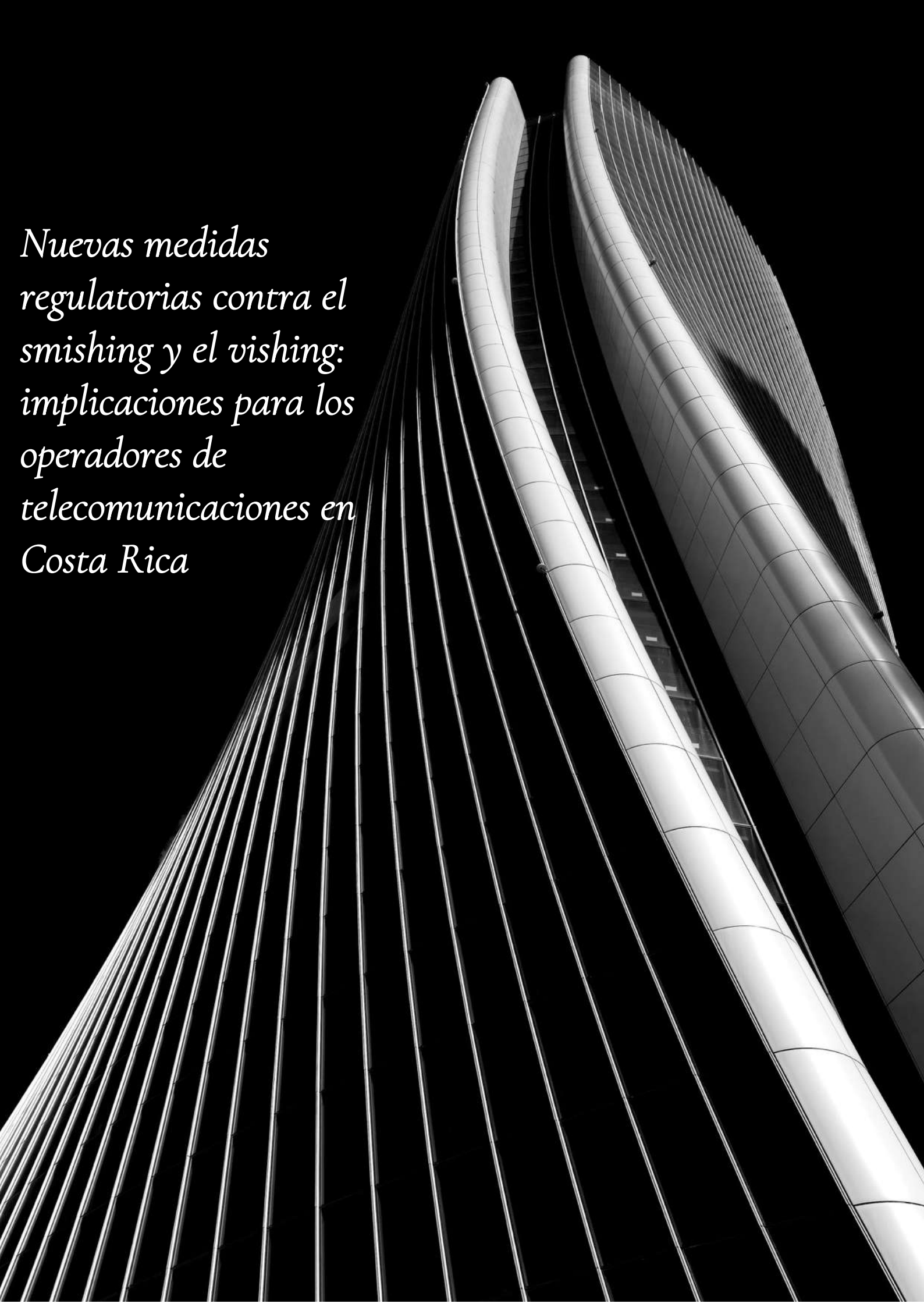


Nuevas medidas regulatorias contra el smishing y el vishing: implicaciones para los operadores de telecomunicaciones en Costa Rica

SUTEL aprobó el 18 de junio de 2026, las medidas regulatorias más completas adoptadas hasta la fecha en Costa Rica para combatir los ciberataques mediante mensajes de texto SMS (smishing) y llamadas telefónicas fraudulentas (vishing). La resolución impone obligaciones vinculantes a todos los operadores y proveedores de servicios de telecomunicaciones.

