116751000G-0271

Bogotá D.C., 4 de agosto 2025.

Doctora
Claudia Ximena Bustamante
Directora Ejecutiva
Comisión de Regulación de Comunicaciones
atencioncliente@crcom.gov.co
Ciudad

Asunto: Comentarios al proyecto de identificación de medidas para mitigar el fraude por medio de servicios móviles.

Respetada Doctora Claudia,

En atención a la invitación para comentar el proyecto regulatorio "Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles", cuyo propósito es fortalecer los mecanismos de verificación para prevenir el contacto a usuarios a través de llamadas de voz y mensajes de texto (SMS) con fines presuntamente fraudulentos, me permito presentar los siguientes comentarios y recomendaciones, con el objetivo de aportar a la construcción de un marco regulatorio integral, eficaz y sostenible.

Magnitud y caracterización del problema del fraude cibernético:

Prevención SMS P2P:
A través de la herramienta Anti-Spam (implementada a partir de junio/24), estas son las cifras de SMS P2P irregulares que se evitaron que llegaran a los clientes

Año	Mes	Total SMS Evitados	Total SMS Aceptados	Total SMS
2024	6	129.117.342	40.760.092	169.877.434
	7	69.135.360	25.638.996	94.774.356
	8	19.114.071	17.832.127	36.946.198
	9	16.181.792	16.302.459	32.484.251
	10	11.322.209	15.643.261	26.965.470
	11	11.727.507	15.771.245	27.498.752
	12	7.392.898	18.210.575	25.603.473
Total 2024		263.991.179	150.158.755	414.149.934

Prevención SMS A2P:
Desde finales de dic/24 se empezó a evidenciar un incremento en los reportes de SMS de códigos cortos, con presunto fraude, por lo cual se realiza restricción preventiva de mensajes con presunta irregularidad:

Mes	Restricción Preventiva SMS Cod Corto
ene-25	19050
feb-25	1190211
mar-25	2676897
abr-25	4424466

Medidas tecnológicas y de ciberseguridad implementadas:

Monitoreos:
Tenemos 2 herramientas que nos permiten validar los SMS:

1) FMS (Hypersense), herramienta donde realizamos monitoreo diario de SMS P2P, en la cual se tienen configuradas unas reglas por tiempo y dispersión del mensaje para que nos alerte, tomando acciones oportunas como la suspensión de la línea si se detecta una irregularidad y
2) Herramienta Anti-Spam que filtra los SMS de P2P y A2P con contenido sospechoso o irregular, evitando que lleguen al usuario, en esta herramienta se evidencia la cantidad de mensajes enviados por un cliente y se puede realizar bloqueo por mensaje, línea móvil y mensajes que contengan URL sospechosos o presuntamente fraudulentas, etc. Si la herramienta detecta una irregularidad, realiza el bloqueo de los mensajes (mediante inteligencia Artificial).

Protocolos internos de respuesta a incidentes:
El procedimiento específico SEG-PO-01030003 establece y describe las actividades para tener una respuesta oportuna y eficiente cuando se presenten incidentes de seguridad que comprometan la información de Telefónica Colombia.

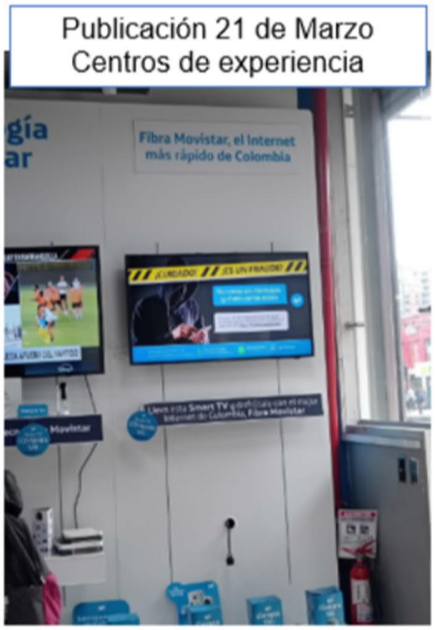
Programas basados en inteligencia artificial (IA), blockchain u otras tecnologías para prevenir el contenido fraudulento hacia nuestros clientes:
Se realiza proceso de takedown a dominios maliciosos usados en las campañas de Smishing, detectados en herramientas de ciberinteligencia y reportes de usuarios.

