

Resumen Ejecutivo	2
Introducción – mdk.digital GmbH	3
Pregunta 1a:.....	4
Pregunta 1b:.....	5
Pregunta 1c:.....	6
Pregunta 2:.....	8
Pregunta 3a:.....	9
Pregunta 3b:.....	11
Pregunta 3c:.....	13
Pregunta 3d:.....	14
1. Posibles VENTAJAS de la migración a E.164 / NDC 940:	15
2. DESAFÍOS y RIESGOS de la migración:.....	15
3. Recomendaciones para una implementación exitosa:.....	16
4. Conclusión:.....	16
Pregunta 3e:.....	17
1. Implementación de un portal central obligatorio de verificación y registro para todos los remitentes de SMS	17
2. Lista blanca obligatoria y certificación de dominios para URLs en SMS.....	17
3. Introducción de niveles de seguridad y perfiles de riesgo según sector / contenido de campaña.....	18
4. Monitoreo en tiempo real y compartición de listas negras entre operadores móviles y el regulador.....	18
5. Información obligatoria de identificación en el contenido del SMS.....	18
6. Sanciones y transparencia pública ante infracciones	19
7. Conclusión.....	19
Pregunta 4a:.....	19
1. Beneficios de dicha regulación:	20
2. Retos en la implementación:.....	20
3. Recomendaciones para su implementación:	21
4. Conclusión:.....	21
Pregunta 4b:.....	22
1. Creación de un registro nacional de originadores de llamadas (Call-Originator Registry)	22
2. Verificación de identidad obligatoria (KYC) al asignar números.....	22

3. Implementación y participación obligatoria en modelos similares a STIR/SHAKEN	23
4. Creación de una lista blanca (whitelist) de números confiables	23
5. Reglas claras sobre comportamientos permitidos y prohibidos en campañas de voz	23
6. Plataforma pública de quejas y sistema de alerta temprana	24
7. Cooperación internacional para bloquear fuentes de fraude extranjeras	24
8. Conclusión:.....	24
Pregunta 5:.....	25
1. Evaluación de la medida propuesta:.....	25
2. Ventajas y oportunidades:	25
3. Factores clave para una implementación efectiva:	26
4. Desafíos y recomendaciones:	26
5. Conclusión:.....	27
Pregunta 6:.....	27
1. Evaluación general:.....	27
2. Ventajas e impactos positivos:	27
3. Factores clave para la implementación:	28
4. Posibles desafíos y soluciones propuestas:.....	29
5. Conclusión:.....	29
Pregunta 7:.....	29
1. Evaluación general:.....	29
2. Otras medidas recomendadas para empoderar a los usuarios:	29
3. Recomendación para su implementación:	31
4. Conclusión:.....	31
Pregunta 8:.....	31
1. Objetivo general:	31
2. Sugerencias para optimizar los procesos de asignación:	32
3. Sugerencias para mejorar los procedimientos de retiro:.....	33
4. Conclusión:.....	34

Resumen Ejecutivo

La empresa **mdk.digital GmbH**, con sede en Bonn (Alemania), es un proveedor independiente y especializado en soluciones digitales para el sector de las telecomunicaciones, con una trayectoria consolidada desde 2011. En cooperación

estrecha con operadores móviles alemanes y austríacos, mdk ha desarrollado herramientas clave que fortalecen la transparencia, la trazabilidad y la confianza en la prestación de servicios móviles, incluyendo mensajería y voz.

Uno de los pilares de su modelo de servicios es la creación y operación de:

- Un sistema centralizado para el **registro de números** (cortos y largos),
- Un **portal de servicios** para el registro, categorización y validación de servicios y proveedores,
- Herramientas de cumplimiento normativo y verificación de identidad para prevenir el fraude.

La experiencia de mdk muestra que una gestión regulada, digitalizada y colaborativa de los recursos numéricos contribuye directamente a reducir prácticas fraudulentas como el **spoofing**, el uso no autorizado de remitentes, y el contacto engañoso con usuarios finales.

A través de su enfoque centrado en la responsabilidad compartida entre reguladores, operadores y proveedores, mdk ha logrado:

- Estandarizar los procesos de aprobación de servicios,
- Apoyar campañas de educación del consumidor,
- Fortalecer los controles de acceso al ecosistema móvil.

Con base en esta experiencia, mdk respalda iniciativas regulatorias como registros nacionales de remitentes, plataformas públicas de consulta y modelos de asignación de recursos basados en verificación previa (KYC), alineados con estándares internacionales

Introducción – mdk.digital GmbH

mdk.digital GmbH es una empresa independiente, de propiedad privada, con sede en Bonn, Alemania. Desde 2011, ha sido un socio confiable de los operadores de redes móviles en Alemania y Austria. Gracias a su amplia experiencia en desarrollo de software, servicios de cumplimiento normativo y soluciones de marketing digital, mdk ofrece servicios personalizados y escalables para el sector de las telecomunicaciones.

Uno de los elementos clave de mdk es el desarrollo y operación de una herramienta de registro de numeración que funciona entre distintos operadores, así como de un portal de servicios para el registro de servicios de telecomunicaciones. Estas plataformas

permiten un registro uniforme, transparente y trazable de números cortos, números largos, los servicios asociados y sus proveedores. Esto genera claridad regulatoria y brinda a los operadores una base confiable para aprobar servicios, lo cual es fundamental para prevenir el fraude y garantizar la transparencia del mercado.

Además, mdk actúa como coordinador neutral en iniciativas sectoriales a nivel nacional, apoyando la armonización de procesos, la provisión de herramientas comunes y la facilitación de consensos regulatorios, especialmente en los ámbitos de Carrier Billing y RCS.

El portafolio de servicios modulares de mdk incluye, entre otros: la gestión integral de servicios de Carrier Billing, procesos de cumplimiento y auditoría en el entorno RCS (incluyendo validación previa), así como el desarrollo y operación de plataformas digitales de marca para operadores móviles y usuarios finales.

Gracias a su experiencia en la implementación técnica y la coordinación operativa de procesos complejos con múltiples actores, mdk es un aliado confiable para soluciones móviles transparentes, basadas en reglas y sostenibles.

Pregunta 1a:

¿Por qué considera usted que el problema definido en este documento es lo suficientemente completo como para abordar todos los elementos que evidencian las dificultades generadas por el fraude cibernético en la prestación de servicios tradicionales de llamadas de voz y mensajes SMS?

En caso de que considere que el problema no contempla todos los elementos necesarios, por favor justifique su posición, aporte evidencia al respecto y proponga una formulación alternativa del problema con sus respectivas causas y consecuencias.

El documento presenta un análisis sólido sobre cómo se manifiesta el fraude cibernético a través de los servicios de voz y SMS. Se identifican elementos clave como el uso indebido de numeraciones, la falta de identificación clara de los remitentes y la escasa información disponible para los usuarios.

Con base en nuestra experiencia en el ámbito de Carrier Billing, observamos que la ausencia de una gobernanza transversal y de procedimientos de registro homogéneos entre los operadores representa un factor de riesgo significativo. mdk abordó una problemática similar mediante el desarrollo de un portal de servicios centralizado, en el cual todos los servicios y proveedores deben registrarse y ser aprobados por los operadores móviles. Esta funcionalidad debería integrarse como un elemento esencial en la definición del problema.

