AMCHAM COLOMBIA
CÁMARA DE COMERCIO COLOMBO AMERICANA

PE-517/2026
Bogotá, 22 de junio de 2026

Doctor
FELIPE AUGUSTO DÍAZ SUAZA
Director Ejecutivo
COMISION DE REGULACIÓN COMUNICACIONES
Bogotá D.C.

Asunto: Comentarios al Proyecto de Resolución "Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones".

Estimado Director,

Reciba un cordial saludo desde la Cámara Colombo Americana, AmCham Colombia, asociación empresarial independiente con 70 años de trayectoria, cuyo propósito es contribuir al fortalecimiento de las relaciones bilaterales entre Colombia y Estados Unidos, así como al desarrollo económico y social del país a través del trabajo conjunto con más de 920 compañías afiliadas en todo el territorio nacional.

Como parte de las gestiones que realizamos en el cumplimiento del propósito que nos constituye, nuestra asociación transmite constantemente a las diferentes ramas del poder público las observaciones de las empresas nacionales y extranjeras que representamos, de manera que se aporte a la generación de entornos económicos y regulatorios favorables para la atracción y retención de la inversión, el aprovechamiento del Tratado de Libre Comercio con los Estados Unidos, y el crecimiento económico y desarrollo social de la Nación.

En esta oportunidad, y atendiendo al interés manifestado por nuestros afiliados del sector tecnológico y de servicios digitales, nos permitimos remitir un alcance a los comentarios presentados frente al Proyecto de Resolución "Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones".

Desde AmCham Colombia reconocemos la importancia de avanzar en medidas regulatorias orientadas a mitigar el fraude cibernético, proteger a los usuarios y fortalecer la confianza en los servicios móviles y digitales. La prevención de prácticas como la suplantación, el uso indebido de canales de mensajería y los ataques asociados a ingeniería social constituye un objetivo legítimo de política pública, especialmente en un entorno en el que la digitalización de servicios financieros, comerciales, tecnológicos y de autenticación continúa creciendo de manera acelerada.

En ese sentido, y con el propósito de aportar elementos técnicos que contribuyan a fortalecer la eficacia, proporcionalidad y viabilidad operativa del proyecto normativo, presentamos a continuación una serie de

comentarios transversales relacionados con el uso de tecnologías dinámicas para la detección del fraude, la conveniencia de modelos interoperables frente a esquemas centralizados de validación y el impacto que ciertas cargas operativas podrían tener sobre la disponibilidad de servicios digitales seguros en Colombia.

COMENTARIOS TRANSVERSALES.

1. Visión de futuro e impacto en la innovación: limitaciones al uso de Inteligencia Artificial para la detección de fraude.

El proyecto de resolución, al estructurar parte de su arquitectura de seguridad sobre un esquema de plantillas rígidas y aprobación previa de contenido, particularmente en los artículos 6.13.4.1 a 6.13.4.3, introduce un modelo de control estático que puede resultar incompatible con las herramientas más avanzadas de protección al usuario.

El fraude cibernético evoluciona de manera constante y utiliza técnicas de ingeniería social, suplantación y manipulación de mensajes que cambian en tiempo real. Por esta razón, la industria global ha venido migrando hacia sistemas de Inteligencia Artificial y aprendizaje automático que permiten analizar patrones de tráfico, identificar comportamientos sospechosos, activar alertas dinámicas y ajustar mecanismos de autenticación de acuerdo con el riesgo detectado. Estas soluciones no dependen necesariamente de textos previamente aprobados, sino de la capacidad de reacción inmediata frente a señales de amenaza.

En este contexto, la exigencia de una plantilla previamente aprobada puede limitar la posibilidad de que los sistemas de seguridad globales adapten los mensajes de alerta, los factores de autenticación o las respuestas automatizadas ante incidentes detectados por Inteligencia Artificial. Esto podría dejar a los usuarios expuestos frente a ataques que no encajen en las plantillas vigentes o que requieran una reacción inmediata, distinta a la previamente validada por el esquema regulatorio.

Por lo anterior, consideramos que una regulación orientada a combatir el fraude debe promover la adopción de tecnologías avanzadas, no restringirlas mediante modelos excesivamente rígidos. En consecuencia, sugerimos que la CRC revise el alcance de las obligaciones asociadas a plantillas y validación previa, de manera que se permita el uso de soluciones dinámicas, automatizadas y basadas en riesgo, siempre que estas cumplan con estándares verificables de seguridad, trazabilidad y protección al usuario.

Así mismo, advertimos que rigidizar los canales SMS y USSD bajo un esquema centralizado de validación de contenido puede desincentivar la transición hacia métodos de autenticación más robustos y adaptativos, en contravía del principio de neutralidad tecnológica. La regulación debería habilitar distintos modelos técnicos de prevención y detección de fraude, permitiendo que los proveedores adopten las mejores herramientas disponibles según la evolución de los riesgos y las capacidades de sus sistemas.

2. Interoperabilidad y estándares técnicos frente al modelo de Validador Centralizado.

El proyecto propone la creación de un Validador Centralizado, operado por un tercero privado único, conforme a los artículos 6.13.1.1 a 6.13.1.6. Si bien entendemos que esta figura busca generar un punto de control para mitigar el uso fraudulento de servicios móviles, consideramos necesario revisar cuidadosamente su diseño, pues

podría convertirse en un punto de falla sistémico, una barrera de entrada y una fuente adicional de costos y latencia para los actores del ecosistema digital.

