

RESPUESTAS:

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.

El problema definido por la CRC abarca de manera integral las dificultades asociadas al fraude cibernético en servicios tradicionales de voz y SMS, ya que:

- Reconoce la ausencia de herramientas regulatorias específicas para prevenir el contacto fraudulento a usuarios.
- Identifica tanto las causas técnicas (falta de trazabilidad, insuficiencia de controles) como las operativas (desconocimiento del usuario, falta de articulación intersectorial).
- Considera las consecuencias económicas, reputacionales y sociales, así como la pérdida de confianza en los servicios.
- Incluye la perspectiva de todos los actores de la cadena de valor (operadores, proveedores de contenido, usuarios, autoridades).

Si consideras que falta algún elemento: Podría complementarse con un enfoque más específico en fraudes emergentes asociados a nuevas tecnologías (por ejemplo, inteligencia artificial generativa para suplantación de voz o mensajes), o en la protección de grupos vulnerables (adultos mayores, menores de edad).

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.

Las causas identificadas (enfoque regulatorio en uso eficiente y no en prevención, insuficiencia de controles, desconocimiento del usuario, falta de articulación nacional) son pertinentes y reflejan la realidad del ecosistema colombiano. Estas causas explican la facilidad con la que los actores maliciosos pueden explotar los servicios tradicionales para cometer fraudes, y la dificultad de los usuarios y operadores para detectarlos y responder oportunamente.

Si consideras que falta alguna causa: Se podría agregar la rápida evolución de las técnicas de fraude y la falta de actualización continua de los marcos regulatorios y tecnológicos.

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.

Las consecuencias descritas (aumento de fraudes, vulneración de derechos, afectaciones económicas y reputacionales, pérdida de confianza) son resultado directo de la falta de controles y de la exposición de los usuarios a campañas fraudulentas. La evidencia presentada en el documento (incremento de incidentes, quejas y pérdidas económicas) respalda esta relación causal.

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.

El documento incluye a los principales grupos de valor: operadores, proveedores de contenido, integradores tecnológicos, usuarios, gremios, autoridades regulatorias y de control. Sin embargo, podría considerarse la inclusión de:

- **Empresas de ciberseguridad** (como aliados tecnológicos).
- **Asociaciones de protección al consumidor digital.**
- **Medios de comunicación** (por su rol en la educación y alerta temprana).

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?

Beneficios:

- Mayor trazabilidad y autenticidad de los remitentes.
- Facilita la identificación de campañas legítimas y fraudulentas.

- Mejora la confianza del usuario.

Desafíos:

- Costos de implementación y mantenimiento.
- Posible resistencia de actores que usan prácticas poco transparentes.
- Necesidad de interoperabilidad entre operadores.

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?

Valoración:

- **Viable** y alineado con tendencias internacionales.
- **Pros:** Mayor flexibilidad, cobertura nacional, mejor control de campañas.
- **Contras:** Complejidad administrativa, riesgo de saturación de numeración si no se gestiona bien.

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?

Efectos positivos:

- Reduce el riesgo de phishing y redirección a sitios maliciosos.

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?

Implicaciones:

- Mayor control y responsabilidad sobre el uso de cada código.
- Reduce la suplantación y el uso indebido.
- **Riesgo:** La cantidad de códigos cortos podría ser insuficiente para todos los sectores, lo que haría necesario migrar a numeración E.164 o ampliar el rango de códigos.

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?

Beneficios:

- Mayor disponibilidad de números.
- Mejor control y trazabilidad.
- Facilita la integración con otros servicios digitales.

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.

- Implementar autenticación multifactor para el envío de campañas masivas.
- Auditorías periódicas a los remitentes registrados.
- Sanciones más severas para el uso indebido de numeración.
- Fomentar la cooperación internacional para el bloqueo de campañas transfronterizas.
- Obligatoriedad de cifrado de extremo a extremo en toda la cadena de valor para la entrega de un SMS al destinatario

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?