Índice

Objeto y alcance de la regulación

La resolución RCS-151-2026 fue adoptada por el Consejo de la SUTEL mediante acuerdo 021-035-2026 en la sesión ordinaria 035-2026 del 18 de junio de 2026. Se trata de una resolución de carácter general que complementa y amplía la resolución RCS-294-2023, que regulaba exclusivamente el enmascaramiento de llamadas, para abarcar ahora también la mensajería de texto SMS en sus modalidades P2P (persona a persona) y A2P (aplicación a persona). Fue publicada en el Alcance N° 83 a La Gaceta N° 119 del 29 de junio de 2026.

La resolución responde al incremento exponencial de los fraudes mediante smishing y vishing. Según los datos citados, los ataques por smishing aumentaron hasta 14 veces a nivel global en 2025, con un crecimiento especialmente pronunciado en Latinoamérica. En Costa Rica, durante 2024, los operadores reportaron el bloqueo de más de 2,5 millones de llamadas enmascaradas, y durante 2025, la SUTEL solicitó a Liberty Telecomunicaciones la suspensión de más de 30 servicios en 15 ocasiones por prácticas prohibidas mediante SMS.

La resolución encuentra su fundamento jurídico en la Ley General de Telecomunicaciones (Ley 8642), en su artículo 2 inciso f), que establece como objetivo promover el uso de los servicios de telecomunicaciones como apoyo a la seguridad ciudadana; en el artículo 42, que impone a los operadores la obligación de adoptar medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes; y en la Ley de la Autoridad Reguladora de los Servicios Públicos (Ley 7593), que otorga a la SUTEL competencia para regular, vigilar y controlar el ordenamiento jurídico de las telecomunicaciones.

Principales obligaciones para los operadores

En materia de mensajería SMS (P2P y A2P)

- Implementar mecanismos técnicos y administrativos para asegurar la trazabilidad del tráfico SMS desde el origen hasta el destino, bloqueando todo tráfico identificado como malicioso, no trazable o que intente evadir filtros de seguridad, incluyendo mensajes con origen internacional que simulen ser locales.
- Implementar **firewalls de SMS con capacidad de inspección profunda de paquetes (DPI)**, exclusivamente para identificar comunicaciones maliciosas, con prohibición expresa de procesar el contenido para fines distintos y obligación de destruir los datos una vez cumplido su cometido.
- Verificar la identidad de los clientes de mensajería A2P y la finalidad del uso pretendido, garantizando que solo empresas legítimas se encuentren en los registros autorizados, los cuales deben compartirse entre operadores interconectados.
- Utilizar sistemas de reputación de enlaces para bloquear mensajes que contengan vínculos a sitios web maliciosos o de dudosa procedencia.
- Presentar informes cuatrimestrales con la cantidad de mensajes SMS identificados como maliciosos (smishing) y sus bloqueos, diferenciando entre P2P y A2P. Conservar los registros detallados por un plazo mínimo de cuatro (4) años, conforme al artículo 52 del RPUF.
- Disponer de Centros de Atención al Usuario Final para la recepción de reportes de smishing.

En materia de servicios de voz (vishing)

- Adoptar e implementar el estándar **Out-of-Band SHAKEN (OOBS)** para la autenticación de todas las llamadas (especificación ATIS-1000096). Con esta medida, Costa Rica se convierte en uno de los primeros países de América Latina en adoptar formalmente este estándar internacional, que se extiende también a redes TDM.

- Destinar un rango de números telefónicos para la implementación de señuelos (honeypots) que faciliten identificar generadores de spam y llamadas fraudulentas.
- Presentar informes cuatrimestrales con la cantidad de llamadas identificadas como maliciosas (vishing) y sus bloqueos, y conservar los registros detallados por un plazo mínimo de cuatro años.

