28 de julio de 2025

Claudia Ximena Bustamante
Directora Ejecutiva
Comisión de Regulación de Comunicaciones
Colombia

Ref. Aportes de la GSMA a la Consulta Pública sobre IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES.

Desde la GSMA celebramos la iniciativa de la Comisión de Regulación de Comunicaciones (CRC) de Colombia en avanzar hacia un marco regulatorio más robusto y acorde con los desafíos actuales del ecosistema digital. En particular, valoramos que se reconozca la creciente problemática del fraude cibernético y la necesidad de fomentar un entorno seguro para los usuarios. Como asociación que representa a la industria móvil global, acercamos a esta consulta pública una serie de reflexiones y recomendaciones construidas a partir de la experiencia internacional y el trabajo técnico conjunto con nuestros miembros en Colombia.

La industria móvil ha demostrado un compromiso permanente con la seguridad de sus usuarios. Los operadores móviles invierten constantemente en herramientas de detección de fraude, filtrado y bloqueo de tráfico malicioso, además de establecer firewalls para SMS y voz. Asimismo, actúan con celeridad ante comportamientos sospechosos, comparten inteligencia con otros sectores y capacitan de forma continua a su personal, al tiempo que educan al consumidor para que pueda identificar y reportar actividades fraudulentas.

Los principios claves que rigen la combinación de técnicas por parte de los operadores móviles para anticiparse al fraude son: especificidad y adaptabilidad de las estrategias, en lugar de soluciones universales; flexibilidad por sobre mandatos rígidos que corren el riesgo de volverse obsoletos e ineficaces; y visión de futuro mediante enfoques pragmáticos y colaborativos. En este contexto, como recomendación general, abogamos constantemente por el desarrollo de un marco flexible, preparado para el futuro y pragmático para abordar el fraude. Esto garantizará mayor eficacia continua de las medidas antifraude, protección – tanto para los consumidores como para el sector – y espacio para la innovación y la adaptación a medida que evolucionan este tipo de amenazas.

Sin embargo, entendemos que el fenómeno del fraude es complejo y que los eventos de ingeniería social se sofistican constantemente, por lo que ninguna acción aislada es suficiente. El enfoque debe ser colaborativo e intersectorial, involucrando a todos los actores de la cadena de valor, con el acompañamiento del regulador.

En línea con lo anterior, compartimos plenamente la visión de la CRC de que se requiere un enfoque holístico y multilateral. Asimismo, resaltamos la importancia de que sea abordado el análisis de todos los servicios asociados a las comunicaciones móviles, estos son: telefonía móvil, mensajes de texto SMS e internet móvil. La lucha contra el fraude exige reconocer la responsabilidad y el margen de acción de cada actor dentro de la cadena de valor. Es indispensable avanzar hacia reglas que distribuyan de forma más equitativa las obligaciones y medidas de prevención entre los distintos participantes, de manera proporcional a su exposición y capacidad de intervención.

Actualmente, el marco regulatorio está principalmente enfocado en los operadores móviles. Esto ha generado un escenario de cierta asimetría, en el que recaen sobre los operadores la mayoría de las exigencias técnicas, operativas y regulatorias, mientras que otros actores clave —como los Proveedores de Contenidos y Aplicaciones (PCA) e Integradores Tecnológicos (IT)— están sujetos a obligaciones más generales o menos específicas. Esta situación no refleja plenamente la evolución del ecosistema ni la distribución actual del riesgo.

Desde la GSMA consideramos que esta asimetría puede abordarse mediante un enfoque colaborativo y equilibrado, en el que la cooperación público-privada resulte clave para encontrar soluciones efectivas. Los operadores móviles ya cumplen con normas estrictas en materia de acceso e interconexión, ciberseguridad, gestión de red y trazabilidad, asumiendo un rol activo y muchas veces preventivo en la identificación de fraudes. Por su parte, el resto de la cadena, especialmente los PCA e IT, podría estar sujetos a obligaciones más alineadas con su nivel de exposición al riesgo, considerando que muchos de los incidentes de fraude y estafa se originan o se canalizan a través de esos entornos.

Además, a pesar de contar con un Régimen Integral de Administración de Recursos de Identificación y un Registro de Proveedores de Contenidos y Aplicaciones e Integradores (RPCAI), observamos espacios de mejora para los procesos de asignación de códigos cortos. Por ejemplo, la asignación por parte de la CRC podría presentar requerimientos más exigentes en términos de información solicitada al potencial asignatario. Esto permitiría garantizar la identificación clara de los asignatarios, evaluar su idoneidad y antecedentes, mientras que aumentaría la capacidad de fiscalización sobre el uso de estos recursos. En este sentido, es necesario que el marco regulatorio promueva la acción proactiva por parte de los PCA e IT – mediante la asignación de responsabilidades y obligaciones – en materia de control, trazabilidad y acción frente a presuntos casos fraudulentos de sus clientes. En contraste, los operadores móviles deben aplicar múltiples controles sobre su infraestructura sin contar con herramientas equivalentes para supervisar adecuadamente el accionar de los PCA e IT.

