Fraude por SMS y Ciberamenazas en las Telecomunicaciones Móviles de América Latina

Un análisis regional del panorama de amenazas, su magnitud económica y un marco de recomendaciones técnicas para operadores, reguladores e industria

Introducción

GMS es una empresa de soluciones de telecomunicaciones con sede en Suiza y más de veinte años de experiencia internacional en mensajería y protección de redes. Estamos conectados directamente con más de 275 operadores de redes móviles en 200 países y mantenemos relaciones comerciales de larga data con importantes plataformas globales como META, Google y TikTok. Actualmente, gestionamos 37 proyectos de servicios administrados en 25 países y hemos implementado con éxito programas de pasarelas a nivel nacional en Asia, con despliegues en curso en Latinoamérica y África.

GMS se complace en presentar a consideración de la CRC el presente documento que tiene la intención de mostrar el estado actual del fraude por SMS y ciberamenazas en las telecomunicaciones móviles de América Latina, así como con base en nuestra amplia experiencia global, sugerir medidas tecnoloógicas y operativas para que el ecosistema colombiano de telecomunicaciones, incremente su seguridad de cara a los suscriptores y a los operadores móviles, lo cual en consecuencia traerá enormes beneficios a la industria y sociedad colombiana.

Resumen Ejecutivo

América Latina enfrenta una escalada sin precedentes en el fraude digital a través de SMS y llamadas de voz. En Colombia, las reclamaciones por estas modalidades superan los COP $252 millones diarios y se triplicaron en dos años. A nivel global, las pérdidas asociadas al fraude por SMS alcanzaron los USD 80 mil millones en 2025. La Comisión de Regulación de Comunicaciones (CRC) de Colombia ha publicado una propuesta regulatoria que aborda aspectos críticos de identificación y trazabilidad; sin embargo, este análisis sostiene que la efectividad de dicha propuesta puede potenciarse con un conjunto de medidas técnicas complementarias a nivel de operador y de red cuya implementación coordinada representaría una reducción estimada del 70-95% en el volumen de tráfico fraudulento.

Contexto y Planteamiento del Problema Regional

Hallazgo 1

América Latina registró más de 286 millones de intentos de phishing en 2023, con un incremento del 140% en estafas basadas en mensajes en 2024, posicionándola como la región de mayor crecimiento para esta tipología de amenaza.

Hallazgo 2

La infraestructura de señalización SS7, columna vertebral de las redes 2G/3G aún prevalentes en gran parte de la región, presenta vulnerabilidades estructurales que permiten la interceptación de SMS y la suplantación de identidad sin detección en tiempo real.

La telefonía móvil se ha convertido en el vector de ataque preferido por actores maliciosos en América Latina, desplazando al correo electrónico como principal canal de fraude. Este fenómeno resulta de una conjunción de factores: la alta tasa de penetración móvil en la región (superior al 80% en la mayoría de los países), la relativamente baja madurez de la cultura de ciberseguridad en la población general, y el alto grado de confianza depositado en el canal SMS, que registra tasas de apertura de hasta el 98%.

El smishing (derivado de SMS y phishing) y el vishing (phishing por voz) representan las dos modalidades de mayor crecimiento. En el primero, el usuario recibe un mensaje de texto que simula provenir de una entidad legítima (banco, mensajería, organismo gubernamental) que contiene un enlace malicioso o una solicitud de información sensible. En el segundo, la llamada telefónica es el vector, con delincuentes que se hacen pasar por representantes de empresas reconocidas para obtener credenciales o inducir transferencias bancarias.

La sofisticación de los ataques ha aumentado considerablemente. Los grupos criminales organizados utilizan plataformas de Fraude como Servicio (FaaS) que permiten lanzar campañas de smishing a escala industrial con una inversión técnica mínima, aprovechando las vulnerabilidades del protocolo de señalización SS7 y la ausencia de mecanismos de autenticación del remitente en la mayoría de las redes móviles de la región.

