

22 de julio de 2026

Felipe Díaz Suaza

Director Ejecutivo

Comisión de Regulación de Comunicaciones

Colombia

Ref. Comentarios de la GSMA al proyecto regulatorio "Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones".

Respetado Director Ejecutivo:

Desde la GSMA celebramos la continuidad del trabajo que viene desarrollando la Comisión de Regulación de Comunicaciones (CRC) para fortalecer la prevención del fraude cibernético por medio de los servicios móviles. Valoramos especialmente el compromiso de la Comisión por mantener un diálogo abierto con la industria y avanzar en el diseño de medidas orientadas a fortalecer la confianza de los usuarios y contribuir a un ecosistema digital más seguro.

El fraude constituye hoy un desafío global que evoluciona permanentemente y trasciende a un único sector o tecnología. Por ello, la GSMA impulsa la iniciativa **United Against Scams**, que promueve respuestas coordinadas entre operadores móviles, entidades financieras, plataformas digitales, proveedores tecnológicos, autoridades y demás actores del ecosistema, bajo un enfoque basado en la colaboración, la innovación y la asignación proporcional de responsabilidades. La experiencia internacional demuestra que las amenazas evolucionan con mayor rapidez que los procesos regulatorios, por lo que los marcos normativos deben facilitar respuestas ágiles y flexibles, capaces de adaptarse continuamente a nuevas modalidades de fraude.

En ese contexto, la GSMA comparte el objetivo de la CRC de fortalecer las capacidades de prevención y mitigación del fraude y considera que el proyecto representa un paso importante en esa dirección. No obstante, con fundamento en la experiencia internacional de la industria móvil y en los principios que orientan la iniciativa **United Against Scams**, nos permitimos formular las siguientes recomendaciones.

1. Promover un marco regulatorio basado en principios, colaboración e innovación

El fraude cibernético constituye un fenómeno dinámico y transversal que evoluciona constantemente en respuesta a las medidas implementadas por los distintos actores del ecosistema digital. Ninguna solución aislada resulta suficiente para combatirlo de manera definitiva, por lo que las políticas públicas deben promover un enfoque integral, colaborativo y preparado para el futuro.

En este sentido, **la GSMA considera que los marcos regulatorios basados en principios ofrecen mejores resultados que aquellos excesivamente prescriptivos, ya que permiten que la industria continúe desarrollando e incorporando nuevas herramientas tecnológicas conforme evolucionan las modalidades de fraude.** La regulación debe crear las condiciones para que la innovación y la cooperación entre el sector público y privado continúen fortaleciendo la capacidad colectiva de prevenir, detectar y responder frente a nuevas amenazas.

2. Alinear la evolución regulatoria del mercado A2P con las inversiones en ciberseguridad

La implementación de nuevas salvaguardas técnicas, incluyendo herramientas de monitoreo, analítica, autenticación, filtrado, trazabilidad e inteligencia contra el fraude, exige inversiones significativas y permanentes por parte de la industria móvil.

En paralelo, el sector de las telecomunicaciones atraviesa una profunda transformación. Los servicios tradicionales de voz y la mensajería persona a persona (SMS P2P) registran una tendencia sostenida de reducción de ingresos y tráfico, producto de la evolución tecnológica y de la creciente utilización de nuevos servicios y plataformas digitales que compiten por las comunicaciones de los usuarios. En este contexto, el mercado de **SMS A2P** se ha consolidado como uno de los pocos segmentos que aún permite sostener inversiones continuas en la evolución de las plataformas de mensajería, la resiliencia de las redes y el fortalecimiento de las capacidades de ciberseguridad.

Por ello, la GSMA considera especialmente importante **avanzar en la desregulación del mercado de SMS A2P**, permitiendo que dicho segmento genere las condiciones económicas necesarias para continuar financiando las inversiones que demanda la creciente sofisticación de las amenazas cibernéticas.

Mantener un esquema de regulación tarifaria mientras, simultáneamente, se incorporan nuevas obligaciones técnicas genera una desalineación entre las exigencias regulatorias y la capacidad económica necesaria para financiarlas. Ello reduce la capacidad del sector para sostener en el tiempo las inversiones crecientes que demandan las herramientas de prevención, monitoreo y respuesta frente al fraude, precisamente en un contexto en el que las amenazas evolucionan de manera permanente y requieren una actualización constante de las capacidades tecnológicas.

Por ello, desde la GSMA consideramos conveniente que la liberalización del mercado de SMS A2P preceda o, al menos, avance de manera paralela con la implementación de las nuevas medidas técnicas contempladas en este proyecto. Alinear ambos procesos permitirá que la industria continúe invirtiendo en soluciones innovadoras de prevención del fraude y fortalecerá la sostenibilidad del propio marco regulatorio, asegurando que las obligaciones técnicas vayan acompañadas de condiciones que permitan financiarlas adecuadamente.

3. Implementación basada en análisis de impacto normativo y plazos técnicamente realistas

La GSMA considera importante que **las medidas propuestas estén acompañadas de un análisis integral de impacto normativo que permita evaluar su efectividad esperada, los costos de implementación, las alternativas regulatorias disponibles y su proporcionalidad** respecto de los beneficios perseguidos.

La experiencia internacional demuestra que muchas de las herramientas contempladas requieren adecuaciones significativas sobre plataformas críticas de red, desarrollos tecnológicos específicos, integración mediante APIs, pruebas de interoperabilidad, adecuaciones operativas y procesos coordinados entre múltiples actores del ecosistema. Estas implementaciones demandan tiempos adecuados de diseño, desarrollo, pruebas y puesta en operación.