Desde nuestra perspectiva internacional – en particular como proveedor de un servicio centralizado de registro para servicios SMS y de voz – identificamos los siguientes retos

clave para Colombia:

1. Falta de mecanismos centralizados de registro y validación:

En Alemania existen bases de datos centralizadas para la gestión y la transparencia de numeraciones cortas y remitentes. En Colombia parece no existir una instancia comparable, lo cual facilita el uso indebido.

2. Insuficiente autenticación técnica de los remitentes:

Muchos casos de fraude se originan mediante la manipulación o suplantación de números de origen ("sender spoofing"). Se requieren mecanismos confiables como listas de remitentes registrados o sistemas de remitentes confiables.

3. Escaso intercambio de información entre actores del ecosistema:

Se evidencian brechas en la comunicación efectiva entre operadores, autoridades y usuarios finales en cuanto a mecanismos de fraude conocidos o numeraciones bloqueadas.

4. Ausencia de filtrado en tiempo real:

En Alemania, varios operadores implementan soluciones inteligentes de filtrado que analizan el tráfico en tiempo real. Este tipo de prevención técnica podría desarrollarse e implementarse también en Colombia.

Pregunta 1b:

¿Por qué considera usted que las causas señaladas en el documento para la aparición del problema son adecuadas? En caso contrario, ¿qué otras causas considera usted más relevantes?

Desde la perspectiva de un proveedor de servicios que lleva años operando sistemas de registro y verificación para servicios de telecomunicaciones, consideramos que las causas mencionadas en el documento son acertadas, aunque no completamente abarcadoras. El documento describe correctamente la fragmentación técnica, económica y regulatoria del sector, pero hace falta una mayor énfasis en las causas estructurales y de proceso que dificultan una prevención efectiva del fraude.

1. Coincidencia con las causas mencionadas:

El documento identifica en particular:

- Altos costos de implementación (barrera financiera).
- Rápida evolución de mecanismos de fraude (asimetría tecnológica).
- Falta de regulación en el segmento A2P (zonas grises legales).
- Colaboración insuficiente entre actores (brechas de información, falta de coordinación).

Estas causas también se observan en otros mercados donde no existen modelos centralizados de control o registro.

2. Causas adicionales desde una perspectiva internacional:

a) Falta de obligatoriedad y estandarización:

La ausencia de un proceso de registro nacional obligatorio y estandarizado para remitentes A2P (como marcas, campañas o numeraciones) crea un espacio no regulado donde el fraude puede prosperar.

Las diferencias en los estándares técnicos entre MNOs y agregadores dificultan la aplicación de medidas de protección eficaces.

b) Falta de transparencia sobre el origen y la ruta del mensaje:

En muchos ecosistemas, los MNOs no pueden rastrear con claridad qué marca, proveedor o agregador ha originado realmente un mensaje.

Esto socava la trazabilidad y limita la posibilidad de una respuesta rápida ante incidentes de abuso.

c) Bajo nivel de información al usuario y falta de confianza:

Muchos usuarios no saben si un mensaje es “oficial” o no, ya que no existen señales visibles de que el remitente esté registrado o verificado.

Esto genera una desconfianza generalizada hacia los canales móviles de comunicación.

3. Propuesta para ampliar el análisis de causas:

Recomendamos complementar las causas con el siguiente planteamiento:

“La ausencia de un sistema obligatorio, estandarizado a nivel nacional, para el registro y verificación de servicios A2P de SMS y voz impide un control y trazabilidad efectivos. Esta situación se agrava por la falta de una plataforma de datos centralizada con acceso coordinado entre actores clave, así como por la falta de claridad regulatoria y de interoperabilidad técnica.”

4. Conclusión:

Las causas identificadas en el documento son, en su mayoría, correctas y realistas. Sin embargo, se debería destacar la necesidad de crear condiciones estructurales (por ejemplo, registro central, interoperabilidad técnica, participación obligatoria de todos los actores del mercado) como causa fundamental del problema actual. Solo a través de un modelo obligatorio y estandarizado se podrá garantizar una protección contra el fraude que sea sostenible y efectiva.

Pregunta 1c:

¿Por qué está de acuerdo con la afirmación de que las consecuencias descritas en el documento están directamente relacionadas con la materialización del problema? Si no está

de acuerdo, ¿qué consecuencias considera usted más realistas?

Desde nuestra perspectiva, coincidimos con la conexión esencial entre las consecuencias mencionadas en el documento y el problema descrito. Es evidente que el uso descontrolado de los servicios móviles tradicionales (SMS y voz) en un entorno fragmentado y no regulado tiene efectos inmediatos sobre la confianza, la seguridad y la integridad de todo el sistema de telecomunicaciones.

1. Concordancia entre el problema y sus consecuencias:

Las consecuencias identificadas en el documento – tales como:

- Pérdida de confianza del usuario,
 - Aumento de actividades fraudulentas,
 - Daños económicos para usuarios y empresas,
 - Capacidad limitada de los operadores para responder,
- son, desde nuestra experiencia práctica, efectos directos de la falta de una estructura técnica y regulatoria capaz de prevenir el fraude de forma sistemática.

Tales relaciones causales también se han observado en otros mercados antes de la implementación de sistemas obligatorios de registro y verificación (por ejemplo, el modelo MDK en Alemania).

2. Otras consecuencias relevantes desde la práctica:

Además de los puntos mencionados, recomendamos considerar explícitamente las siguientes consecuencias:

a) Retiro de proveedores y marcas legítimas del canal:

Las empresas tienden a evitar el uso de SMS o voz cuando estos no se perciben como canales seguros y confiables.

Esto debilita el canal a largo plazo y reduce su relevancia económica en el ecosistema digital.

b) Fragmentación de estructuras de cumplimiento:

La falta de un sistema unificado lleva a la creación de soluciones aisladas a nivel de MNOs o agregadores, las cuales no son interoperables y generan costos adicionales.

Esto incrementa los costos operativos y reduce la escalabilidad de las medidas de seguridad.

c) Daños reputacionales para los operadores:

Cuando los operadores no logran bloquear comunicaciones fraudulentas, se ve afectada la percepción de su marca y su credibilidad regulatoria.

d) Debilitamiento de estrategias nacionales de transformación digital:

La falta de seguridad en los canales de comunicación impacta negativamente en iniciativas

públicas de digitalización (por ejemplo, gobierno electrónico, banca móvil).

3. Propuesta de ampliación:

Proponemos la siguiente formulación extendida:

“La falta de control sobre actores y contenidos en los servicios móviles de comunicación no solo aumenta el riesgo de fraude y la pérdida de confianza, sino que también debilita a largo plazo el canal como soporte de innovación digital y como plataforma económica para marcas, entidades públicas y consumidores.”

4. Conclusión:

Las consecuencias mencionadas en el documento están claramente relacionadas con el problema identificado. No obstante, debe ampliarse el análisis para incluir daños económicos, regulatorios y reputacionales a nivel general. La implementación de un modelo de registro obligatorio, transparente e interoperable reduciría significativamente estos riesgos.

Pregunta 2:

¿Por qué deberían incluirse más grupos de interés relevantes (“grupos de valor”) en el desarrollo de este proyecto regulatorio? ¿Cuáles serían esos grupos y por qué? En caso de considerar que ya se incluyeron todos los grupos relevantes, por favor justifique su respuesta.