Medidas pedagógicas y de sensibilización:

Si han realizado campañas de educación a usuarios en los últimos 3 años, cómo fueron y qué canales usaron.
1. En la página de Movistar: https://atencionalcliente.movistar.co/seguridad/ , encontré información sobre estas modalidades: Smishing, Phishing, cuidados que se deben tener, ejemplos, etc

También en la página de Facebook:

Centros de Experiencia:



Al margen de la campaña, hay otras acciones que se están trabajando por distintas áreas:

1. Sistema de reporte de fraude por SMS, líneas y enlaces (links). Desde septiembre de 2024, se habilitó un canal interno para reportar incidentes relacionados con códigos SMS, líneas sospechosas y enlaces maliciosos. Esta herramienta permite una trazabilidad más ágil y fortalece la capacidad de respuesta ante intentos de fraude.

2. Campaña informativa a clientes sobre canales oficiales. Activa desde diciembre, esta campaña busca educar a los usuarios sobre los canales legítimos de contacto, reduciendo la probabilidad de que caigan en fraudes por suplantación.

3. Pop-up en la App Mi Movistar con consejos de prevención. Desde marzo, se desplegó un mensaje emergente en la aplicación móvil con recomendaciones prácticas para evitar fraudes. Esta acción apunta a la sensibilización directa del cliente en el punto de contacto digital.

4. Doble factor de autenticación en las plataformas internas. En producción desde el 8 de marzo, esta medida refuerza la seguridad en el acceso a las diferentes plataformas, especialmente para operaciones sensibles o de alto impacto.

5. Nuevo modelo de ajustes B2B con aprobador. Implementado en marzo, este modelo introduce un flujo de aprobación para ajustes en el segmento B2B, fortaleciendo los controles internos y reduciendo el riesgo de manipulaciones indebidas.

Propuestas sobre alternativas de intervención de la CRC:

1. Fortalecimiento de la coordinación interinstitucional

Se recomienda desplegar una estrategia sólida de articulación entre la CRC y entidades clave como la Policía Nacional, el Ministerio TIC, la Superintendencia de Industria y Comercio, así como autoridades locales, con el objetivo de consolidar una respuesta integral frente al fraude cibernético en servicios móviles. Esta coordinación debe contemplar mecanismos efectivos de intercambio de información, protocolos claros para la actuación conjunta y campañas de prevención que estén alineadas entre todas las partes involucradas.

2. Restringir el envío de URLs por SMS

Se recomienda restringir o prohibir el envío de enlaces (URLs) a través de mensajes de texto (SMS), debido a la dificultad técnica de verificar su autenticidad en tiempo real y al alto riesgo que representan en términos de suplantación de identidad, robo de datos personales y fraudes financieros. Esta medida busca reducir la exposición de los usuarios a ataques de smishing, una modalidad de fraude que ha demostrado ser altamente efectiva y rentable para los delincuentes.

3. Campañas de educación y sensibilización

Se recomienda implementar campañas masivas y sostenidas en medios tradicionales (radio, televisión, prensa) y digitales (redes sociales, plataformas móviles, sitios web institucionales) para informar a los usuarios sobre las modalidades de fraude como el smishing y el vishing. Estas campañas deben incluir ejemplos reales, mensajes de alerta, consejos prácticos y canales de denuncia directa. Es fundamental que estas acciones sean accesibles, continuas y adaptadas a distintos perfiles de usuarios, incluyendo poblaciones vulnerables o con baja alfabetización digital.

4. Responsabilidad de IT, PCA y generadores de contenido.

Se propone establecer un marco regulatorio claro y exigente para los integradores de mensajería (SMS aggregators) y proveedores de contenido (PCAs), que los responsabilice directamente por la prevención del fraude cibernético en el canal de mensajería móvil. Esto incluye:

- La obligación de implementar controles técnicos robustos para detectar patrones irregulares en el tráfico de mensajes, como envíos masivos no autorizados, URLs sospechosas o remitentes no verificados.
- La creación de mecanismos de auditoría periódica, trazabilidad de campañas y sanciones proporcionales en casos de reincidencia o negligencia que facilite el fraude.