Por ello, estimamos recomendable que el análisis técnico y económico preceda la definición de los cronogramas regulatorios, de manera que los plazos de implementación reflejen adecuadamente la complejidad de cada medida y permitan una adopción segura, eficiente y ordenada.

4. Responsabilidades proporcionales a lo largo de toda la cadena de valor

La GSMA considera indispensable que el marco regulatorio continúe evolucionando hacia **un esquema de responsabilidades proporcionales entre todos los participantes del ecosistema digital**.

El fraude cibernético no se origina ni se desarrolla exclusivamente en las redes móviles. En la cadena de valor intervienen proveedores de contenidos y aplicaciones (PCA), integradores tecnológicos, plataformas digitales, entidades financieras, proveedores tecnológicos y otros actores que cuentan con distintos niveles de control y visibilidad sobre las actividades fraudulentas.

En este sentido, consideramos importante continuar fortaleciendo las obligaciones aplicables a aquellos actores que administran o intermedian el tráfico A2P, particularmente en materia de identificación de clientes, procesos de conocimiento del cliente (KYC), validación de identidad, trazabilidad y respuesta frente a reportes de actividades sospechosas. Un mayor nivel de diligencia en estos procesos contribuirá a prevenir que actores maliciosos utilicen estos canales para desarrollar actividades fraudulentas.

Asimismo, valoramos positivamente aquellas medidas que fortalecen la capacidad de actuación temprana frente a actividades potencialmente fraudulentas. Consideramos conveniente que el marco regulatorio permita la adopción de medidas preventivas frente a patrones de tráfico objetivamente sospechosos, dentro de procedimientos claros, transparentes y con las debidas garantías para todos los actores involucrados. Este tipo de herramientas contribuye a contener oportunamente actividades fraudulentas y fortalece la protección de los usuarios.

En relación con las medidas orientadas a mitigar el **CLI Spoofing**, estimamos igualmente importante preservar el principio de proporcionalidad. Si bien los operadores móviles continúan realizando importantes inversiones para proteger sus redes y usuarios, muchas modalidades de suplantación de identidad tienen origen en actores y segmentos del ecosistema que escapan a su ámbito de control técnico, particularmente cuando involucran originadores internacionales, proveedores de tránsito u otros intermediarios.

En consecuencia, **las obligaciones regulatorias deberían asignarse considerando el nivel efectivo de control que cada participante ejerce sobre el tráfico y procurando que las inversiones exigidas resulten proporcionales al beneficio esperado**. Este principio cobra especial relevancia considerando que varias de las medidas propuestas implican inversiones significativas sobre servicios tradicionales de voz que actualmente enfrentan una disminución sostenida de tráfico debido a la creciente migración de las comunicaciones hacia aplicaciones OTT y otras plataformas digitales.

5. Fortalecer la colaboración y el intercambio de información entre los actores del ecosistema

La prevención del fraude depende cada vez más de la capacidad de compartir oportunamente inteligencia e información entre los distintos actores que participan en el ecosistema digital. Por ello, la GSMA considera conveniente que el marco regulatorio habilite y promueva mecanismos efectivos para el intercambio de indicadores de riesgo, patrones de comportamiento, campañas fraudulentas, incidentes relevantes y demás información que permita una respuesta temprana y coordinada frente a nuevas amenazas.

En este sentido, resulta igualmente importante que la CRC continúe promoviendo **espacios de colaboración y marcos flexibles que otorguen certeza jurídica para el intercambio de**

información con fines exclusivos de prevención del fraude, preservando en todo momento la privacidad de los usuarios, la protección de los datos personales, los secretos comerciales y las reglas de competencia. Una mayor claridad regulatoria en este ámbito facilitará respuestas más rápidas y coordinadas sin generar incertidumbre para los distintos participantes del ecosistema.

6. Fomentar la educación y concientización digital de los usuarios

Finalmente, la **GSMA considera muy positiva la incorporación de iniciativas orientadas a fortalecer la educación y concientización digital de los usuarios.**

La ingeniería social continúa siendo uno de los principales mecanismos utilizados por los delincuentes y, en consecuencia, el fortalecimiento de las capacidades de los ciudadanos para reconocer intentos de fraude constituye un complemento indispensable de las medidas tecnológicas y regulatorias. Las campañas permanentes de educación digital permiten incrementar la resiliencia de los usuarios y reducir significativamente la efectividad de las modalidades de fraude basadas en el engaño.

En este sentido, consideramos que el proyecto regulatorio representa una valiosa oportunidad para consolidar campañas permanentes de educación y sensibilización, articuladas entre autoridades, industria y demás actores del ecosistema digital, como complemento indispensable de las medidas técnicas contempladas en la presente iniciativa.

La GSMA reitera su disposición para continuar colaborando con la CRC en la construcción de un marco regulatorio que fortalezca la confianza en el ecosistema digital, incentive la inversión en nuevas capacidades de ciberseguridad, promueva la innovación y distribuya las responsabilidades de manera equilibrada entre todos los actores de la cadena de valor.

Agradecemos la oportunidad de participar en esta consulta pública y quedamos a disposición de la Comisión para continuar aportando la experiencia internacional de la industria móvil en el desarrollo de iniciativas orientadas a combatir el fraude cibernético.

Atentamente,



Ing. Lucas Gallitto
Director para América Latina y el Caribe
GSMA

Información adicional:

Sitio web de United Against Scams [aquí](#).

United Against Scams: [Call to Action](#).

[Biblioteca de casos de prevención de fraudes y estafas en el ecosistema móvil](#).

[The Impact of Cybersecurity Regulation on Mobile Operators](#), 2025, GSMA.

[Fraud and Scams: Staying Safe in the Mobile World](#), 2025, GSMA.

[Seguridad y privacidad a lo largo del ecosistema móvil](#), 2023, GSMA.