Desde nuestra perspectiva, el documento actual ya contempla actores centrales como los operadores de redes móviles (MNOs), los agregadores, las autoridades reguladoras y los usuarios finales. Sin embargo, consideramos fundamental involucrar a otros grupos estratégicos en el proceso de desarrollo e implementación del proyecto regulatorio, especialmente en lo relacionado con la interoperabilidad, la estandarización, la ejecución técnica y la aceptación por parte del mercado.

1. Otros grupos relevantes que deberían considerarse:

a) Operadores de plataformas de registro centralizadas / entidades de verificación:

En modelos internacionales como el de MDK (Alemania / Austria), proveedores especializados cumplen un rol neutral en la gestión del registro de remitentes y servicios. Ellos garantizan que todas las partes tengan acceso a interfaces estandarizadas e información en tiempo real.

Su participación asegura la viabilidad técnica, escalabilidad y sostenibilidad del sistema.

b) Marcas / anunciantes / proveedores de servicios:

Estos actores son origen de muchas campañas A2P (como bancos, comercio electrónico,

entidades públicas o plataformas) y son responsables del contenido transmitido.

Su participación es esencial para:

- garantizar legitimidad y visibilidad de sus marcas,
- generar confianza y seguridad en los usuarios finales,
- minimizar riesgos de incumplimiento normativo desde el origen.

c) Proveedores de tecnología / plataformas API:

Muchos operadores trabajan con socios tecnológicos externos que proporcionan funciones clave dentro del ecosistema de mensajería.

Estos proveedores son clave para garantizar interoperabilidad técnica, cumplimiento de estándares internacionales (como GSMA o CTIA) e implementación de mecanismos de seguridad.

d) Organizaciones de consumidores y de protección de datos:

Una perspectiva centrada en el usuario es fundamental para generar confianza en el nuevo sistema.

Estas entidades pueden definir requisitos de transparencia, canales de quejas y manejo adecuado de los datos personales.

2. Justificación para su inclusión:

Un sistema moderno, eficaz y confiable contra el fraude en el ámbito móvil no puede basarse únicamente en el control técnico de los MNOs o la regulación estatal. Requiere una colaboración abierta y coordinada entre todos los actores del ecosistema. En mercados donde se busca recuperar la confianza en la comunicación digital, este enfoque multiactor resulta clave para el éxito.

3. Conclusión:

Aunque el documento ya menciona actores importantes, recomendamos ampliar sistemáticamente el conjunto de los “grupos de valor”. Es fundamental incluir:

- operadores neutrales de registro o plataformas,
- las propias marcas emisoras y proveedores de servicios,
- proveedores de infraestructura tecnológica,
- y organizaciones de la sociedad civil centradas en la protección del usuario.

Estos grupos deben participar activamente en la consulta, diseño, pruebas y gobernanza del sistema para crear un modelo sólido, aplicable y sostenible a largo plazo.

Pregunta 3a:

¿Cómo evalúa usted la creación de un registro de remitentes que integre tanto números cortos como números de servicio no geográficos (numeración E.164 bajo el NDC 940), siempre que se actualicen las categorías de asignación? ¿Considera que este modelo es viable? ¿Cuáles son las ventajas y desventajas que observa?

Desde nuestra perspectiva como operador de un sistema consolidado de registro y verificación de números cortos y de servicio en los mercados de Alemania y Austria,

consideramos que la solución propuesta es fundamentalmente viable y orientada al futuro, siempre que se cumplan ciertas condiciones.

1. Evaluación de la solución propuesta:

La integración de números cortos y números de servicio E.164 no geográficos en un registro central representa un paso lógico hacia una mayor transparencia, control y gobernanza unificada en el ámbito completo de la comunicación A2P (Application-to-Person).

Un registro de este tipo puede contribuir a estandarizar la estructura del mercado y, al mismo tiempo, permitir una prevención eficaz del fraude, siempre que esté respaldado por marcos técnicos y regulatorios claros.

2. Ventajas (PROs):

a) Normativa uniforme para diferentes tipos de numeración:

Tratar por igual los números cortos y los números de servicio E.164 proporciona claridad y transparencia para proveedores, operadores y autoridades regulatorias.

Facilita una revisión, aprobación y trazabilidad homogénea de todos los tipos de números usados en A2P.

b) Mayor lucha contra el uso indebido y el spoofing:

Un registro central puede detectar y bloquear el uso no autorizado de numeraciones (por ejemplo, suplantación de identidad).

Una categorización y asignación clara aumenta la responsabilidad de los proveedores de servicios.

c) Fomento de la innovación tecnológica y comercial:

El uso de números no geográficos ofrece mayor flexibilidad para modelos de comunicación modernos (como campañas omnicanal).

Una política de numeración más abierta con categorías bien definidas puede atraer nuevos actores al mercado.

d) Reducción de la carga para los operadores:

Procesos estandarizados para la asignación y uso de números pueden reducir los costos administrativos de los operadores móviles.

El registro asume muchas funciones de verificación y documentación que actualmente están fragmentadas.

3. Desafíos y riesgos (CONTRAs):

a) Necesidad de categorías y criterios de asignación bien definidos:

Una categorización diferenciada y adaptada a la práctica es esencial para evitar un uso excesivo o indebido de los recursos NDC 940.

Las categorías deben ser dinámicas y adaptarse a nuevos casos de uso.

b) Posibles problemas de transición y necesidad de coordinación:

Consolidar los rangos existentes en un sistema central requiere una estrategia de migración precisa para evitar interrupciones o inconsistencias.

Es clave la coordinación entre reguladores, operadores y titulares de números actuales.

c) Armonización técnica de la infraestructura de enrutamiento:

Diferencias en lógicas de enrutamiento y cobro entre números cortos y E.164 requieren una implementación técnicamente alineada, especialmente en terminación y tarifas.

d) Riesgo de distorsiones del mercado por falta de responsabilidades claras:

Si no se involucra a todos los actores por igual (por ejemplo, agregadores, OTT), pueden surgir zonas grises en cuanto a responsabilidades.

4. Conclusión:

Consideramos que la alternativa propuesta es viable y valiosa si se cumplen los siguientes requisitos:

- Implementación de un registro unificado y transparente con roles definidos (marca, agregador, operador).
- Categorías de asignación definidas regulatoriamente pero flexibles tecnológicamente.
- Obligación de registrar toda comunicación A2P, independientemente del tipo de número utilizado.
- Interfaces abiertas (APIs) para integrar operadores, agregadores y autoridades.
- Capacitación, asistencia en migración y soporte a usuarios actuales de números cortos y E.164.

Este enfoque podría alinear a Colombia con las mejores prácticas internacionales como las europeas (MDK) y representar un paso clave hacia un entorno de comunicación móvil más seguro y confiable.

Pregunta 3b:

¿Qué impacto tendría una medida regulatoria que prohíba insertar enlaces (URLs) en los contenidos de los mensajes SMS? ¿Podría esta restricción contribuir a la prevención del fraude? ¿Qué consecuencias tendría para el mercado de envío de SMS?

Desde nuestra perspectiva, una regulación general que prohíba todas las formas de enlaces en mensajes SMS no sería efectiva para combatir el fraude de manera eficiente y tendría efectos negativos significativos sobre actores legítimos del mercado, modelos de negocio y la experiencia del usuario. Esta medida trasladaría el problema en lugar de resolverlo y limitaría seriamente la comunicación legítima.

