medida tiene un alcance limitado y no constituye una solución estructural al problema del fraude por SMS. En primer lugar, los códigos alfanuméricos solo podrán ser utilizados por un subconjunto reducido de remitentes (grandes superficies, entidades financieras, etc.), pero el ecosistema seguirá coexistiendo con códigos cortos numéricos tradicionales, que continuarán siendo explotados por los actores fraudulentos para engañar al usuario.

Por lo tanto, aunque el uso de alfanuméricos puede ser útil para generar confianza en mensajes específicos de algunos remitentes autorizados, no reduce ni elimina la cantidad de mensajes fraudulentos que seguirán llegando desde numeraciones numéricas, que es donde realmente se concentra el riesgo para el usuario.

“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:

Con respecto a la propuesta de creación de un registro de remitentes que utilice cada uno de los recursos de numeración corta o larga existentes en el país, consideramos que dicha iniciativa no es viable ni técnica ni operativamente, por las siguientes razones:

1. Desconocimiento por parte de la CRC de la cadena de valor real del ecosistema de mensajería A2P. El modelo actual involucra múltiples actores: operadores locales e internacionales, integradores, plataformas globales de distribución y proveedores de contenido (PCA), que pueden variar según el país de origen, el tipo de contenido, el canal, e incluso el horario o la ruta de menor costo. Pretender registrar el 100% de los remitentes que usan una numeración, cuando muchos de ellos están fuera del territorio nacional o no tienen relación directa con el asignatario del recurso, es desconocer la complejidad operativa y técnica del sistema.

2. Es imposible garantizar una trazabilidad total del origen de cada remitente: Los identificadores alfanuméricos o numéricos son configurados por múltiples plataformas, muchas veces de manera automática o rotativa, y no siempre es viable asociar de forma única un remitente con un código corto o largo específico. Esto genera falsos positivos y hace inviable un esquema rígido de registro.
3. Las demoras administrativas por parte de la CRC y de los operadores en la asignación y habilitación de la numeración de SMS afectarían gravemente la viabilidad comercial del ecosistema: En la práctica, tanto la habilitación de numeraciones como la implementación de nuevos remitentes enfrenta tiempos de espera mucho más largos que los contemplados en la regulación vigente. Esto afecta la agilidad necesaria para operar campañas dinámicas o de corta duración, como las de seguridad bancaria, notificaciones legales o campañas de interés público. Con un sistema de registro obligatorio previo, muchas campañas quedarían imposibilitadas de salir a tiempo, afectando a usuarios y a las empresas que prestan estos servicios.

“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:

Frente a la consulta relacionada con los efectos que tendría una eventual prohibición del uso de URLs en los mensajes de texto, manifestamos nuestra total oposición a esta medida, por considerarla desproporcionada, ineficaz en el mediano plazo y altamente perjudicial para el ecosistema de telecomunicaciones.

1. Aunque la restricción podría contener parte del fraude, tendría un impacto devastador sobre el mercado legítimo de mensajería SMS. Hoy en día, las URLs son un componente esencial de miles de servicios críticos: autenticación en dos pasos, recuperación de contraseñas, notificaciones de entrega, facturación, turnos médicos, acceso a promociones, trámites bancarios, y más. Eliminar las URLs afectaría de forma directa la utilidad del canal SMS como medio de comunicación transaccional y comercial, desincentivando su uso.
2. La medida afectaría los ingresos de todos los actores del ecosistema de telecomunicaciones, incluyendo operadores móviles, proveedores de contenido, integradores tecnológicos y plataformas de mensajería, lo cual

tendría consecuencias directas en el empleo, la inversión y la sostenibilidad del sector.

3. Según los propios datos del sector, el volumen de mensajes con contenido presuntamente fraudulento no supera el 1% del total de SMS que circulan en el país. Por lo tanto, esta medida perjudicaría gravemente al 99% restante de mensajes legítimos y útiles para millones de ciudadanos y empresas, generando un desequilibrio regulatorio inaceptable.
4. Eliminar las URLs no eliminaría el fraude, sino que lo trasladaría a otros canales, como llamadas de voz, enlaces vía redes sociales o mensajes ofuscados que terminen afectando aún más la trazabilidad.

