Bogotá D.C., 23 de junio 2026

Señores
Comisión de Regulación de Comunicaciones CRC
Ciudad

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”.

Respetados señores:

La Cámara Colombiana de Comercio Electrónico CCCE se permite presentar comentarios al Proyecto de Resolución de la referencia, mediante el cual la Comisión de Regulación de Comunicaciones propone adoptar medidas para mitigar el fraude cibernético por medio de servicios móviles.

Si bien compartimos el objetivo de fortalecer la protección de los usuarios y preservar la confianza en el ecosistema digital, consideramos necesario formular observaciones sobre algunas disposiciones que podrían generar cargas desproporcionadas, afectar comunicaciones legítimas de autenticación y seguridad, e introducir barreras operativas y regulatorias para la prestación de servicios digitales.

El Proyecto de Resolución tiene como finalidad combatir el fraude cibernético, proteger a los usuarios frente a la suplantación, el phishing y el smishing, y preservar la confianza en el ecosistema digital. Desde esta perspectiva, se coincide con dicho propósito y se reconoce la necesidad de implementar las medidas necesarias e idóneas para salvaguardar la seguridad y el bienestar de los usuarios.

Pese a lo anterior, se considera necesario advertir que el Proyecto de Resolución podría producir efectos contrarios a la finalidad que persigue. En particular, la iniciativa resulta preocupante en la medida en que: (i) utiliza la competencia de la CRC sobre recursos de identificación para imponer obligaciones sustantivas sobre proveedores de contenidos y aplicaciones, incluidos actores que no tienen la calidad de PRST, lo cual exige una habilitación legal clara, expresa y suficiente; (ii) establece un esquema de validación previa de plantillas y de condicionamiento operativo del tráfico A2P que puede afectar comunicaciones legítimas y críticas, como OTP, 2FA, alertas de seguridad y mensajes transaccionales; (iii) impone cargas que podrían resultar desproporcionadas frente a alternativas menos restrictivas e igualmente eficaces, comprometiendo la neutralidad tecnológica, la continuidad de servicios críticos y la seguridad digital de los usuarios; y (iv) algunas propuestas incluidas en el Proyecto generan tensiones con la libertad de empresa, la libre competencia y la innovación tecnológica.

A continuación, se presentan los comentarios frente al Proyecto de Resolución:

I. Comentarios Generales

a. Ausencia de competencias legales de la CRC

El Proyecto incluye obligaciones en cabeza de los PCA, definidos de forma amplia como los “responsables directos por la producción o generación o consolidación de contenidos o aplicaciones”, incluyendo “todos aquellos actores que presten sus funciones como

productores, generadores o agregadores de contenido" (artículo 2). Sobre estos actores se imponen obligaciones de registro, KYC, aprobación previa de contenido, validación anual y sujeción a un validador centralizado.

Al respecto, se reconoce que la CRC cuenta con competencias legales para regular y administrar los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones, incluyendo aquellos que permiten identificar redes, servicios o usuarios dentro del ecosistema de comunicaciones. En ese sentido, no se desconoce que la CRC pueda adoptar medidas orientadas a prevenir el uso indebido de recursos como los códigos cortos A2P o el SENDER ID, siempre que dichas medidas estén directamente relacionadas con la administración eficiente, segura y no discriminatoria de tales recursos.

Sin embargo, el Proyecto va más allá de la regulación del recurso de identificación como tal. Bajo la estructura propuesta, la administración del SENDER ID, del código corto A2P y de las plantillas de contenido se utiliza para imponer obligaciones sustantivas sobre los proveedores de contenidos y aplicaciones (PCA), incluyendo obligaciones de registro, KYC, validación, aprobación previa de plantillas, renovación periódica, monitoreo y eventual bloqueo o restricción del envío de mensajes. En la práctica, estas medidas no solo regulan el uso técnico de un recurso de identificación, sino que condicionan la posibilidad misma de que ciertos agentes generen y envíen comunicaciones legítimas a sus usuarios.

Esta distinción es relevante porque la competencia para administrar recursos de identificación no debería entenderse como una habilitación general para regular integralmente la actividad económica de los generadores de contenido, ni para someter sus comunicaciones a un régimen de autorización previa. Cuando la regulación pasa de ordenar el uso de un recurso de identificación a establecer condiciones sustantivas de acceso, permanencia y operación para actores que no son proveedores de redes y servicios de telecomunicaciones, se requiere una habilitación legal clara, expresa y suficiente, así como una justificación reforzada de necesidad, idoneidad y proporcionalidad.