1. Posibles efectos positivos (reducción de riesgos):

a) Limitación del uso de métodos comunes de fraude:

Muchos ataques de phishing y smishing se basan en enlaces falsos que redirigen a sitios fraudulentos.

Una prohibición general de enlaces bloquearía esta posibilidad técnica de redirección.

b) Reducción de clics impulsivos por parte de los usuarios:

Sin enlaces clicables, es menos probable que los usuarios reaccionen inmediatamente ante mensajes fraudulentos.

Esto puede ayudar a reducir daños, especialmente en usuarios con poca alfabetización digital.

2. Impactos negativos significativos (mercado, innovación, comunicación):

a) Restricción masiva de la comunicación legítima:

Muchas entidades legítimas usan SMS con enlaces, como:

Bancos para autenticación de dos factores (p. ej., enlaces TAN),

Entidades públicas para citas o acceso a documentos,

Comercio electrónico para estados de envío o devoluciones,

Servicios de salud para resultados de pruebas o portales de pacientes.

Una prohibición limitaría severamente el uso legítimo del canal SMS o lo haría poco atractivo.

b) Desplazamiento del fraude hacia otros mecanismos:

Los estafadores cambiarían de táctica, usando:

Números ocultos, llamadas devueltas o códigos QR,

Canales alternativos como WhatsApp, RCS o correo electrónico.

La medida no aborda el problema estructural de la verificación del remitente.

c) Desventaja competitiva frente a servicios OTT:

Mientras plataformas como WhatsApp, Telegram o iMessage seguirían permitiendo enlaces, el canal SMS A2P perdería relevancia.

Esto puede debilitar la soberanía digital y el control sobre las infraestructuras nacionales de comunicación.

3. Medidas alternativas más efectivas:

En lugar de una prohibición general, recomendamos una combinación de medidas:

Registro y verificación obligatoria de remitentes y campañas en un sistema centralizado.

Uso de enlaces cortos certificados y verificados (p. ej., dominios de confianza o acortadores de URLs integrados al sistema).

Revisión automática de enlaces contra malware y phishing por parte de operadores o plataformas antifraude centralizadas.

Identificación clara de campañas oficiales, mediante elementos visuales o estructuras de enlace predefinidas.

4. Conclusión:

Una prohibición general de enlaces en mensajes SMS obstaculizaría severamente la comunicación útil y legítima, sin resolver la raíz del problema del fraude. La mejor alternativa incluye:

Registro obligatorio de remitentes y campañas,

Transparencia y trazabilidad,
 Uso de URLs verificadas y de confianza,
 y detección tecnológica de fraude en tiempo real.
 Solo un enfoque ecosistémico y diferenciado puede reducir el riesgo de fraude de forma efectiva, sin afectar negativamente el mercado o la experiencia del usuario.

Pregunta 3c:

¿Qué impacto tendría la prohibición de la reventa o subarrendamiento de números cortos por parte de sus titulares, asignando cada número corto de forma exclusiva a un propósito definido (por ejemplo, servicios financieros) y a un solo remitente (por ejemplo, Banco X)?
 ¿Es suficiente el stock actual de números cortos o sería necesario migrar a otros tipos de numeración?

1. Evaluación de la medida – Principio de exclusividad para números cortos:

La asignación de cada número corto a un único remitente identificado dentro de una categoría claramente definida puede ofrecer importantes beneficios en términos de transparencia, seguridad y trazabilidad. No obstante, requiere un análisis detallado de los recursos disponibles y de los posibles impactos en el mercado.

2. Ventajas de la asignación exclusiva:

a) Máxima trazabilidad y seguridad:

Cada número corto está vinculado de manera inequívoca a un proveedor de servicios y una categoría (por ejemplo, "86000 = Banco X").
 Esto impide el spoofing y el uso indebido por parte de terceros que intenten suplantar la identidad.

b) Generación de confianza en los usuarios:

La asignación estática facilita el reconocimiento inmediato del remitente legítimo.
 Esto mejora la confianza y disposición a interactuar por parte del usuario.

c) Eliminación de estructuras opacas de intermediación:

La eliminación de agregadores que revenden números reduce el riesgo de abuso.
 El registro puede identificar con claridad quién es responsable legal y operativamente del tráfico.

3. Desafíos y riesgos:

a) Posible escasez de números disponibles:

Dependiendo del plan de numeración (por ejemplo, 5 dígitos), el total de combinaciones es limitado (~90,000 desde 10000).

El uso exclusivo por remitente y categoría podría saturar el sistema rápidamente, especialmente con la digitalización en crecimiento.

b) Acceso limitado para pymes y campañas pequeñas:

Si cada organización requiere su propio número corto, los costes y la complejidad aumentan.

Esto desfavorece a los actores más pequeños, que actualmente se benefician de modelos compartidos.

c) Mayor carga administrativa:

La entidad encargada debe gestionar categorías, marcas, usos y estado de los números, lo que implica un esfuerzo considerable.

Los cambios (fusiones de marcas, ampliación de categorías) deben ser reflejados sistemáticamente.

4. Soluciones y alternativas:

a) Modelo mixto de uso exclusivo y compartido:

Asignación exclusiva para sectores sensibles (finanzas, gobierno, salud).

Uso compartido (a través de agregadores verificados) para campañas de menor riesgo (retail, eventos).

b) Uso de numeraciones alternativas:

Si no hay suficientes números cortos, pueden emplearse:

Números E.164 no geográficos (ej. NDC 940),

o remitentes alfanuméricos.

c) Registro de verificación en lugar de exclusividad total:

Un registro centralizado con validación en tiempo real puede ofrecer altos niveles de seguridad y transparencia sin requerir exclusividad absoluta.

5. Conclusión:

La asignación exclusiva por remitente y categoría es una herramienta efectiva contra el fraude y para generar confianza, pero debe:

focalizarse en sectores de alto riesgo,

complementarse con un sistema de gestión de numeración estructurado,

y, si es necesario, apoyarse en otros tipos de numeración.

La exclusividad total para todos los sectores sería problemática desde el punto de vista de la disponibilidad y la estructura del mercado, aunque podría ser viable en un modelo híbrido.

Pregunta 3d:

¿Qué ventajas o desafíos identifica en la migración del uso de números cortos tradicionales a una numeración de servicio no geográfica E.164 (NDC 940) para el uso de contenidos y aplicaciones a través de SMS y USSD, bajo la condición de una estricta regla de exclusividad y prohibición de comercialización por terceros?

La migración propuesta representa una medida orientada al futuro para la consolidación y estandarización de la estructura nacional de numeración. Ofrece la oportunidad de superar

las limitaciones actuales del sistema de números cortos, aunque conlleva desafíos operativos, técnicos y comerciales.

1. Posibles VENTAJAS de la migración a E.164 / NDC 940:

a) Mayor disponibilidad de números y mejor escalabilidad:

El formato E.164 ofrece una cantidad significativamente mayor de combinaciones disponibles que los números cortos (por ejemplo, millones de combinaciones posibles con números de 10 dígitos).

Esto es especialmente relevante bajo un esquema de asignación exclusiva por servicio o remitente.

b) Armonización con estándares internacionales:

La numeración E.164 es reconocida a nivel mundial y compatible con las infraestructuras de red y ruteo existentes.

Facilita la interoperabilidad regional y global, incluso para roaming, integración OTT o proveedores internacionales.

c) Unificación del acceso por SMS y USSD:

Los usuarios pueden acceder a distintos servicios móviles (SMS, USSD, carrier billing) a través de un número unificado.

