Bogotá D.C. 3 de julio de 2025

Doctora
CLAUDIA XIMENA BUSTAMANTE
Directora Ejecutiva
Comisión de Regulación de Comunicaciones
Correos: atencioncliente@crcom.gov.co; medidasantifraude@crcom.gov.co
Bogotá, D.C

Asunto: Alcance al documento remitido a la CRC el día 19 de mayo de 2025 al correo electrónico *medidasantifraude@crcom.gov.co* con el asunto *"Propuesta técnica y jurídica en el marco del proyecto "**Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles**" de la Agenda Regulatoria CRC 2025–2026: Migración a enlaces dedicados en conexiones PCA–PRST como medida antifraude en servicios SMS"*

Respetada Doctora Bustamante:

DIEGO DAMIAN VALDIVIESO PIFNILLA mayor de edad, identificado con la cédula de ciudadanía **80.876.160** expedida en Bogotá, obrando en calidad de Apoderado General de **HABLAME COLOMBIA S.A. E.S.P**. sociedad identificada con NIT 900.994.857-4, me permito dar alcance a la comunicación indicada en el asunto con el propósito de exponer un aspecto adicional que no incluimos en nuestro documento inicial.

En atención al proceso que actualmente adelanta la CRC para fortalecer las medidas de prevención del fraude por medio de mensajes de texto, como empresa prestadora de servicios de mensajería SMS (Integrador Tecnológico), nos permitimos elevar una respetuosa sugerencia:

Primero: Consideramos fundamental que se adopte una medida regulatoria que exija que la transmisión de mensajes de texto entre integradores tecnológicos y PRSTM se realice exclusivamente a través de canales punto a punto no expuestos a Internet, tales como enlaces dedicados o redes privadas (MPLS).

Segundo: Esta recomendación no está relacionada con la mitigación del smishing, sino con la prevención de la interceptación de mensajes en tránsito, dado que actualmente muchos de estos mensajes viajan por canales públicos. Esto

representa una vulnerabilidad grave, ya que los SMS suelen contener información altamente sensible como contraseñas, códigos OTP y datos personales.

Tercera: La CRC ya ha exigido canales cerrados para la transmisión de llamadas telefónicas, reconociendo los riesgos de exponer las comunicaciones a Internet. Solicitamos que esta misma lógica se aplique a los mensajes de texto, anticipándose a una modalidad de ciberdelito que aún no es común, pero cuya ocurrencia puede ser inminente en el contexto actual de aumento de ataques informáticos.

Cuarto: Reconocemos que uno de los principios fundamentales de la CRC es proteger y salvaguardar la seguridad de los usuarios de servicios de telecomunicaciones. En ese marco, proponemos una regulación que exija que la transmisión de mensajes de texto entre integradores tecnológicos y operadores móviles se realice exclusivamente por canales punto a punto no expuestos a Internet, como redes privadas dedicadas (ej. MPLS).

Riesgo real - Intercepción y ciberdelitos

Actualmente, muchos SMS circulan por redes públicas, lo que los hace vulnerables a interceptaciones. Estos mensajes a menudo contienen información crítica como contraseñas, códigos OTP y datos personales, lo que los convierte en un blanco atractivo para ciberdelincuentes. La CRC ya exige canales cerrados para las llamadas telefónicas por estos mismos motivos.

Para ilustrar de manera concreta la magnitud del riesgo al que actualmente están expuestos los sistemas de información y los datos personales, se ha documentado recientemente el hallazgo de más de 16.000 millones de credenciales de acceso (usuarios y contraseñas), las cuales fueron recopiladas y expuestas a través de múltiples bases de datos distribuidas en línea, como resultado de la propagación masiva de malware tipo "info stealer".

Este tipo de software malicioso tiene como objetivo principal la extracción silenciosa de información sensible directamente desde los dispositivos de los usuarios, sin requerir acciones visibles por parte de la víctima. Si bien no se trató de una única vulneración de seguridad, la agregación y exposición masiva de estas credenciales ha facilitado el desarrollo de ataques a gran escala, incluyendo campañas de phishing altamente dirigidas, robo de identidad, fraude financiero y suplantación de identidad digital.