Desde una perspectiva técnica y regulatoria, resulta más conveniente avanzar hacia un modelo basado en interoperabilidad, estándares abiertos y protocolos de seguridad verificables. Este enfoque permitiría que distintos proveedores, tanto locales como globales, integren sus propios sistemas de verificación, autenticación y prevención de fraude con el ecosistema colombiano, sin depender necesariamente de un intermediario obligatorio y centralizado.

La experiencia de otros sectores regulados demuestra que los modelos interoperables pueden permitir una coordinación efectiva entre actores públicos y privados, sin sacrificar innovación, escalabilidad ni resiliencia técnica. En lugar de concentrar la validación en un único operador, la CRC podría promover el uso de APIs de seguridad, estándares técnicos de intercambio de información, mecanismos automatizados de reporte de fraude y criterios comunes de identificación de riesgos.

En particular, consideramos que debería evaluarse la adopción de un estándar técnico para el intercambio de información relacionada con procesos de conocimiento del cliente, reporte de incidentes, señales de fraude y autenticación de mensajes. Esto permitiría una respuesta más ágil y coordinada frente a amenazas cibernéticas, reduciendo fricciones operativas y facilitando la integración de proveedores globales con el marco colombiano.

Por lo anterior, sugerimos respetuosamente que la CRC reevalúe la necesidad de establecer un Validador Centralizado obligatorio y, en su lugar, considere un modelo regulatorio basado en interoperabilidad, estándares abiertos, certificaciones técnicas y obligaciones de resultado en materia de prevención del fraude. Este enfoque permitiría cumplir el objetivo de protección del usuario sin sacrificar innovación, competencia ni eficiencia operativa.

3. Carga operativa local y disponibilidad de servicios digitales 24/7.

Finalmente, consideramos indispensable evaluar el impacto de las cargas operativas derivadas del modelo propuesto, especialmente para proveedores de servicios digitales transfronterizos que operan bajo esquemas globales de soporte, seguridad y autenticación.

El proyecto, al exigir la validación periódica de plantillas y la resolución de rechazos en plazos reducidos, de 24 a 48 horas, puede imponer de facto la necesidad de contar con una estructura operativa local, en idioma español y con disponibilidad permanente para interactuar con el Validador. Si bien la atención oportuna de incidentes es relevante, el diseño de estas obligaciones debe ser proporcional y considerar las diferencias entre operadores locales de telecomunicaciones, agregadores, proveedores de contenido, plataformas digitales y servicios globales de autenticación.

Para los proveedores de servicios digitales transfronterizos, estas exigencias pueden generar cargas desproporcionadas cuando se combinan con requisitos adicionales, como la eventual obligación de establecer una sucursal en Colombia para acceder al SENDER ID. En la práctica, esto podría obligar a las empresas a crear

estructuras operativas dedicadas exclusivamente al cumplimiento de un proceso local de validación de plantillas, sin que exista una relación clara entre esa carga y una mejora técnica efectiva en la seguridad del usuario.

Desde AmCham Colombia advertimos que una carga operativa excesiva puede producir efectos no deseados. Algunos proveedores podrían limitar o descontinuar el uso de canales SMS o USSD para autenticación en Colombia, restringir la disponibilidad de ciertos servicios digitales, demorar procesos de verificación o migrar hacia mecanismos menos accesibles para determinados usuarios. En lugar de fortalecer la seguridad, estas consecuencias podrían aislar a los usuarios colombianos de estándares globales de autenticación y protección.

La disponibilidad de servicios digitales 24/7 depende de arquitecturas globales altamente automatizadas, con equipos distribuidos, sistemas de monitoreo continuo y protocolos de respuesta inmediata. Imponer procesos manuales, locales o dependientes de validaciones previas puede afectar la eficiencia de estos modelos y reducir la capacidad de reacción frente a incidentes de seguridad. Por ello, sugerimos que la CRC incorpore criterios de proporcionalidad, gradualidad y reconocimiento de modelos operativos globales en la definición de las obligaciones aplicables.

En este sentido, recomendamos que las obligaciones asociadas a plantillas, validaciones, soporte y tiempos de respuesta sean revisadas para permitir esquemas automatizados, integraciones técnicas directas y mecanismos de cumplimiento basados en riesgo. Esto permitiría preservar la protección del usuario sin imponer cargas que puedan afectar la disponibilidad de servicios digitales seguros en el país.

CONCLUSIÓN.

Desde AmCham Colombia reiteramos nuestro respaldo al propósito de fortalecer la prevención del fraude cibernético y proteger a los usuarios de servicios móviles y digitales. No obstante, solicitamos respetuosamente a la CRC revisar las disposiciones relacionadas con la aprobación previa de plantillas, el modelo de Validador Centralizado y las cargas operativas derivadas del soporte local y los tiempos de respuesta, de manera que la regulación sea compatible con la innovación tecnológica, la neutralidad tecnológica, la interoperabilidad y la operación eficiente de servicios digitales transfronterizos.

Agradecemos la oportunidad de presentar estas consideraciones adicionales y reiteramos nuestra disposición para continuar participando en los espacios de diálogo que la Comisión disponga. Estamos convencidos de que una regulación basada en interoperabilidad, innovación y proporcionalidad permitirá avanzar en la mitigación del fraude cibernético sin afectar la disponibilidad, seguridad y competitividad de los servicios digitales en Colombia.

Cordialmente,

MARÍA CLAUDIA LACOUTURE P.
Presidente Ejecutiva