Esto favorece la coherencia en la interacción con el cliente y facilita el acceso a los servicios.

d) Mayor control por parte del regulador y los operadores móviles:

La asignación clara de un número E.164 a un proveedor exclusivo evita el spoofing. Permite una aplicación más precisa de normas de seguridad, uso y cumplimiento.

e) Sostenibilidad tecnológica a largo plazo:

A diferencia de los números cortos, que ya están siendo retirados en algunos mercados, los números E.164 son interoperables entre redes y sostenibles a futuro.

2. DESAFÍOS y RIESGOS de la migración:

a) Menor recordación y efecto de marca:

Los números cortos (ej. "12345") son más fáciles de memorizar y más breves que los números E.164 ("940xxxxxxx").

Una migración podría generar confusión temporal en los usuarios finales y debilitar el vínculo con la marca.

b) Necesidad de amplias campañas de comunicación:

Una migración requiere amplias actividades de información al usuario, cambios técnicos y

campañas comunicacionales, especialmente en servicios consolidados (ej. bancos, entidades públicas).

c) Ruteo y modelo tarifario más complejo:

La facturación y el ruteo de números E.164 a través de múltiples operadores pueden ser técnicamente más complejos y costosos que con números cortos.

Se deberá definir una estructura tarifaria uniforme.

d) Dificultades en la migración de servicios existentes:

Los servicios y números actuales deberán ser re-registrados, adaptados y migrados técnicamente, con posibles interrupciones y problemas de interoperabilidad.

e) Posible aumento de barreras para pymes:

La exigencia de exclusividad y asignación individual podría elevar los costos o la complejidad técnica, lo que podría desincentivar la participación de proveedores pequeños.

3. Recomendaciones para una implementación exitosa:

- **Modelo híbrido durante una fase de transición:**
Operación paralela de números cortos y números E.164, según caso de uso, categoría de riesgo o sector.
- **Comunicación y formación activa del usuario:**
Campañas claras para explicar los nuevos formatos numéricos, por ejemplo, vía SMS, medios, sitios web.
- **Entidad central de asignación y directorio público:**
Creación de un registro transparente con información sobre los números asignados, sector, marca y propósito.
- **Permitir mantener la identidad de marca mediante shortcodes opcionales:**
Operación paralela opcional o asignación de “nombres amigables” a números E.164 para mejorar la recordación.
- **Garantizar acceso equitativo a pequeños proveedores:**
Estructura de tarifas escalonada, portales de autoservicio, opciones de infraestructura compartida bajo control del regulador.

4. Conclusión:

La migración de números cortos a numeración de servicio no geográfica basada en E.164 (NDC 940) es una opción estratégica viable para un modelo de comunicación escalable, seguro y con proyección internacional.

Es viable, pero no trivial, y debe ir acompañada de:

- gobernanza clara,
- reglas de asignación definidas,

- modelos de transición
- y una comunicación activa con el mercado y los usuarios.

Pregunta 3e:

¿Qué otras alternativas regulatorias podrían, en su opinión, contribuir a prevenir el uso indebido de números cortos y el contacto fraudulento con usuarios finales a través de SMS? Por favor descríbalas en detalle.

Además de las medidas ya discutidas (por ejemplo, registro de remitentes, modelos de exclusividad, control de enlaces), recomendamos con base en nuestra experiencia internacional en gestión de numeración y prevención de fraude, las siguientes medidas regulatorias adicionales que han demostrado ser especialmente eficaces en otros mercados:

1. Implementación de un portal central obligatorio de verificación y registro para todos los remitentes de SMS

Descripción:

Creación de un registro nacional para la comunicación A2P, donde todas las marcas, agregadores, números, campañas y contenidos deben ser registrados y aprobados antes del envío.

Integración con los sistemas de los operadores móviles para su aplicación en el acceso a la red.

Ventajas:

- Trazabilidad total de cada campaña.
- Prevención del spoofing y del uso no autorizado de números.
- Permite sanciones específicas en tiempo real (por ejemplo, bloqueo en caso de infracción).

Ejemplo:

MDK en Alemania/Austria (portal central de servicios para números cortos, incluyendo categorización de servicios).

2. Lista blanca obligatoria y certificación de dominios para URLs en SMS

Descripción:

En lugar de prohibir todos los enlaces: solo se permiten dominios verificados y registrados. Asociación de dominios con remitentes y evaluación previa de seguridad.

Ventajas:

- Protección frente a enlaces de phishing.
- Fomento de comunicaciones legítimas.
- Flexible y adaptable ante nuevas amenazas.

3. Introducción de niveles de seguridad y perfiles de riesgo según sector / contenido de campaña

Descripción:

Clasificación de campañas SMS por categoría de riesgo (alta/media/baja).
Exigencias de seguridad más altas (por ejemplo, autenticación multifactorial) para sectores de alto riesgo (banca, salud).

Ventajas:

- Enfoque diferenciado: se protege estrictamente la comunicación sensible sin perjudicar el comercio legítimo.

4. Monitoreo en tiempo real y compartición de listas negras entre operadores móviles y el regulador

Descripción:

Creación de un sistema central de monitoreo para supervisar campañas SMS en vivo.
Establecimiento de una lista negra y sistema de reporte de incidentes compartido.

Ventajas:

- Detección temprana de patrones de ataque.
- Respuesta coordinada del mercado ante amenazas detectadas.

5. Información obligatoria de identificación en el contenido del SMS

Descripción:

Cada SMS A2P debe incluir al inicio o al final:

- Identificación clara del remitente,
- Referencia al registro o campaña (ej. "REGISTRO CRC #123456").

Ventajas:

- Transparencia para el usuario.

- Mejor identificación de comunicaciones oficiales.
- Facilita la recolección de pruebas en casos de fraude.

6. Sanciones y transparencia pública ante infracciones

Descripción:

Publicación de advertencias, multas y bloqueos por uso indebido de números.
Obligación para los operadores de denegar acceso a la red en caso de reincidencia.

Ventajas:

- Efecto disuasorio.
- Generación de confianza en la ciudadanía.

7. Conclusión:

Un marco regulatorio eficaz para combatir el uso indebido de números cortos debe ser:

- sistémico,
- preventivo,
- apoyado tecnológicamente,
- y obligatorio para todos los actores del mercado.

La combinación de un registro central de remitentes y campañas, verificación técnica, requisitos de visibilidad, sanciones y cooperación entre todos los actores (incluidos operadores, marcas, agregadores y autoridades) brinda la mayor protección frente al fraude cibernético vía SMS.

Pregunta 4a:

¿Qué ventajas y desafíos identifica en la implementación de un registro de originadores de llamadas comerciales y publicitarias que incluya los siguientes elementos:

- Identificación alfanumérica visible para los usuarios,
- uso exclusivo de rangos numéricos dedicados,
- bloqueo de números internacionales inválidos o sospechosos,
- registro obligatorio de campañas de voz?

1. Beneficios de dicha regulación:

a) Mayor confianza gracias a la identificación clara del origen:

Las identificaciones alfanuméricas (ej. “MiBanco”) permiten a los usuarios reconocer inmediatamente al llamante, en lugar de ver un número desconocido o falsificado.

Esto reduce la probabilidad de aceptar llamadas fraudulentas y fortalece el canal legítimo de voz.

b) Protección contra el spoofing y el uso indebido de identidades:

El uso exclusivo de rangos numéricos registrados y el bloqueo de números sospechosos combate activamente el spoofing (suplantación de identidad numérica).