Tabla 1. Crecimiento del Fraude por SMS en Países Seleccionados de América Latina (2024)

País	Crecimiento Anual (%)	Modalidad Predominante	Clasificación Regional
Peru	+360%	Smishing / Mensajería falsa	Criticidad alta
Argentina	+300%	Vishing / Suplantación bancaria	Criticidad alta
Brazil	+267%	Smishing / Interceptación de OTP	Criticidad alta
Chile	+125%	Smishing A2P fraudulento	Criticidad media-alta
Colombia	+120%	Smishing + Vishing combinado	Criticidad media-alta
Mexico	Mayoría regional (55%)	Ransomware + Smishing	Criticidad alta

Fuente: Kaspersky Security Bulletin 2025; Proofpoint State of the Phish 2024. Los porcentajes representan el incremento interanual en intentos bloqueados.

Análisis de Magnitud Económica

Hallazgo 3

Las pérdidas globales por fraude de SMS se estimaron en USD 80 mil millones en 2025 (Juniper Research), con América Latina representando aproximadamente el 11% del total del cibercrimen mundial.

Hallazgo 4

En Colombia, las reclamaciones por smishing y vishing se triplicaron en dos años — de COP $30.622 millones a COP $92.235 millones — con un costo diario que supera los COP $252 millones según la CRC.

El análisis económico del fraude por SMS debe distinguir entre impacto directo (pérdidas efectivamente reclamadas y recuperadas) e impacto indirecto, que incluye costos de oportunidad, deterioro de la confianza en el ecosistema digital, costos operativos de gestión del fraude y el impacto en la adopción de servicios digitales entre poblaciones vulnerables.

A nivel global, el ecosistema de fraude por SMS representa una industria criminal de USD 80 mil millones anuales (2025), con proyecciones de reducción a USD 71 mil millones en 2026 como resultado de firewalls mejorados y reducción del tráfico de mensajería empresarial (Juniper Research, noviembre de 2025). Sin embargo, estas cifras globales subestiman el impacto real en economías emergentes como las de América Latina, donde los mecanismos de denuncia y cuantificación son menos maduros.

El caso colombiano es paradigmático por la calidad de los datos disponibles gracias al trabajo de la CRC. La cifra de COP $252 millones en reclamaciones diarias equivale a más de USD 60.000 por día solo en Colombia (un país de 52 millones de habitantes) que al proyectarse a escala regional sugiere pérdidas de cientos de millones de dólares anuales para América Latina en su conjunto. Las pérdidas totales por cibercrimen en Colombia superaron los USD 800 millones en 2024.

Tabla 2. Impacto Económico del Fraude por SMS — Perspectiva Multinivel

Nivel	Indicador	Valor Estimado	Fuente
Global	Pérdidas anuales por fraude SMS (2025)	USD 80 billion	Juniper Research
Global	Proyección 2026	USD 71 billion	Juniper Research
Global	Pérdida por minuto (cibercrimen)	USD 20 million	INTERPOL 2026
LATAM	Participación en el cibercrimen global	~11%	Estimación del sector
LATAM	Intentos de phishing bloqueados (2024)	+697 million	Kaspersky
Colombia	Reclamaciones diarias (SMS/voz)	COP $252M / ~USD 60K	CRC 2026
Colombia	Reclamaciones smishing+vishing (2024)	COP $92.235 million	CRC 2026
Colombia	Pérdidas totales por cibercrimen (2024)	USD 800 million	Prey Project

Fuente: CRC Colombia — Regulatory Proposal June 2026; Juniper Research; Kaspersky Security Bulletin 2025; INTERPOL Cybercrime Report Mar. 2026.

Marco de Recomendaciones Técnicas

La propuesta regulatoria de la CRC articula medidas necesarias y pertinentes en materia de identificación del remitente, monitoreo del tráfico y coordinación intersectorial. Este análisis complementa ese marco con recomendaciones técnicas a nivel de operador y de red, organizadas por su capa de implementación dentro del ecosistema de telecomunicaciones móviles.