Por lo anterior, reiteramos que nos oponemos rotundamente a la implementación de esta medida, y recomendamos enfocar los esfuerzos en estrategias de control de tráfico, análisis de patrones, trazabilidad técnica, educación del usuario y colaboración entre actores, sin afectar la operatividad ni la legitimidad del canal SMS como herramienta clave en la economía digital.

“a.4. ¿Qué implicaciones considera que tendría la prohibición de la intermediación o reventa del uso de numeración de códigos cortos por parte de los asignatarios, estableciendo la identificación exclusiva de remitentes de mensajes de texto (SMS) a través de un único código corto atribuido a una modalidad y rango numérico exclusivo? Es decir, un código corto como canal dedicado de comunicación entre un originador de mensajes de texto y sus destinatarios, atribuido en la modalidad de servicios financieros. Ejemplo: código corto: 86000; modalidad: servicios financieros; uso: para uso exclusivo por parte de la entidad financiera: Banco X ¿Considera que la cantidad disponible de numeración de códigos cortos sería suficiente para atender la demanda de estos servicios, o sería necesario migrar a otro tipo de numeración con mayor disponibilidad de números?”

RESPUESTA:

En relación con la consulta planteada sobre las implicaciones que tendría la prohibición de la intermediación o reventa de códigos cortos por parte de los integradores tecnológicos, manifestamos que esta medida sería completamente inviable tanto técnica como económicamente y generaría un retroceso en el desarrollo del ecosistema de mensajería A2P en el país.

1. La CRC subestima la complejidad operativa y los tiempos reales involucrados en la asignación y habilitación de un código corto. Obtener un código corto directamente ante la CRC implica un proceso excesivamente burocrático, lento

y engorroso, con múltiples trámites administrativos, análisis de documentación, demoras no controlables y una carga operativa que muchas empresas finales no están en capacidad de asumir. Esta es precisamente la razón por la cual existen los integradores tecnológicos: para simplificar esa complejidad y facilitar el acceso al servicio.

2. La habilitación del código ante los operadores es, en la práctica, una de las mayores barreras del modelo. Aunque la Resolución CRC 5050 establece un plazo de 20 días para dicha habilitación, la realidad del mercado es que este proceso puede tomar 90 días o más. Los PRSTM imponen trabas técnicas, económicas y contractuales, como exigencias de garantías, proyecciones de tráfico poco realistas, evaluaciones de conveniencia e incluso excusas arbitrarias que no están contempladas en la regulación.
3. Esta medida destruiría la viabilidad del modelo comercial actual. Si se prohíbe la intermediación, los integradores no podríamos salir a ofrecer servicios a un cliente sin decirle que tendremos que esperar 7 u 8 meses para operar, sumando el tiempo de trámite ante la CRC más el de los PRSTM. Esto es completamente descabellado, anticompetitivo y desconectado de la realidad empresarial.
4. La medida desconoce la función esencial que cumplen los integradores tecnológicos: dinamizar el mercado, abrirlo a nuevos actores, facilitar el acceso y permitir que empresas medianas o pequeñas puedan usar el canal SMS sin enfrentar barreras regulatorias y operativas desproporcionadas.

En conclusión, nos oponemos rotundamente a cualquier iniciativa que pretenda prohibir o restringir la figura de intermediación de códigos cortos. Esta medida no solo afectaría gravemente a los integradores tecnológicos, sino que pondría en riesgo la sostenibilidad del ecosistema de mensajería A2P en Colombia y limitaría el acceso de cientos de empresas a una herramienta de comunicación legítima, regulada y útil para los usuarios.

“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:

Respecto a la consulta sobre los beneficios o desafíos de una eventual migración del envío de mensajes de texto desde códigos cortos hacia códigos largos,

consideramos que esta propuesta no aporta valor alguno en la mitigación del problema de fraude cibernético expuesto en el documento y, por el contrario, introduce complejidad innecesaria sin solución estructural.