Solo números autorizados podrán ser usados en campañas, similar al concepto de “Identificación Verificada del Llamante”.

c) Transparencia y trazabilidad de las campañas:

El registro obligatorio de cada campaña de voz – vinculando remitente, fecha y contenido – permite:

- rastrear abusos,
- gestionar quejas eficientemente,
- reaccionar rápidamente desde la regulación.

d) Equidad en el mercado:

Reglas iguales para todos los actores del mercado generan confianza en los usuarios y equidad para los proveedores serios.

Quienes actúan de forma abusiva pueden ser identificados y excluidos mediante el registro.

e) Coherencia con modelos internacionales:

Estos mecanismos ya existen, por ejemplo, en:

- EE. UU. (STIR/SHAKEN + Voice Campaign Registry),
- Reino Unido (registro CLI de Ofcom),
- Alemania (directrices CLI de BNetzA y sistema de sanciones).

2. Retos en la implementación:

a) Implementación técnica y modernización de redes:

No todos los operadores en Colombia disponen de la infraestructura necesaria para mostrar identificaciones alfanuméricas.

La implementación requiere inversiones tecnológicas tanto por parte de los MNOs como de plataformas IP.

b) Riesgo de sobrecarga regulatoria para pequeñas empresas:

Pequeños proveedores o centros de llamadas podrían verse sobrepasados por los requisitos técnicos y de registro.

Se necesitan modelos de escalabilidad claros (por ejemplo, según volumen de campaña o sector).

c) Necesidad de una entidad central de verificación confiable:

Este sistema requiere de una plataforma neutral y centralizada para registrar y verificar:

- remitentes,
- números,
- campañas,
- y la identidad de los solicitantes.

d) Dificultad de aplicar medidas a llamadas fraudulentas desde el extranjero:

Muchos fraudes provienen de llamadas internacionales con números falsificados o sin regulación.

Se requieren mecanismos de coordinación internacional, bloqueo y rastreo, posiblemente con apoyo de bases de datos globales de carriers y fraudes.

3. Recomendaciones para su implementación:

- **Fase piloto con enfoque basado en riesgo:**
Iniciar con sectores de alto riesgo (finanzas, seguros, entidades públicas) y expandir gradualmente a otros.
- **Vinculación con registro central de numeración y validación de identidad (KYC):**
Solo empresas verificadas podrán acceder a rangos numéricos oficiales para campañas.
- **Procesos de denuncia y quejas transparentes para consumidores:**
Canales fáciles para reportar llamadas sospechosas (ej. línea corta o formulario web), acompañados de sanciones claras.
- **Requisitos técnicos mínimos para todos los carriers y proveedores VoIP:**
Obligación de soportar identificadores alfanuméricos y verificación en tiempo real con el registro.

4. Conclusión:

Un registro centralizado para originadores de llamadas – complementado con rangos dedicados, mecanismos de bloqueo y registro obligatorio de campañas – es una herramienta eficaz contra el fraude telefónico y el mal uso de numeración E.164.

Proporciona transparencia, seguridad y responsabilidad, especialmente si se combina con tecnologías modernas de identificación y un marco regulatorio claro.

Sin embargo, su implementación requiere estandarización técnica, introducción por fases y una estructura de gobernanza sólida para garantizar eficacia, equidad de mercado y protección al usuario.

Pregunta 4b:

¿Qué otras medidas regulatorias podrían, en su opinión, ayudar a prevenir el uso indebido de números E.164 y proteger a los consumidores de contactos de voz presuntamente fraudulentos?

1. Creación de un registro nacional de originadores de llamadas (Call-Originator Registry)

Descripción:

Registro obligatorio de todas las campañas de llamadas comerciales o públicas, incluyendo:

- entidad emisora (persona jurídica),
- número(s) E.164 utilizados,
- objetivo de la campaña (ej. publicidad, información, autenticación),
- horarios y alcance.

Objetivo:

- Trazabilidad total de las campañas de voz,
- posibilidad de desactivación inmediata en caso de abuso.

2. Verificación de identidad obligatoria (KYC) al asignar números

Descripción:

Toda persona natural o jurídica que desee utilizar un número E.164 para llamadas masivas debe:

- identificarse plenamente (KYC),
- declarar el uso previsto,
- cumplir requisitos de certificación (por ejemplo, de la autoridad reguladora o entidad autorizada).

Objetivo:

- Prevenir el uso anónimo o fraudulento de números,
- aplicar sanciones dirigidas en caso de abuso.

3. Implementación y participación obligatoria en modelos similares a STIR/SHAKEN

Descripción:

Adopción de un sistema de autenticación digital de llamadas, donde cada llamada incluya una firma digital que:

- confirme la autenticidad del número de origen,
- impida técnicamente la suplantación de identidad (spoofing).

Objetivo:

- Garantizar al destinatario la autenticidad técnica del llamante,
- bloquear automáticamente identificaciones falsas.

4. Creación de una lista blanca (whitelist) de números confiables

Descripción:

Creación de un directorio público que:

- contenga los números E.164 registrados, verificados y aprobados para campañas de voz,
- indique la entidad correspondiente y el propósito autorizado.

Objetivo:

- Permitir que usuarios y operadores distingan entre llamadas legítimas y sospechosas,
- habilitar el uso automatizado de listas blancas en la operación de red.

5. Reglas claras sobre comportamientos permitidos y prohibidos en campañas de voz

Descripción:

Las directrices regulatorias deben establecer:

- horarios permitidos,
- frecuencia máxima de llamadas,
- obligación de ofrecer opción de exclusión (por ejemplo, mediante tecla),
- sanciones en caso de incumplimiento.

Objetivo:

- Proteger contra llamadas molestas,
- establecer obligaciones claras para los proveedores de servicios de voz.

6. Plataforma pública de quejas y sistema de alerta temprana

Descripción:

Creación de un sistema centralizado de reporte de llamadas sospechosas:

- los usuarios pueden reportar números fácilmente (vía app, SMS o formulario web),
- análisis automático y retroalimentación a los operadores,
- publicación de números reportados con frecuencia como lista de advertencia.

Objetivo:

- Detectar patrones de fraude de forma anticipada,
- involucrar activamente a la ciudadanía en el sistema de protección.

7. Cooperación internacional para bloquear fuentes de fraude extranjeras

Descripción:

Colaboración con entidades regulatorias y operadores internacionales para:

- bloquear llamadas internacionales suplantadas,
- restringir el acceso de proveedores extranjeros sin identificación válida de origen.

Objetivo:

- Reducir las llamadas fraudulentas internacionales que no pueden controlarse eficazmente desde el ámbito nacional.

8. Conclusión:

La prevención efectiva del uso indebido de números E.164 para fraudes en llamadas requiere un modelo de múltiples componentes, que combine:

- soluciones técnicas (filtrado, firmas digitales, listas blancas),
- medidas regulatorias (registro, KYC, sanciones),
- y participación transparente del mercado y los usuarios (canales de queja, alertas tempranas).

Solo a través de este modelo integral, Colombia podrá fortalecer la protección del usuario y al mismo tiempo consolidar el canal de voz legítimo.