La creación de un marco regulatorio robusto y vinculante que promueva la cooperación efectiva entre operadores móviles, integradores tecnológicos (IT), proveedores de contenido (PCA), generadores de contenido, entidades usuarias de códigos cortos y autoridades regulatorias representa un paso decisivo en la mitigación del fraude cibernético en servicios móviles. Actualmente, la ausencia de obligaciones explícitas para que los PCA e IT respondan ante alertas de comportamiento sospechoso limita gravemente la capacidad de reacción frente a incidentes de fraude, y fragmenta la trazabilidad de los mensajes en la cadena de valor.

Por ello, se propone que todos los actores involucrados estén sujetos a mecanismos de trazabilidad técnica, control operativo y responsabilidad compartida, incluyendo metodologías rigurosas para identificar el origen de los mensajes, verificar la legitimidad de los remitentes y sancionar a quienes faciliten el uso indebido de los canales móviles. Esta trazabilidad debe extenderse también a los generadores de contenido, quienes desempeñan un rol activo al utilizar los canales móviles para transmitir mensajes a sus audiencias. Su inclusión en los mecanismos de seguimiento y control es esencial para cerrar brechas de responsabilidad y prevenir el uso malicioso de sus campañas.

5. Herramientas tecnológicas y trazabilidad para Combatir el Fraude por SMS

Las propuestas de implementar identificadores alfanuméricos únicos, bloqueo inmediato de remitentes no autorizados y herramientas de detección en tiempo real representan medidas fundamentales para fortalecer la seguridad en las comunicaciones por SMS. Estas iniciativas se alinean con tendencias internacionales y tecnologías emergentes que están transformando la lucha contra el fraude.

Implementar identificadores alfanuméricos únicos por entidad.

Base de Datos Centralizada de Identificadores

La implementación de identificadores alfanuméricos únicos requiere el establecimiento de una base de datos centralizada gestionada por la autoridad regulatoria. Este modelo, inspirado en la experiencia española donde la CNMC gestiona el registro de alias alfanuméricos, permite:

- Registro y validación de entidades autorizadas para usar identificadores específicos
- Trazabilidad completa de cada mensaje hasta su origen legítimo
- Verificación automática de la autenticidad del remitente antes del envío

En Colombia, la CRC ya tiene experiencia regulando códigos cortos numéricos, pero la normativa actual no contempla identificadores alfanuméricos para SMS comerciales. La transición hacia este sistema requeriría actualizar el marco regulatorio para incluir:

- Procedimientos de registro para empresas que deseen usar Sender ID alfanuméricos
- Criterios de elegibilidad y documentación requerida
- Mecanismos de revocación por uso indebido

Permitir el bloqueo inmediato de remitentes no autorizados o mensajes con enlaces maliciosos.

Sistemas de Filtrado en Tiempo Real

Las tecnologías modernas permiten implementar sistemas de bloqueo automático que operan en múltiples niveles:

Filtrado a Nivel de Operador

- Validación de identificadores: Comparación automática contra la base de datos centralizada
- Bloqueo de números no asignados: Prevención del uso de numeración no autorizada
- Detección de origen internacional: Bloqueo de mensajes que simulan origen nacional siendo internacionales

6. Portal público y transparencia

Se propone la creación de un portal público de consulta ciudadana que centralice información sobre casos reportados de fraude cibernético, estadísticas actualizadas, herramientas de verificación de mensajes y remitentes, y canales de denuncia directa. Este portal debe ser accesible, interoperable con otras plataformas estatales y contar con funcionalidades que permitan a los usuarios verificar si un número, código corto o mensaje ha sido reportado como fraudulento. Además, debe incluir mecanismos para que las entidades usuarias de códigos cortos y los generadores de contenido puedan consultar alertas, reportes y recomendaciones regulatorias.

Quedamos atentos a cualquier aclaración adicional mediante el correo electrónico regulacion.colombia@telefonica.com

Cordialmente,

(Original firmado)
MARIA FERNANDA BERNAL
Directora de Asuntos Públicos y Regulatorios
COLOMBIA TELECOMUNICACIONES S.A. ESP BIC