1. La longitud del número de origen (ya sea corto o largo) no tiene relación directa con la comisión o prevención del fraude. En la práctica, que el número A tenga 4, 6, 11 o 15 dígitos no cambia en absoluto la dinámica ni el riesgo del fraude. Los usuarios promedio no tienen cómo verificar el origen del número por su longitud, ni asocian automáticamente un número largo con una fuente legítima o fraudulenta. El fraude se basa en ingeniería social, no en formato de numeración.
2. Esta migración supondría altos costos técnicos, comerciales y contractuales para todos los actores de la cadena, sin ninguna ganancia real en términos de seguridad o trazabilidad. Cambiar infraestructuras, integraciones y modelos de negocio basados en códigos cortos que permiten diferenciación, branding y fácil recordación, por números largos, afectaría la experiencia del usuario y la efectividad de las campañas legítimas.
3. La propuesta se aleja del foco real del problema, que es la ausencia de mecanismos robustos de validación, control, trazabilidad y educación al usuario. Migrar a numeración larga no impide que se sigan enviando mensajes maliciosos; simplemente cambia el canal de origen. Es una solución cosmética, no estructural.

Por lo tanto, consideramos que esta iniciativa no tiene beneficios reales frente al objetivo del proyecto regulatorio, y sí implicaría múltiples desafíos técnicos y comerciales para un sector que ya opera bajo condiciones complejas. En lugar de enfocarse en el formato del número emisor, los esfuerzos regulatorios deberían centrarse en controles inteligentes, detección de patrones anómalos, validación de remitentes y articulación sectorial.

“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:

Proponemos que la CRC faculte a COLCERT, como entidad independiente y neutral, para la creación, operación y administración de una base de datos nacional y en tiempo real que centralice los reportes y patrones de contenido fraudulento, especialmente relacionados con URLs maliciosas utilizadas en campañas de smishing y fraudes electrónicos.

Esta base de datos funcionaría de forma análoga a sistemas ya existentes como el Registro de Números Excluidos (RNE) o la Base de Datos Administrativa de Portabilidad Numérica, y tendría como finalidad:

- Consolidar reportes técnicos y operativos de los operadores, PCA e integradores sobre URLs detectadas como maliciosas.
- Permitir la sincronización en tiempo real con todos los agentes de la cadena de valor para aplicar bloqueos inmediatos de mensajes con contenido sospechoso.
- Generar alertas y reportes automáticos cuando se detecten patrones de fraude emergente, utilizando incluso mecanismos de inteligencia artificial o análisis heurístico.
- Proveer trazabilidad y respaldo técnico ante eventuales solicitudes de las autoridades o usuarios afectados.

Esta herramienta permitiría responder de forma ágil y colaborativa a la evolución constante de los métodos de fraude, reduciendo sustancialmente el tiempo de exposición de los usuarios ante amenazas activas. Al centralizar el conocimiento en una fuente confiable y sincronizable, se mejora la eficiencia de los bloqueos preventivos, se evita la duplicidad de esfuerzos y se estandariza la respuesta ante incidentes.

Reiteramos que ninguna medida técnica aislada podrá resolver un fenómeno tan dinámico como el fraude por ingeniería social. Por ello, una base como la que proponemos permitiría consolidar capacidades colectivas del sector, elevando los niveles de protección sin interferir con la operación legítima del ecosistema.

“b. Respecto del 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:

En respuesta a la consulta sobre la creación de un registro centralizado de originadores de llamadas internacionales comerciales y publicitarias, así como medidas como el uso exclusivo de rangos de numeración válidos, el bloqueo de

numeración sospechosa o inválida, y el registro previo de campañas de voz, manifestamos lo siguiente:

1. Sobre la creación de un registro centralizado de originadores: Consideramos esta medida totalmente ineficaz e inoficiosa. En la práctica, los usuarios no van a consultar en tiempo real si una llamada entrante se encuentra registrada o no. Es irreal pensar que un ciudadano, antes de contestar una llamada, va a ingresar a una plataforma web para verificar el número. Esto no se traduce en protección efectiva, ni previene el contacto fraudulento, y genera una falsa sensación de control que no se materializa en la experiencia del usuario.
Adicionalmente, la mayoría de estas llamadas comerciales son realizadas por call centers o BPO, un sector altamente desarrollado en Colombia. En estos casos, el número visible al usuario no corresponde a la entidad final (por ejemplo, el banco), sino al call center que ejecuta la campaña. Por lo tanto, el registro solo mostraría una larga lista de nombres de empresas operadoras de call center que no le dicen nada al usuario final, y que no aportan valor para la trazabilidad efectiva o la confianza del consumidor.
2. Sobre el bloqueo de numeración inválida o extranjera sospechosa: Estamos de acuerdo con esta medida siempre que se respete y mantenga la estructura de numeración bajo el formato E.164. Esto garantiza coherencia técnica, interoperabilidad internacional, y evita la entrega de llamadas con números truncados, falsificados o con formatos atípicos que dificultan la identificación del origen real. Este tipo de bloqueos sí puede aportar a la mitigación del fraude y la protección al usuario.
3. Sobre el registro previo de campañas de voz: Esta medida también nos parece inoficiosa y operativamente inviable. La intención de registrar cada campaña de voz antes de ejecutarse no solo resulta en una traba adicional innecesaria para el funcionamiento del ecosistema, sino que genera una carga administrativa injustificada para los actores del mercado, incluidas entidades legítimas como bancos, aseguradoras, operadores de recaudo o casas de cobranza. Tampoco tiene impacto real en el usuario, quien no tiene cómo anticipar si la llamada que recibe corresponde a una campaña registrada. En resumen, es más carga, más burocracia y nulo efecto práctico.

“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

En relación con la consulta de la CRC sobre la percepción del uso de técnicas tecnológicas de filtrado (“screening”) para la identificación y bloqueo de llamadas o mensajes presuntamente fraudulentos, expresamos una alta preocupación y escepticismo frente a su implementación, debido a los riesgos significativos que esta práctica implica para los usuarios finales y la operación de servicios legítimos.

En nuestra experiencia concreta en Háblame Colombia, y en coordinación con otros Proveedores de Redes y Servicios de Telecomunicaciones (PRSTs) del país, se han realizado pruebas controladas de este tipo de tecnologías, y los resultados han demostrado que, si bien se logra filtrar una fracción mínima del contenido efectivamente fraudulento, el impacto negativo sobre los mensajes legítimos es mucho mayor.

En la práctica, estos filtros tienden a:

Generar altos niveles de falsos positivos, bloqueando mensajes y llamadas válidas, solicitadas por el usuario o de origen legítimo (por ejemplo, notificaciones bancarias, claves OTP, recordatorios médicos, gestiones de cobranza, etc.).

Afectar gravemente al usuario final, quien termina sin recibir una comunicación que está esperando y que puede ser crítica para su vida cotidiana.

Reducir la confiabilidad del canal SMS o de llamadas, desincentivando su uso por parte de empresas y generando frustración en los usuarios.

Por lo tanto, estas tecnologías de filtrado no logran contener el fraude de forma efectiva (solo un porcentaje muy bajo del total), y sí introducen graves interrupciones en la entrega de contenidos legítimos. En ese sentido, el remedio termina siendo peor

“En relación con el desconocimiento de los usuarios sobre privacidad de la información 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

Frente a la consulta relacionada con la pertinencia de establecer una obligación de divulgación pedagógica orientada a la prevención del fraude, manifestamos que sí consideramos apropiado y necesario que exista dicha obligación para todos los actores que intervienen en la cadena de valor del servicio de mensajería y llamadas: operadores móviles, proveedores de contenido (PCAs) e integradores tecnológicos.

Sin embargo, esta obligación debe estar claramente estructurada y diferenciada en cuanto a responsabilidades, medios de divulgación y costos asociados, de la siguiente manera:

1. Responsabilidad de cada actor:

Cada actor (operador, PCA, integrador) debe asumir directamente la divulgación en sus propios canales digitales, tales como:

- Sitios web corporativos,
- Redes sociales oficiales
- Canales de atención virtual.

Los costos de estas acciones deberán ser asumidos directamente por cada actor.

2. Envío de mensajes de texto educativos coordinados entre los PRST, PCA e IT: También es necesario que se permita el envío de mensajes de texto con contenido pedagógico para la prevención del fraude, dirigidos a los usuarios. No obstante, estos mensajes deberían ser exentos del pago de cargos de acceso a los PRST, ya que son campañas de beneficio público tanto para los usuarios PRST como para los PCA e IT y su finalidad no es comercial sino educativa.