3.1 Capa de Red y Señalización

Las vulnerabilidades a nivel de señalización constituyen el vector de mitigación más difícil debido a su naturaleza sistémica y la complejidad de actualizar la infraestructura legada. Las siguientes recomendaciones operan en esta capa.

3.2 Capa de Aplicación y Mensajería

En la capa de aplicación, las medidas se centran en el control del ecosistema A2P y la verificación de la legitimidad del remitente, complementando la propuesta de la CRC sobre identificadores SMS visibles.

3.3 Capa de Inteligencia y Coordinación

La efectividad de las medidas técnicas se multiplica cuando existe un marco de intercambio de inteligencia sobre amenazas entre los actores del ecosistema. Esta capa complementa directamente al Comité Técnico propuesto por la CRC.

Tabla 3. Marco de Recomendaciones Técnicas complementario a la Propuesta Normativa de la CRC.

Recomendación	Detalle
Firewall de SMS con Clasificación IA/ML	Desplegar firewalls de SMS con algoritmos de IA/ML para interceptar tráfico SMPP y SS7. Cobertura en red, fuera de red y roaming. Reducción estimada del 70-95% en tráfico fraudulento en tiempo real.
Firewall de Señalización SS7 y Diameter	Filtrado de mensajes SS7 maliciosos (MAP SRI, PSI) en puntos de interconexión. Extensión a Diameter en redes 4G/5G. Mitiga la interceptación de OTP, el rastreo de ubicación y la redirección fraudulenta de SMS.
Firewall de Voz	Garantizar únicamente tráfico legal en los canales de voz, reduciendo llamadas Flash/texto a voz y otros tipos de fraude como CLI Spoofing, Wangiri, bypass de voz internacional y otros
Gateway Centralizado de Mensajería A2P	Permitir la visibilidad de los SMS A2P internacionales del regulador instalando un SMSC en las instalaciones del regulador para procesar y entregar el tráfico a todos los operadores.
Firewall de Datos	Garantizar la entrega adecuada de mensajes OTP internacionales a través del canal SMS legal, en lugar de los canales OTT de RCS y WhatsApp
API de Red	Habilitar solicitudes de empresas globales para capacidades basadas en la red: verificación de número, detección de cambio de SIM, localización de dispositivo, calidad bajo demanda
Canal de Reporte Ciudadano Integrado con el Firewall	Canal estandarizado de reporte de SMS fraudulentos (p. ej., número corto 7726) cuyos reportes alimentan automáticamente las reglas del firewall de SMS y listas negras compartidas entre operadores.

Análisis de Beneficios e Impacto Esperado

La adopción coordinada del marco de recomendaciones técnicas descritas generaría impactos positivos cuantificables en las dimensiones operativa, económica, regulatoria y de confianza digital. El siguiente análisis proyecta los beneficios esperados más significativos:

Tabla 4. Matriz de Beneficios por Dimensión de Impacto

Beneficio	Impacto Esperado
Reducción del fraude en tiempo real (70-95%)	Los firewalls de SMS con inteligencia de amenazas compartida reducen el tráfico fraudulento antes de que llegue al usuario, con tasas de bloqueo documentadas de entre el 70% y el 95% en implementaciones de referencia (GSMA 2025).
Restauración de la confianza en el canal SMS	La verificación del remitente A2P restaura la credibilidad del SMS como canal legítimo, revirtiendo la tendencia de rechazo de mensajes institucionales. Impacto directo en la adopción de la banca digital y el gobierno electrónico.
Cumplimiento regulatorio proactivo y reducción de sanciones	La implementación temprana de medidas técnicas posiciona a los operadores en cumplimiento con la propuesta de la CRC y los estándares internacionales (3GPP TS 33.117, GSMA FS.07), reduciendo el riesgo de sanciones y fortaleciendo su posición en auditorías regulatorias.
Diferenciación competitiva y protección de ingresos A2P	Los operadores que ofrezcan SMS verificado y seguro se posicionarán como socios preferidos para empresas de alto valor (sector financiero, gobierno, salud). Protección de ingresos A2P frente a la competencia de canales OTT.
Impacto multiplicador en la inclusión financiera digital	Un ecosistema de mensajería segura con API de Red habilitada reduce las barreras para la adopción de servicios financieros digitales y pagos móviles, especialmente en segmentos de la población que dependen de los SMS como canal de acceso principal.
Reducción de costos operativos directos e indirectos	Reducción en costos de atención al cliente, litigios y gestión de fraude por suplantación de marca. Para los operadores, eliminar el tráfico de rutas grises libera capacidad de red y reduce los costos de interconexión.