Pregunta 5:

¿Cómo evalúa la implementación de obligaciones obligatorias de educación y prevención para operadores móviles, proveedores de contenido de aplicaciones (PCA) e integradores técnicos, complementadas con un portal operado por la CRC con información sobre remitentes denunciados?

1. Evaluación de la medida propuesta:

Acogemos positivamente esta medida, ya que puede contribuir de manera decisiva al fortalecimiento de la capacidad de los usuarios y a la prevención sostenible del fraude. La educación y la transparencia son esenciales para complementar las medidas técnicas y regulatorias con mecanismos de protección conductuales.

2. Ventajas y oportunidades:

a) Fortalecimiento de la resiliencia digital del usuario:

Muchos fraudes exitosos se basan en el desconocimiento, la manipulación psicológica o la falta de conciencia de riesgo (por ejemplo, smishing, vishing).

La educación obligatoria y comprensible por parte de los operadores y proveedores puede mejorar significativamente la capacidad de respuesta de los usuarios en caso de emergencia.

b) Fuente de información unificada y confiable mediante portal de la CRC:

Un portal centralizado operado por la CRC sobre remitentes denunciados, números sospechosos o campañas fraudulentas genera confianza y orientación.

Los usuarios pueden verificar la fuente antes de abrir enlaces o devolver llamadas.

c) La obligación para todos los actores del mercado aumenta la eficacia:

La inclusión de:

- operadores móviles (MNO),
 - proveedores de contenido de aplicaciones (PCA),
 - integradores tecnológicos y comerciales,
- asegura que la educación no sea puntual sino sistémica, por ejemplo, en disclaimers SMS, portales o comunicaciones al cliente.

d) La prevención reduce el impacto regulatorio y económico a largo plazo:

Usuarios informados reportan más rápidas actividades sospechosas, evitan liberar información personal por error,

y reducen el riesgo de daños extensivos o perjuicios reputacionales a proveedores legítimos.

3. Factores clave para una implementación efectiva:

a) Definición clara de requisitos mínimos para la educación:

Por ejemplo, contenidos obligatorios sobre:

- cómo identificar fraudes comunes,
- comunicación segura por SMS y voz,
- importancia de la identificación del remitente y los enlaces cortos,
- cómo actuar en caso de sospecha.

b) Obligación de contacto regular con el cliente, por canal específico:

Ejemplo: notificaciones push, SMS, ventanas emergentes en portales de clientes, avisos en el momento de contratación.

c) Integración técnica con el portal de la CRC:

Ejemplo: interfaz API para que los operadores móviles consulten en tiempo real el estado de números y campañas.

d) Posibilidad de interacción directa del usuario con el portal CRC:

- Búsqueda de remitentes / números,
- reporte en línea de actividades sospechosas,
- materiales educativos y alertas actuales.

4. Desafíos y recomendaciones:

a) Riesgo de fragmentación sin coordinación centralizada:

Debe evitarse que cada proveedor genere campañas informativas por separado; por ello: obligación de alinearse con contenidos y lineamientos de diseño de la CRC.

b) Riesgo de incumplimiento práctico:

Sin sanciones claras o criterios de evaluación, algunas empresas podrían cumplir de manera formal pero no efectiva (ej. enlaces ocultos en el pie de página).

Recomendación: la CRC debe evaluar periódicamente la visibilidad, claridad y vigencia de las medidas educativas.

5. Conclusión:

La combinación de:

- educación obligatoria por parte de los actores del mercado,
- una plataforma nacional de referencia (portal CRC), constituye una herramienta eficaz, proporcional y accesible para prevenir ataques de ingeniería social.

Esta medida cierra la brecha entre la seguridad técnica y el comportamiento humano, y debe formar parte obligatoria de un sistema integral antifraude.

Esto es algo que también hemos implementado en Alemania y Austria para DCB en conjunto con operadores y autoridades regulatorias.

Pregunta 6:

¿Cómo evalúa la creación de un sistema intersectorial para la trazabilidad de los recursos de identificación (por ejemplo, números telefónicos, identificadores de remitente), administrado por la CRC, que centralice todas las quejas PQRD9 de los usuarios y se complemente con acciones educativas conjuntas de todos los sectores involucrados?

1. Evaluación general:

Consideramos que la creación de dicho sistema es una medida altamente efectiva, estratégicamente acertada y urgentemente necesaria para combatir el uso indebido de números, identificadores de remitente y otros recursos de comunicación a través de los distintos sectores.

Ofrece beneficios regulatorios concretos y protección directa a los usuarios finales, siempre que se implemente con estándares claros, participación abierta y obligatoriedad operativa.

2. Ventajas e impactos positivos:

a) Trazabilidad integral entre sectores:

Muchos casos de fraude atraviesan sectores (por ejemplo, telecomunicaciones ↔ finanzas ↔ comercio electrónico).

Un sistema centralizado bajo administración de la CRC permite unir información de múltiples industrias para detectar estructuras de fraude complejas.

b) Detección temprana de patrones de abuso:

El análisis centralizado de quejas PQRD9 (Petición, Queja, Reclamo, Denuncia) permite identificar a tiempo:

- infractores recurrentes,
- patrones fraudulentos de comunicación,
- debilidades técnicas en el sistema.

c) Promoción de la colaboración y la responsabilidad compartida:

La CRC se convierte en el punto de coordinación para seguridad y cumplimiento, no solo con operadores, sino también con:

- entidades financieras,
- plataformas digitales,
- desarrolladores de apps,
- proveedores de pagos,
- y otros sectores críticos.

Esto fortalece la confianza entre sectores y frente a la ciudadanía.

d) Mejor base de datos para prevención y educación:

El análisis de quejas y trazabilidad permite definir campañas educativas según públicos, regiones y canales específicos.

3. Factores clave para la implementación:

a) Estándares de datos e interfaces unificados (APIs):

Todos los actores deben adoptar formatos estandarizados para reportes de incidentes, números, campañas y quejas.

Es clave disponer de interfaces interoperables y seguras para el intercambio de información.

b) Participación obligatoria para sectores críticos:

La participación debe ser obligatoria por ley o por acuerdos con CRC para:

- operadores móviles,
- agregadores,
- bancos,
- plataformas digitales.

c) Participación de los usuarios finales mediante búsqueda y reporte:

El sistema debe ser accesible al público, con:

- buscador de números/remitentes,
- estado del número (investigado, bloqueado, registrado),
- formulario fácil de denuncias PQRD9.

d) Enlace con campañas educativas:

CRC debe coordinar campañas de sensibilización con apoyo de telecomunicaciones, sector financiero, autoridades, etc.

Enfoque multicanal: TV, SMS, radio, redes sociales, apps bancarias.

4. Posibles desafíos y soluciones propuestas:

Desafío

Solución recomendada

Riesgos de privacidad por el manejo centralizado de datos

Finalidad clara, control de acceso, cifrado y auditoría

Sistemas de TI heterogéneos en los sectores

Kit de integración estandarizado gestionado por CRC

Baja disposición de colaboración en algunos sectores

Participación obligatoria para sectores clave + incentivos para otros

Exceso de información irrelevante en quejas PQRD

Uso de IA para agrupar, filtrar y priorizar reclamos

5. Conclusión:

Un sistema intersectorial de trazabilidad de recursos de identificación, administrado por la CRC y combinado con un canal unificado de quejas (PQRD9) y un portal informativo público, es una herramienta clave para combatir el fraude sistémico en las comunicaciones.