Por eso, consideramos fundamental establecer obligaciones y responsabilidades claras a los PCA, IT y generadores de contenido; en complemento al fomento de una colaboración más estrecha y un intercambio efectivo de información entre estos actores y los operadores móviles. Actualmente, no existe un marco que obligue a los PCA e IT a responder o actuar ante alertas por comportamientos sospechosos, lo que limita la eficacia de la respuesta ante posibles fraudes. La creación de un marco regulatorio claro que promueva la cooperación entre todos estos actores, incluidas las entidades usuarias de los códigos cortos y las autoridades, representaría un avance sustancial en la mitigación del fraude cibernético. Además, reconocemos que los generadores de contenido también desempeñan un rol activo en esta cadena de valor, al utilizar los canales móviles para transmitir mensajes a su público objetivo. Por ello, proponemos que estos actores sean incluidos en los mecanismos de seguimiento, control e identificación, mediante metodologías rigurosas que permitan su trazabilidad y los hagan responsable en caso de que sus mensajes sean utilizados para cometer fraudes.

Valoramos la voluntad que ha demostrado la CRC en la recuperación de numeración asociada a usos indebidos. No obstante, consideramos importante que esta medida no sea el punto final. La recuperación del código debe ir acompañada de una consecuencia en la relación de acceso, cuando la conducta es sistemática y reiterada, por cuanto el objetivo principal del regulador es salvaguardar los intereses de los usuarios. Hoy, este proceso se diluye entre diferentes autoridades y no existe ninguna consecuencia administrativa ni penal de las actuaciones realizadas. De hecho, considerando que el procedimiento administrativo es la principal herramienta que tenemos como nación para identificar a los verdaderos responsables detrás del fraude y sancionarlos adecuadamente, es fundamental empoderar y capacitar a las autoridades para que puedan realizar investigaciones sobre casos de comportamientos fraudulentos.

En esta misma línea, sugerimos evaluar la posibilidad de habilitar el bloqueo preventivo de tráfico sospechoso por parte de los operadores móviles, sin que esto implique cuestionamientos regulatorios por presunta obstrucción del servicio. En muchas ocasiones, los operadores identifican patrones de fraude de forma anticipada, pero su margen de acción es limitado. Poder bloquear de forma preventiva sería una herramienta útil no solo para proteger la red, sino también a los usuarios finales.

Adicionalmente, proponemos que se establezcan consecuencias proporcionales para los casos en los que, a través de un recurso de numeración, se facilite o se repita una conducta que derive en fraude cibernético. Por ello se reitera que una opción válida sería habilitar la posibilidad de terminar la relación de acceso o interconexión con aquellos PCA e IT que hayan incurrido reiteradamente en infracciones. Este tipo de medidas deben ser previstas como parte de un régimen de consecuencias para proteger la integridad del ecosistema.

Es esencial incluir en el debate y en el eventual marco regulatorio que de él surja a los servicios provistos por plataformas OTT. Es consabido el aumento de fraudes y estafas llevadas a cabo por servicios de mensajería instantánea tipo WhatsApp o casos de suplantación de identidad por redes sociales. El vacío regulatorio y la falta de un marco que promueva la colaboración entre los distintos actores de la cadena de valor complejiza el abordaje eficaz de estos delitos. A pesar de que la consulta no profundiza en los delitos cibernéticos perpetrados mediante OTT, existe la oportunidad para integrarlos a la discusión sobre la búsqueda de soluciones a una problemática que afecta a todos los usuarios del ecosistema digital.

Por otra parte, consideramos necesario avanzar en medidas que permitan enfrentar otro fenómeno emergente: la suplantación mediante llamadas internacionales que utilizan numeración nacional (CLI spoofing). En este sentido, apoyamos que la CRC evalúe la posibilidad de habilitar a los operadores para bloquear tráfico de llamadas entrantes del exterior que presenten números colombianos como identificador, prefijos o caracteres especiales, salvo en casos de roaming internacional. Esta medida ayudaría significativamente a prevenir estafas originadas fuera del país. Asimismo, se debería revisar la participación de actores como los Operadores Móviles Virtuales y los servicios Machine To Machine (M2M), cuya gestión de numeración también presenta vulnerabilidades que pueden resultar en casos de fraude.

Finalmente, sabemos que el comportamiento humano suele ser el eslabón más débil de la cadena de seguridad, y los delincuentes recurren cada vez más a técnicas de ingeniería social para obtener la información necesaria para perpetrar sus delitos en línea. Por lo tanto, más allá de las soluciones técnicas y regulatorias, una defensa insustituible es la concientización y la formación. Es necesario informar a las personas sobre las tácticas comunes que utilizan los delincuentes, cómo reconocerlas y cómo denunciar actividades sospechosas. Es fundamental concientizar y educar a los usuarios, principalmente a los más vulnerables, sobre la protección de la información personal, indicándoles qué hacer en situaciones donde esta pueda verse comprometida.

Reiteramos nuestro respaldo a los esfuerzos de la CRC por fortalecer la regulación en materia de seguridad y prevención del fraude. Confiamos en que esta consulta pública marcará un punto de inflexión para avanzar hacia un marco más equilibrado, preventivo y eficiente, que permita a todos los actores —incluyendo operadores móviles, PCA, IT, OTT y demás integrantes del ecosistema digital— cumplir un rol activo y coordinado en la lucha contra el fraude cibernético. Estamos a su disposición para ampliar cualquiera de los puntos mencionados o compartir experiencias regulatorias internacionales que puedan resultar útiles en este proceso.

Lo saluda atentamente,

Ing. Lucas Gallitto
Director para América Latina
GSMA

Información adicional:

Fraud and Scams: Staying Safe in the Mobile World, 2025, GSMA.

Seguridad y privacidad a lo largo del ecosistema móvil, 2023, GSMA.