Sobre la trazabilidad de las comunicaciones

La resolución define operativamente la trazabilidad como la capacidad del operador de identificar, autenticar, correlacionar y registrar de forma confiable el origen, la ruta de transmisión y el destino de cada comunicación. Un mensaje SMS se considerará trazable cuando su origen pueda ser inequívocamente determinado y validado, ya sea como tráfico P2P asociado a un usuario final legítimo o como tráfico A2P proveniente de un agregador previamente registrado y autorizado. Los operadores están facultados para bloquear, rechazar o etiquetar llamadas cuya trazabilidad no pueda ser garantizada.

Plazos de implementación

La resolución establece una implementación gradual dividida en tres fases a partir de la fecha de publicación (29 de junio de 2026):

- Fase 1 (180 días / 6 meses): Implementación de medidas básicas en SMS: trazabilidad, bloqueo de tráfico sin atributos de identificación, diferenciación P2P/A2P, bloqueo de tráfico internacional enmascarado, verificación en tiempo real, detección de umbrales anómalos, bloqueo de enlaces maliciosos, informes cuatrimestrales, conservación de registros por 4 años, registro de excepciones A2P y centros de atención al usuario. Se incluyen asimismo las obligaciones básicas en materia de voz: señuelos, informes y registros.

- Fase 2 (12 meses): Implementación de medidas avanzadas: firewalls SMS con inspección profunda de paquetes (DPI), verificación de identidad de clientes A2P, registro y validación de plantillas A2P, e intercambio de información entre operadores y proveedores.

- Fase 3 (18 meses): Implementación del estándar Out-of-Band SHAKEN (OOBS) para la autenticación de todas las llamadas de voz.

Aspectos jurídicos relevantes

Tensión entre la inspección DPI y las garantías constitucionales

La implementación de la inspección profunda de paquetes (DPI) sobre el tráfico de mensajes SMS constituye uno de los aspectos jurídicamente más sensibles de la resolución. El artículo 24 de la Constitución Política consagra la inviolabilidad de las comunicaciones escritas, orales o de cualquier otro tipo. A su vez, el artículo 42 de la Ley General de Telecomunicaciones establece que los operadores deberán garantizar que las comunicaciones y los datos de tráfico asociados no serán escuchados, grabados, almacenados, intervenidos ni vigilados por terceros sin su consentimiento, salvo autorización judicial.

La resolución mitiga esta tensión mediante tres salvaguardas: (i) prohibición de procesar el contenido del tráfico SMS para fines distintos a los especificados; (ii) procesamiento mediante sistemas automatizados en tiempo real; y (iii) obligación de destruir los datos una vez cumplido el cometido del firewall.

En el derecho comparado europeo, varias jurisdicciones han optado por establecer una excepción legal expresa a la confidencialidad de las comunicaciones para habilitar el procesamiento mecánico de SMS con fines antifraude.