Los porcentajes de reducción del fraude provienen de benchmarks de la industria documentados en implementaciones similares en Europa y Asia-Pacífico (GSMA Fraud Intelligence Report 2025).

V. Conclusiones y Recomendaciones Finales

La propuesta regulatoria de la CRC representa un avance significativo y necesario para el ecosistema colombiano y puede servir de modelo para otros reguladores de la región. La combinación de identificadores de remitente verificados, monitoreo del tráfico y la creación de un Comité Técnico Antifraude constituye una base sólida sobre la que construir.

Sin embargo, el análisis presentado en este documento sugiere que la máxima efectividad de estas medidas regulatorias depende de ser complementadas con intervenciones técnicas en las capas de red, aplicación e inteligencia de amenazas. Un enfoque fragmentado (regulación sin implementación técnica profunda, o tecnología sin coordinación sectorial) limita estructuralmente el impacto sobre la amenaza.

El marco técnico de ocho recomendaciones propuesto en este análisis opera en capas complementarias a la propuesta regulatoria y puede ser adoptado incrementalmente por los operadores, priorizando medidas con la mayor relación costo-beneficio: el Firewall SMS (R1), Firewall de Voz, SS7/Protección de señalización de diámetro (R2), Firewall de Datos y el Gateway de mensajería A2P centralizado representan el conjunto mínimo viable con impacto inmediato.

El costo de la inacción es conocido: COP $252 millones diarios en Colombia; potencialmente miles de millones de dólares anuales en el agregado regional. La ventana de oportunidad para implementar estas medidas con liderazgo regulatorio es precisamente la que define la propuesta de la CRC, con comentarios públicos abiertos hasta el 23 de junio de 2026.

Referencias

[1] Comisión de Regulación de Comunicaciones (CRC). (2026, junio). Propuesta Regulatoria: Identificación de medidas para mitigar el fraude por cibercrimen a través de servicios móviles. Proyecto 2000-41-7-1. Bogotá: CRC.

[2] Kaspersky Lab. (2025). Kaspersky Security Bulletin 2025: El panorama del phishing en América Latina. Moscú: Kaspersky.

[3] Proofpoint. (2024). State of the Phish 2024: Un análisis profundo de la conciencia, vulnerabilidad y resiliencia del usuario. Sunnyvale: Proofpoint Inc.

[4] Juniper Research. (2025, noviembre). Las pérdidas por fraude SMS alcanzarán los 71.000 millones de dólares en 2026. Hampshire: Juniper Research Ltd.

[5] INTERPOL. (2026, marzo). Panorama de amenazas del cibercrimen: América Latina 2025-2026. Lyon: Secretaría General de INTERPOL.

[6] GSMA. (2025). GSMA Fraud Intelligence: Informe de Referencia sobre Fraude SMS 2025. Londres: GSM Association.

[7] Prey Project. (2025). Estadísticas de ciberseguridad en Chile, México y Colombia 2024-2025. Santiago: Prey.

[8] 3GPP. (2023). TS 33.117: Catálogo de requisitos generales de garantía de seguridad. Release 18. Sophia Antipolis: 3GPP.