CSTv-247/2025

Bogotá D.C., 4 de agosto de 2025

Doctora
CLAUDIA XIMENA BUSTAMANTE
Directora Ejecutiva
COMISIÓN DE REGULACIÓN DE COMUNICACIONES REPÚBLICA DE COLOMBIA
Ciudad

Referencia: comentarios proyecto regulatorio "Identificación de medidas para mitigar el fraude cibernético por medio de los servicios móviles"

Respetada doctora Bustamante,

Reciba un cordial saludo desde la Asociación Nacional de Empresas de Servicios Públicos y Comunicaciones – ANDESCO.

En relación con el proyecto de la referencia, respetuosamente y en aras de aportar en el desarrollo del mismo, ponemos a su consideración nuestros comentarios y propuestas para combatir el fraude cibernético a través de los servicios móviles.

El documento propuesto para comentarios, identifica como problema central la ausencia de herramientas regulatorias eficaces para prevenir el contacto con fines fraudulentos mediante servicios tradicionales, situación que se ha agravado por el incremento sostenido de delitos informáticos y quejas de usuarios.

Frente a la problemática planteada, consideramos que la CRC cuenta con facultades que le permiten adoptar medidas que ataquen las causas del problema y contribuyan a solucionarlo. No obstante, hay otras medidas que se deben armonizar intersectorialmente e incluso con participación del sector privado. Así las cosas, la CRC puede dar el primer paso al definir condiciones para prevenir el uso indebido de la numeración y en caso de que ocurra se tomen medidas oportunas y eficientes para la protección del usuario.

En general, es importante tener en cuenta las siguientes consideraciones:

- Aunque se contemplan medidas de trazabilidad, control y monitoreo, el marco actual no disuade suficientemente a los PCA/IT reincidentes en malas prácticas.
- No se impone una consecuencia directa y contundente sobre la relación de acceso entre el infractor y los operadores de red.

- La reincidencia no tiene consecuencias claras. El regulador propone recuperar códigos cortos por mal uso, pero no vincula directamente esta reincidencia con consecuencias contractuales, esto puede generar incentivos perversos, pues el costo de la reincidencia puede ser menor al beneficio económico obtenido por facilitar fraude.
- Mientras persista la posibilidad de seguir operando tras múltiples recuperaciones de numeración, no hay un incentivo para el cumplimiento de la regulación.
- La reincidencia sistemática en el uso indebido de códigos cortos demuestra una fallida gestión interna de seguridad por parte del PCA o IT.
- Las prácticas fraudulentas no solo afectan a usuarios, sino que también debilitan la integridad del ecosistema de telecomunicaciones, al erosionar la confianza en los canales tradicionales como el SMS y la voz.
- La repetida intervención del regulador para recuperar numeración demuestra un patrón, no una falla aislada.

Sobre el problema planteado:

El problema planteado por la CRC no parte del usuario como centro del perjuicio. En virtud de lo anterior, sugerimos reformular el problema con el fin de hacer visible que el fraude es una externalidad del modelo actual de acceso a la red y que, al no interrumpirlo, perpetúa la exposición del usuario a un entorno inseguro, así:

“Persistencia de canales habilitados para la comisión de fraudes a usuarios mediante servicios móviles, debido a vacíos regulatorios y a la falta de consecuencias efectivas frente a agentes reincidentes y/o frente a cualquier actor o agente que origine esta práctica fraudulenta.”

Sobre las causas

Las causas mencionadas deben complementarse. Se debe incluir i) la falta de consecuencias estructurales frente a la reincidencia, ii) el vacío regulatorio y la inhabilitación a los PRSTM para implementación de medidas de control, permiten la propagación y crecimiento exponencial de los fraudes de voz y SMS. Iii) imposibilidad de terminar relación de acceso con PCA o IT reincidente en el envío de SMS con contenido fraudulento.

Sobre las consecuencias

Se deben adicionar las siguientes consecuencias: i) Incremento en los costos operativos de mitigación. Las empresas deben invertir en soluciones tecnológicas como firewalls, IA, monitoreo de tráfico, auditorías y personal especializado para suplir la ausencia de consecuencias para el PCA o IT infractor por el envío de mensajes con contenido presuntamente fraudulento. ii) Continuidad en la relación de acceso entre PCA y/o IT y PRSTM.