Protección de datos personales

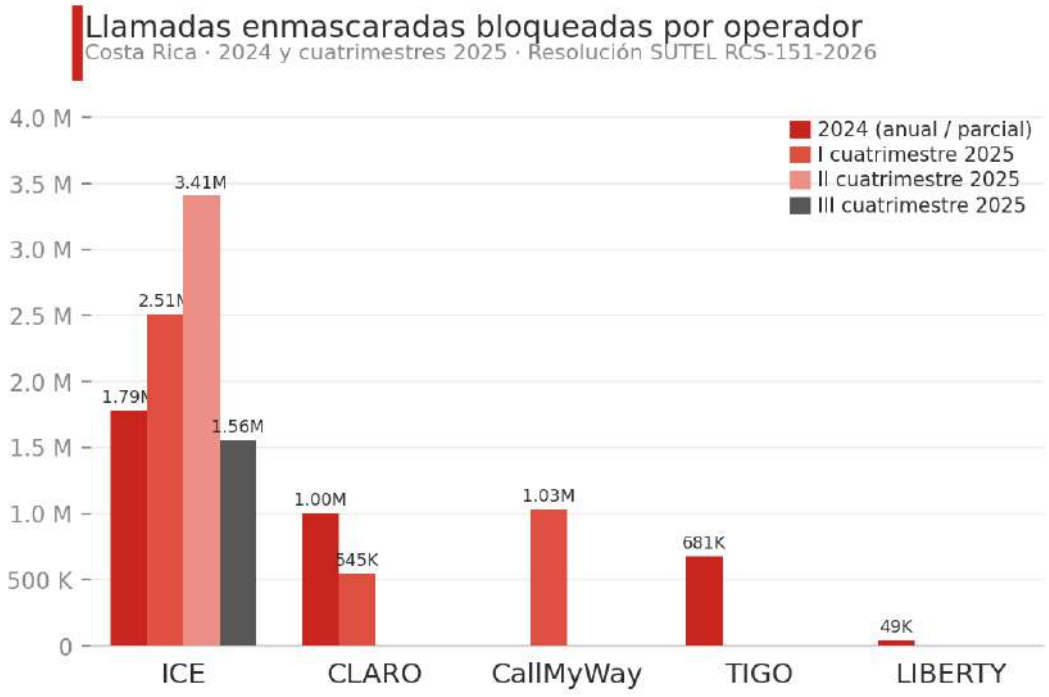
La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Ley 8968) y su Reglamento (Decreto Ejecutivo 37554-JP) imponen obligaciones de seguridad, confidencialidad y minimización en el tratamiento de datos personales. La conservación obligatoria de registros de comunicaciones por cuatro años y el procesamiento mediante DPI deben analizarse a la luz de los principios de finalidad, proporcionalidad y calidad previstos en la ley.

Proporcionalidad regulatoria

La exigencia simultánea de reportes cuatrimestrales, conservación de registros por cuatro años, firewalls SMS con DPI, estándar OOBS y registro y validación de clientes A2P puede generar una carga significativa para operadores de menor tamaño. El diseño escalonado en tres fases mitiga parcialmente este riesgo, pero el impacto económico deberá evaluarse cuidadosamente por cada operador.

Datos clave de bloqueo

Los datos reportados por los operadores durante el proceso regulatorio, e incluidos en la resolución de SUTEL, evidencian la magnitud del problema que la resolución busca abordar:



Nota: TIGO y LIBERTY reportaron cifras anuales 2024. CLARO reportó Sep–Dic 2024 y I cuatrimestre 2025. CallMyWay reportó cifra acumulada al 30 de abril de 2025. Las cifras no incluyen tráfico SMS malicioso.
Fuente: Resolución RCS-151-2026, SUTEL.

En total, solo en materia de llamadas enmascaradas, los operadores costarricenses reportaron el bloqueo de **más de 11 millones de llamadas** entre 2024 y el primer semestre de 2025. Estas cifras no incluyen el tráfico de mensajes SMS maliciosos, respecto del cual la regulación anterior no imponía obligaciones de reporte.

Próximos pasos y cómo podemos ayudarle

Desde ÉCIJA Costa Rica damos seguimiento permanente a los desarrollos regulatorios en materia de telecomunicaciones y ciberseguridad. Nuestro equipo puede asistirle en:

- Análisis del impacto de la resolución RCS-151-2026 en las operaciones de los operadores y proveedores de servicios de telecomunicaciones.
- Evaluación de la compatibilidad de las medidas de DPI con las garantías constitucionales y el marco de protección de datos personales (Ley 8968).
- Asesoramiento en el diseño e implementación de los planes de cumplimiento para las tres fases de la resolución.
- Revisión de contratos de interconexión y acuerdos con agregadores de mensajería A2P a la luz de las nuevas obligaciones regulatorias.
- Asistencia en la elaboración de los informes cuatrimestrales y protocolos de atención al usuario exigidos por la resolución.
- Representación ante la SUTEL en procedimientos de consulta, cumplimiento o impugnación.

Para más información:

Mauricio París | SOCIO

Prácticas de TMT y Digital Defense · mparis@ecija.com

El presente comunicado tiene carácter informativo y no constituye asesoramiento jurídico.

Desde ECIJA, quedamos a su disposición ante cualquier consulta relacionada con esta materia.