Junto con el registro obligatorio, la verificación técnica de remitentes y la educación al usuario, esta medida puede aumentar de forma sostenible la resiliencia del ecosistema digital colombiano

Pregunta 7:

¿Qué otras medidas considera adecuadas para fortalecer el conocimiento y la capacidad de autoprotección (empoderamiento) de los usuarios frente a los riesgos de fraude cibernético a través de servicios móviles?

1. Evaluación general:

La protección frente al fraude cibernético en el sector móvil no puede depender únicamente de la tecnología o la regulación.

Es fundamental que los usuarios estén capacitados para reconocer los riesgos, interpretarlos correctamente y actuar de forma activa.

Además de los enfoques ya discutidos (obligaciones de información, portal CRC, colaboración intersectorial), recomendamos otras medidas específicas, accesibles y de alto impacto para fomentar la resiliencia digital y la alfabetización mediática.

2. Otras medidas recomendadas para empoderar a los usuarios:

a) Indicadores de seguridad móvil en las interfaces de usuario (por ejemplo, alertas en SMS, etiquetas de llamadas)

Descripción:

Integración de alertas visuales de seguridad en apps de SMS y pantallas de llamadas:

Ej.: "Remitente verificado", "Origen desconocido", "Número no registrado".

Texto en llamadas entrantes: "No registrado oficialmente ante la CRC".

Beneficio:

Las señales visibles fortalecen la conducta del usuario y fomentan la desconfianza ante mensajes o llamadas sospechosas.

Ejemplo:

En EE. UU., los operadores móviles etiquetan llamadas como "Scam Likely" o "Verified Business".

b) Implementación de micropruebas o advertencias obligatorias antes de ciertas transacciones

Descripción:

Previo a acciones sensibles (ej. SMS solicitando pagos), los usuarios recibirían advertencias tipo Pop-Up o micropruebas, por ejemplo:

"¿Sabe cómo identificar un remitente legítimo?"

o:

"Nunca comparta su PIN por SMS o llamada."

Beneficio:

Interrumpe acciones impulsivas y aumenta la atención del usuario en momentos críticos.

c) Programa de certificación en "resiliencia digital" para usuarios

Descripción:

Desarrollo de un programa voluntario por parte de la CRC o en alianza con instituciones educativas:

Ej.: módulos interactivos sobre "Ciberseguridad móvil básica", con entrega de certificado como "Usuario con competencias verificadas en seguridad digital".

Beneficio:

Fortalece el aprendizaje a largo plazo y puede estar vinculado a incentivos (bonificaciones en planes, prioridad en atención al cliente).

d) Campañas educativas gamificadas en redes sociales y plataformas de mensajería

Descripción:

Formatos educativos lúdicos, como:

"Quiz de la semana" sobre fraudes comunes, mini historias interactivas tipo "Adivina el intento de estafa", concursos con premios.

Beneficio:

Mayor alcance en población joven y memorización emocional de los conceptos de seguridad.

e) Inclusión de contenidos de seguridad móvil en programas de inclusión digital

Descripción:

La CRC puede trabajar con ministerios, alcaldías y ONG para integrar contenidos sobre seguridad móvil en capacitaciones dirigidas a:

adultos mayores, comunidades rurales o población vulnerable.

Beneficio:

Llega a grupos con mayor riesgo de ser víctimas de fraude.

3. Recomendación para su implementación:

Las medidas deben estructurarse en tres niveles:

- Acciones reactivas (por ejemplo, alertas ante contenido sospechoso),
- Iniciativas preventivas (como certificaciones y juegos),
- Integración estructural en programas de educación e inclusión social.

La CRC debería crear un grupo de trabajo intersectorial permanente sobre educación al usuario, incluyendo:

- Operadores móviles,
- Organizaciones de defensa del consumidor,
- Bancos,
- Instituciones educativas,
- Medios públicos.

4. Conclusión:

Los mecanismos técnicos y regulatorios deben ser complementados por iniciativas de empoderamiento creativas, accesibles y respaldadas por toda la sociedad.

Solo si todos los grupos de usuarios comprenden cómo funciona el fraude y cómo identificarlo, será posible construir una protección sostenible frente a los ciberataques en el entorno móvil.

Pregunta 8:

¿Tiene sugerencias o recomendaciones para optimizar los procedimientos de asignación y retiro de recursos de identificación dentro del régimen de numeración?

1. Objetivo general:

Los procedimientos de asignación y retiro de recursos de identificación deben diseñarse en un marco regulatorio moderno que sea:

- transparente,
- eficiente,
- digitalmente automatizable,
- y basado en la responsabilidad,

con el fin de garantizar seguridad de los recursos, prevención de abusos y equidad en el acceso al mercado.

2. Sugerencias para optimizar los procesos de asignación:

a) Creación de un portal digital de autoservicio para todos los recursos numéricos

Desarrollo de una plataforma en línea gestionada por la CRC, en la que los actores autorizados puedan:

- Solicitar números,
- Declarar el propósito de uso,
- Subir documentación,
- Consultar estado de trámites,
- Gestionar renovaciones o devoluciones.

Ventajas:

Reduce tiempos y costos administrativos.

Permite trazabilidad completa y rutas de aprobación auditables.

b) Definición de categorías de uso con reglas de asignación estandarizadas

Cada número solicitado (corto, E.164 o alfanumérico) debe asociarse a una categoría predefinida:

- servicios financieros,
- comunicación gubernamental,
- campañas de marketing,
- autenticación de usuarios.

Ventajas:

Facilita el control de uso adecuado.

Mejora la protección contra el abuso al dar contexto a la solicitud.

c) Asignación con duración limitada y renovación obligatoria

Las asignaciones deben ser por un periodo fijo (por ejemplo, 12 o 24 meses).

Posteriormente, se requiere renovación con actualización de datos.

Ventajas:

Evita la acumulación o abandono de números.

Obliga a mantener la información actualizada.

d) Asignación sujeta a verificación previa del solicitante (modelo KYC)

Solo organizaciones con identidad verificada y responsabilidad legal pueden acceder a recursos.

Ventajas:

Aumenta la trazabilidad y reduce el anonimato.
Previene fraudes y suplantaciones.

3. Sugerencias para mejorar los procedimientos de retiro:

a) Retiro automático por inactividad o incumplimiento

Los recursos se revocan automáticamente si:

- No se usan en cierto tiempo,
- Se detectan violaciones a las reglas de uso (por ejemplo, spoofing, falta de actualización).

Ventajas:

Reduce cargas administrativas.
Libera recursos escasos para nuevas solicitudes legítimas.

b) Registro público del estado de los números

Una base de datos pública muestra:

- Números asignados,
- Organización titular,
- Finalidad y vigencia,
- Estado activo o inactivo.

Ventajas:

Fomenta confianza y validación.
Facilita control por parte de operadores y usuarios.

c) Sanciones y bloqueos temporales ante uso indebido o información falsa

Aplicación de sanciones claras (multas, bloqueos) en casos de:

- Uso fraudulento,
- Cesión no autorizada,
- Ocultamiento de identidad del usuario real.

4. Conclusión:

Optimizar los procesos de asignación y retiro de recursos de identificación es clave para la seguridad, la equidad y la eficiencia en el ecosistema digital.

Un sistema digitalizado, transparente y basado en responsabilidades, con criterios claros, obligaciones de uso y mecanismos de devolución, es esencial para gestionar de forma sostenible los recursos nacionales de numeración.