Respecto de los grupos de valor:

- Plataformas de mensajería y agregadores internacionales. Muchos fraudes se originan desde plataformas o rutas internacionales (A2P SMS, OTTs, etc.). La regulación debe considerar cómo se integran estos actores en la cadena de valor y cómo se les puede exigir trazabilidad, autenticación de remitentes, responsabilidad y cumplimiento de normas locales.

- Entidades del sector educativo y académico (universidades, centros de investigación) Pueden apoyar en el diseño de campañas de sensibilización digital y estudios de impacto del fraude. Su participación puede fortalecer la base técnica y metodológica de las medidas regulatorias.

Alternativas regulatorias:

Desde la perspectiva de prevención del fraude en los servicios móviles, se considera pertinente proponer las siguientes alternativas regulatorias orientadas a fortalecer el control, la trazabilidad y la seguridad en el uso de la numeración de códigos cortos para el envío de mensajes cortos de texto (SMS):

- Autorizar la terminación del contrato de acceso o interconexión cuando un PCA o IT haya sido objeto de recuperación de dos o más códigos cortos en un mismo año calendario, por causas asociadas al uso indebido con fines fraudulentos. Con esta solución, el medio técnico se cierra, el tráfico del infractor ya no puede circular por la red, y se interrumpe la recurrencia del fraude.

- Como medida temporal y en línea con las mejores prácticas internacionales, es fundamental que la regulación colombiana habilite a los operadores móviles para realizar bloqueos de líneas y/o códigos cortos cuando existan quejas fundadas por parte de los usuarios. Esta medida permitiría contener de forma inmediata el posible daño mientras se realiza la verificación correspondiente.

- Establecer la posibilidad de que la CRC realice auditorías periódicas a los PCA o IT con el fin de verificar el debido uso de los códigos cortos, lo cual atiende la recomendación de la OCDE de auditorías regulatorias periódicas como parte de un enfoque de cumplimiento inteligente.

- La posibilidad de terminar, suspender o desconectar los acuerdos de acceso con PCA o IT reincidentes en recuperación de numeración ya sea un código corto o 940.

- Fortalecimiento del régimen sancionatorio por uso indebido de numeración.

- Incentivos regulatorios para buenas prácticas en protección al usuario.

- Establecer un esquema de reconocimiento público o beneficios regulatorios para los operadores, PCA e integradores que demuestren altos estándares en educación al usuario, prevención del fraude y atención de PQRD relacionadas con seguridad.

- Revisar y actualizar el régimen sancionatorio aplicable a los operadores y asignatarios que permitan el uso indebido de numeración E.164, incluyendo, suspensión de asignaciones, y posibilidad de terminar contratos. Un régimen sancionatorio más estricto y visible generaría un efecto disuasivo y promovería el cumplimiento de las obligaciones regulatorias.

Finalmente, observamos que la CRC con sus propuestas busca gravar más, e imponer obligaciones a los PRST, los cuales han implementado herramientas para identificar el envío de mensajes con contenido fraudulento, sin tener en cuenta que son unos pocos PCA o IT los que fomentan o permiten el envío mensaje con contenido fraudulento, por ello las medidas propuestas van orientadas a solucionar esta causa del problema.

Por otra parte, en relación con la suplantación del identificador de llamadas, conocida como *caller ID spoofing*, la cual es una práctica fraudulenta cada vez más común, utilizada por delincuentes para ocultar el verdadero origen de una llamada, dado que a través de tecnologías VoIP y herramientas especializadas, los estafadores pueden alterar los metadatos de una llamada en cuestión de segundos, generando grandes volúmenes de llamadas que apelan a la urgencia o confianza del usuario para obtener datos personales o financieros. Pese a la existencia de protocolos de autenticación y ciertas regulaciones, los atacantes logran evadir los controles aprovechando redes internacionales, proveedores poco seguros o sistemas con vulnerabilidades.

Para combatir esta práctica se propone:

- Establecer condiciones bajo las cuales los operadores de larga distancia deban realizar el bloqueo de llamadas internacionales con CLI nacional y prefijos o caracteres especiales.

- Publicación por parte de la CRC de una lista de rangos no asignados y exigencia de su bloqueo automático.

- Uso de herramientas tecnológicas para identificar y bloquear llamadas internacionales sospechosas.

Andesco
ASOCIACIÓN NACIONAL DE EMPRESAS DE SERVICIOS PÚBLICOS Y COMUNICACIONES

Agradecemos su atención y estaremos atentos a participar en el desarrollo del proyecto.

Cordialmente,

SERGIO VALDÉS BELTRÁN
Director Cámara TIC y TV