Beneficios:

- Facilita la identificación y bloqueo de llamadas fraudulentas.
- Mejora la transparencia y confianza del usuario.

Retos:

- Complejidad en la gestión y actualización del registro.
- Posible evasión por parte de actores maliciosos usando numeración extranjera.

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?

Percepción:

- Son efectivas para reducir el volumen de llamadas y mensajes sospechosos.
- Deben complementarse con regulación sobre el uso de numeración y sanciones claras para evasores.

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.

- Implementar listas negras y blancas de numeración.
- Requerir validación previa de campañas comerciales.
- Integrar sistemas de reporte ciudadano para llamadas sospechosas.

c) 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?

Opinión:

- Es fundamental para empoderar al usuario y reducir la vulnerabilidad ante fraudes.

- El portal debe ser de fácil acceso y actualizado en tiempo real.

*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?*

Efectos:

- Permite alertar a los usuarios y operadores sobre recursos comprometidos.
- Facilita la acción preventiva y correctiva.

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?

Valoración:

- Altamente positivo, permite una respuesta coordinada y eficiente.
- Requiere interoperabilidad y compromiso de todos los actores.

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.

- Integración de alertas automáticas en dispositivos móviles.
- Incentivos para la denuncia oportuna de fraudes.
- Acompañamiento de un ente regulador para que el cliente que sea víctima de fraude pueda realizar la denuncia penal ante las entidades competentes.

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?

Medidas Propuestas

- Automatizar procesos de asignación y recuperación con sistemas digitales.
- Establecer criterios claros y transparentes para la recuperación por uso indebido.
- Publicar reportes periódicos de asignación y recuperación para transparencia sectorial.
- Sumar a la ecuación de responsabilidades, los intermediarios en el flujo de envíos de SMS

- Implementar un mecanismo de verificación de los códigos, similar a la verificación de cuentas en whatsapp
- Que las URLs contenidas en el SMS sean verificadas antes de ser enviado el SMS
- Definir marco de controles mínimos de seguridad que deben tener implementados todos los actores que accedan (usen) las plataformas o herramientas a traves de las cuales se envían los sms
- Definir y exigir el cumplimiento de un estándar de seguridad para: la comunicación, administración de las plataformas por las que se envían los sms, lo anterior para todos los actores que participan en el envío de SMS
- Establecerle al operador, PCA o IT la responsabilidad de responder económicamente por los fraudes ocasionados por el envío de url maliciosas no autorizadas a traves de los códigos cortos asignados.
- Definir los lineamientos de seguridad para los PCA para registrarse, usar códigos cortos propios y responder ante alertas.
- **Revisión del régimen de recursos de identificación:**
 - Fortalecer los procedimientos de asignación y recuperación.
 - Establecer reglas específicas para prevenir el uso indebido de numeración E.164 y códigos cortos.
- **Registro de remitentes y campañas:**
 - Crear un registro obligatorio de remitentes de SMS y llamadas comerciales.
 - Prohibir la inclusión de enlaces en SMS y la intermediación de códigos cortos.
- **Tecnologías de prevención:**
 - Implementar filtros de tráfico, autenticación de llamadas (STIR/SHAKEN), y monitoreo con IA. Con respecto al monitoreo con IA, fortalecer nuestras herramientas de prevención de fraude en tiempo real para ser cada vez oportunos.
 - Fomentar el uso de numeración no geográfica (NDC 940) para servicios A2P.
- **Educación y empoderamiento del usuario:**
 - Campañas pedagógicas sobre privacidad y prevención del fraude: Ya se hacen y están vigiladas por la SFC
 - Portal público con remitentes denunciados y recursos de identificación bloqueados: Aquí tendríamos que hacer un proceso para actualizar esa información.
- **Coordinación interinstitucional:**
 - Fortalecer la colaboración entre CRC, MinTIC, SIC, Fiscalía, Policía, ColCERT y sector privado.
 - Integrar esfuerzos con la Estrategia Nacional de Seguridad Digital 2025–2027.