3. Liderazgo institucional por parte de la CRC: Consideramos que la cabeza de toda esta estrategia educativa debe ser la Comisión de Regulación de Comunicaciones (CRC). Es esta entidad la que debe establecer los lineamientos generales, mensajes unificados, criterios técnicos y mecanismos de medición del impacto. Además, las campañas masivas en medios de comunicación tradicionales (televisión, radio, prensa, medios digitales) deben estar lideradas directamente por la CRC, y los costos de dichas campañas deben ser asumidos con recursos públicos de esta entidad, dado que su alcance es institucional y de seguridad nacional, toda vez que hace parte natural de las funciones de la CRC asignadas en el artículo 22 de la ley 1341 de 2009

“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:

Frente a la propuesta de crear un portal público que contenga una lista negra con los recursos de identificación más denunciados ante la CRC, consideramos que la efectividad de esta medida sería nula o, en el mejor de los casos, extremadamente limitada.

1. **Baja utilidad práctica para el usuario final:** La gran mayoría de usuarios no va a consultar de forma activa una lista negra antes de decidir si interactúa con un mensaje o responde una llamada. Este tipo de herramientas no se integran naturalmente en el comportamiento cotidiano de los ciudadanos, y no representan una barrera efectiva contra el fraude.
2. **Riesgo de confusión y daño a contenidos legítimos:** Muchos de los recursos de identificación (como códigos cortos, alfanuméricos o números largos) que podrían llegar a ser incluidos en esa lista son utilizados mayoritariamente para enviar contenidos legítimos y esperados por los usuarios. Por tanto, incluirlos en una lista negra puede generar falsas percepciones, afectar injustamente a actores legales y perjudicar la entrega de comunicaciones útiles para el usuario.
3. **Desviación de esfuerzos institucionales:** En lugar de invertir recursos en el desarrollo y mantenimiento de una plataforma con baja o nula efectividad, la CRC debería enfocar sus esfuerzos en campañas de pedagogía y educación digital. Estas campañas sí tienen un impacto real y sostenible al enseñar a los usuarios a identificar posibles fraudes, a reconocer patrones comunes en los mensajes fraudulentos y a tomar decisiones informadas.

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

RESPUESTA:

Frente a la consulta sobre la viabilidad y conveniencia de implementar un sistema intersectorial de trazabilidad de recursos de identificación, administrado por la CRC y que centralice las PQRs presentadas por los usuarios, manifestamos con total claridad que esta propuesta nos parece profundamente equivocada, riesgosa e inoficiosa.

1. Grave afectación a la privacidad y confidencialidad de la información: La creación de un sistema de este tipo representa un riesgo directo para la seguridad, privacidad y confidencialidad de la información de los usuarios, la cual está protegida y supervisada por la Superintendencia de Industria y Comercio (SIC) en su rol de autoridad nacional de protección de datos personales.

Centralizar PQRs asociadas a recursos de identificación en una única base gestionada por la CRC genera riesgos de fuga, mal manejo o uso indebido de información sensible, lo cual puede constituir una vulneración al régimen de habeas data y a la Ley 1581 de 2012.

2. Falta de valor práctico del sistema propuesto: El hecho de que un recurso de identificación tenga múltiples PQRs asociadas no implica, por sí solo, que esté vinculado a prácticas fraudulentas o ilegales. Muchos de estos reportes pueden ser falsos positivos, quejas genéricas, errores de usuarios o desacuerdos con comunicaciones legítimas. Por lo tanto, acumular PQRs sin validación de fondo carece de valor probatorio, genera estigmatización de canales legítimos y no contribuye a una trazabilidad real ni útil.
3. Falta de finalidad clara y duplicación de funciones: La propuesta no resuelve ninguna necesidad concreta del sector ni del usuario. No existe una justificación técnica ni operativa para implementar un sistema tan complejo, y en todo caso, ya existen mecanismos formales para la gestión de PQRs ante los operadores, PCAs y la SIC.

Crear un sistema adicional en la CRC implica duplicidad de funciones, mayores cargas administrativas y más burocracia, sin ningún impacto positivo comprobable.

“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:

1. Campañas permanentes de educación digital lideradas por la CRC
Formato: Audiovisuales, gráficos, podcast, videos cortos (tipo reels/TikTok), infografías sencillas.

Canales: TV nacional, redes sociales, apps de operadores, estaciones de transporte masivo, radios comunitarias.