Este escenario pone de manifiesto no solo la capacidad de daño de las amenazas cibernéticas actuales, sino también la urgencia de implementar medidas preventivas

robustas que incluyan educación del usuario, autenticación multifactor, monitoreo continuo y respuesta temprana a incidentes.

Aunque no se trató de una única brecha, estos datos fueron fácilmente accesibles y pudieron ser utilizados para ataques masivos de phishing, robo de identidad y suplantaciones. Este caso evidencia la magnitud de los peligros digitales que enfrentamos hoy.

Justificación de la medida propuesta

La Comisión de Regulación de Comunicaciones – CRC, ha reconocido previamente la necesidad de proteger la seguridad de las comunicaciones al establecer, por ejemplo, que la transmisión de llamadas telefónicas debe realizarse mediante canales cerrados, dedicados y protegidos, precisamente para evitar su exposición a redes públicas como Internet, lo que representa un riesgo alto de interceptación, suplantación o manipulación de contenido.

Esta medida ha sido clave para garantizar la integridad, disponibilidad y confidencialidad de las llamadas, en cumplimiento de los principios de seguridad de la información y en coherencia con el marco normativo que rige las telecomunicaciones.

Bajo esa misma lógica, proponemos extender esta obligación a la mensajería de texto (SMS), considerando que estos mensajes cumplen funciones similares en cuanto a su uso para la verificación de identidad, autenticación de usuarios y transmisión de información sensible. De hecho, los SMS son hoy uno de los canales más utilizados por entidades bancarias, plataformas digitales, aseguradoras y el mismo Estado, para enviar códigos de seguridad, alertas, accesos y notificaciones críticas.

El riesgo de interceptación de mensajes SMS en tránsito ha sido ampliamente documentado en publicaciones especializadas en ciberseguridad. Este tipo de ataque se vuelve más factible cuando los mensajes viajan por canales públicos de Internet, que son susceptibles a técnicas como el *man-in-the-middle (MITM)*, sniffing o acceso no autorizado a través de vulnerabilidades en redes compartidas.

A diferencia de la voz, cuyo cifrado y gestión de red suele estar más controlado por los operadores, los SMS son muchas veces gestionados por terceros que se interconectan directamente con los operadores móviles. Cuando estos enlaces no están protegidos mediante redes privadas o cifrado extremo a extremo, el mensaje queda expuesto durante todo su tránsito.

Este escenario configura una modalidad de ciberdelito aún incipiente en el país, pero cuyo potencial de daño es altísimo, especialmente si se considera que:

- La mayoría de los usuarios no sabe que sus mensajes pueden viajar por redes no seguras.
- Los atacantes pueden capturar información sin necesidad de vulnerar el dispositivo final.
- Las consecuencias pueden ser inmediatas: accesos no autorizados, robo de cuentas, transacciones fraudulentas, etc.

En un contexto donde los ataques informáticos han aumentado exponencialmente, y en donde Colombia ha sido blanco de múltiples incidentes de ciberseguridad, no basta con medidas reactivas. Resulta indispensable adoptar un enfoque preventivo, proporcional al nivel de riesgo y alineado con estándares internacionales de seguridad, como los promovidos por la UIT, el Foro de Gobernanza de Internet y las recomendaciones de ENISA (Agencia de Ciberseguridad de la Unión Europea).

Por todo lo anterior, resulta urgente adoptar una regulación que exija que la transmisión de SMS entre operadores se realice mediante canales punto a punto cerrados, tales como enlaces dedicados, redes privadas MPLS u otros mecanismos equivalentes que aseguren la confidencialidad y autenticidad del mensaje.

Por lo tanto, más allá de combatir el smishing, esta regulación anticiparía y mitigaría una amenaza aún no explotada masivamente: la intercepción de SMS en tránsito, preservando la confidencialidad y tranquilidad de millones de colombianos.

Agradecemos su atención al presente y quedamos atentos a colaborar en la implementación de esta medida, que refuerza el mandato de la CRC y fortalece la seguridad nacional.

Cordialmente,

DIEGO VALIVIESO PINILLA
Apoderado General
HABLAME COLOMBIA SA ESP
notificacionesjudiciales@hablame.co