Enfoque: Enseñar a los usuarios a identificar patrones comunes de fraude (URLs, premios falsos, llamadas con amenazas, phishing bancario, etc.).

2. Inclusión de contenidos sobre prevención del fraude en facturas o portales de autoservicio Que PRST, PCA e IT incluyan mensajes cortos educativos en:

- Facturas mensuales.
- Aplicaciones móviles.
- Correo electrónico transaccional.
- IVR de atención.

3. Sistema de simulación o "simulacro" de fraude controlado
En coordinación con la CRC, operadores podrían enviar mensajes de prueba simulando estafas reales (con un aviso al final que diga "Esto fue un simulacro de educación").

Objetivo: sensibilizar y entrenar a los usuarios en tiempo real sobre cómo identificar amenazas.

4. Participación de entidades bancarias y Fintech
Muchas estafas están asociadas al entorno financiero.

5. Propuesta: CRC lidere una mesa interinstitucional con bancos, PRSTM, PCA e IT para crear material educativo conjunto.

Cada banco podría enviar contenidos a sus clientes desde sus propios canales.

6. Inclusión del tema en programas de ciudadanía digital en colegios y universidades.
El Ministerio TIC y el Ministerio de Educación podrían incluir módulos sobre fraude móvil y ciberseguridad en programas educativos.

CRC puede articular estas iniciativas para formar desde edades tempranas.

7. Establecer un "Sello de confianza" para remitentes verificados
Similar al "check azul" de redes sociales.

La CRC puede liderar un programa que certifique remitentes legítimos con base en criterios técnicos y legales.

Al usuario se le enseñaría que los SMS o llamadas con sello de confianza son verificados.

8. Alertas en tiempo real sobre fraudes activos
Crear un canal oficial (web + bot de WhatsApp o app) donde la CRC publique tipos

de fraude activos en circulación, y los usuarios puedan suscribirse para recibir alertas, e incluso permitir reportes rápidos por parte de ciudadanos.

“d. Sobre la revisión integral 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

Frente a la consulta sobre posibles mejoras en los procedimientos de asignación y recuperación de recursos de identificación, consideramos que el mayor obstáculo para cualquier iniciativa que la CRC pretenda implementar en materia de trazabilidad o control del fraude parte precisamente de la alta burocracia que caracteriza la obtención de estos recursos ante la misma Comisión.

Actualmente, el proceso de solicitud de un recurso escaso (como lo son los códigos cortos, numeración larga o identificadores alfanuméricos) está lleno de trámites excesivos, demoras administrativas, requisitos documentales innecesarios y poca agilidad en la respuesta. Esto no solo dificulta el acceso efectivo a dichos recursos por parte de los actores habilitados, sino que hace inviable cualquier esquema dinámico de control, seguimiento o implementación de nuevas medidas para combatir el fraude.

En este sentido, nuestra principal recomendación es:

- Reducir los requisitos formales y documentales innecesarios.
- Digitalizar completamente los procesos.
- Establecer plazos perentorios de respuesta realistas y obligatorios para la CRC.
- Los tiempos de asignación debe ser más ágil.
- Revisión exhaustiva de las solicitudes presentadas ante la CRC, ya que en algunas oportunidades la CRC solicita información que ya ha sido incluida dentro de la solicitud inicial, lo cual lleva a reprocesos y dilaciones.

Finalmente, y teniendo en cuenta los tiempos de demora a los que nos vemos expuestos en los procesos de habilitación de nueva numeración en las redes de los PRSTM, proponemos que, una vez se realice la asignación de nuevos recursos de numeración, sea la misma CRC quien notifique y autorice directamente a los PRSTM la habilitación de dichos recursos en sus centrales, de manera análoga a como actualmente la CRC notifica a los PRSTM la recuperación de los recursos de identificación para su respectiva deshabilitación.

Reafirmamos nuestra disposición para continuar participando activamente en estos espacios de diálogo técnico y regulatorio, y aportar desde nuestra experiencia operativa y tecnológica a la creación de entornos digitales más seguros y confiables para todos los usuarios.

Cordialmente,



DIEGO VALDERRAMA PINILLA
Apoderado General
HABLAME COLOMBIA SA ESP
notificacionesjudiciales@hablame.co