Es importante resaltar que las autoridades sólo pueden hacer aquello para lo cual están expresamente facultadas por la Constitución y la ley. Además, la intervención del Estado, particularmente en la economía y en los servicios, debe hacerse por mandato de la ley; y la actividad económica y la iniciativa privada son libres, y para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley (artículos 333 y 334 de la Constitución Política). En este sentido, una regulación que impone obligaciones, restricciones y un esquema de control previo sobre actores no pertenecientes al sector de telecomunicaciones exige una habilitación legal clara, específica y suficiente, que no se encuentra explícitamente señalada en el Proyecto de Resolución.

Por ejemplo, el Proyecto no identifica una norma legal que habilite expresamente a la CRC para: (i) crear un registro y un régimen de obligaciones aplicable a PCA que no tienen la calidad de PRST; (ii) establecer un validador centralizado privado como condición de acceso al mercado; ni (iii) condicionar el envío de mensajes A2P a la aprobación previa de plantillas de contenido. De hecho, la invocación de los numerales 1, 3 y 12 del artículo 22 de la Ley 1341 de 2009 debería ser complementada con una justificación específica sobre por qué tales competencias permiten imponer obligaciones directas a generadores de contenido y no únicamente reglas de administración de recursos de identificación.

Finalmente, toda medida regulatoria que imponga este tipo de obligaciones debe ser necesaria, idónea y proporcional, y debe sustentarse en evidencia de que el beneficio esperado supera sus costos y riesgos para los obligados. El Proyecto debería acreditar con mayor detalle que las medidas propuestas en relación con los PCA son necesarias e idóneas frente al fraude que pretende combatir, y que no existen alternativas menos restrictivas, tales como validación basada en riesgo, reportes posteriores, auditorías selectivas o controles reforzados únicamente frente a agentes o contenidos de mayor riesgo.

b. Efecto negativo sobre la seguridad digital

El Proyecto establece obligaciones sobre quienes generan mensajes de autenticación (OTP), segundo factor (2FA), verificación de identidad, alertas de seguridad y comunicaciones transaccionales. Estas comunicaciones son, en muchos casos, parte intrínseca de servicios digitales prestados desde fuera del sector de telecomunicaciones e incluso desde fuera del país.

Frente a lo anterior, resulta pertinente indicar que la autenticación multifactor mediante OTP y 2FA es una de las medidas de seguridad más utilizadas para mitigar la apropiación de cuentas, la suplantación y el fraude en internet. El Proyecto somete estos mensajes al mismo aparato de plantillas obligatorias, aprobación previa, validación anual y eventual bloqueo aplicable a otras modalidades de mensajería A2P. Aunque el Proyecto reconoce que los mensajes de autenticación y seguridad tienen una naturaleza especial y no requieren consentimiento adicional, dicha diferenciación pierde eficacia si, en la práctica, estos mensajes quedan sujetos al mismo esquema de validación previa y bloqueo operativo que las comunicaciones comerciales o publicitarias.

En este sentido, el Proyecto de Resolución desconoce que cada uno de esos pasos introduce latencia, costos y puntos de falla en una cadena que debe ser instantánea y de altísima disponibilidad, especialmente teniendo en cuenta que su finalidad es proteger las cuentas de los usuarios.

Si un OTP no se entrega por falta de plantilla vigente, por una desactivación, por una caída del validador o por un bloqueo del PRST, el usuario no podrá iniciar sesión, recuperar su cuenta ni autenticar el uso de su cuenta. El efecto previsible podría ser no menos fraude, sino más exposición a usuarios bloqueados, migración a factores menos seguros y mayor superficie para el fraude de cuentas. Una medida concebida para mitigar el fraude no debe perjudicar la herramienta que más lo previene y afectar desproporcionadamente medidas de seguridad reconocidas como eficaces internacionalmente.

Es esencial distinguir con precisión entre (i) las comunicaciones legítimas de autenticación y seguridad, solicitadas por el propio usuario o derivadas de un servicio contratado, y (ii) las prácticas fraudulentas de phishing, smishing, suplantación de marca, ingeniería social, malware, SIM swapping y granjas de SIM. El OTP y el 2FA son mecanismos reconocidos de respuesta al fraude, no su causa. Por lo tanto, imponerles barreras podría generar riesgos de seguridad adicionales para el ecosistema digital.

II. Comentarios específicos

1. Preocupación frente a las medidas impuestas relacionadas con el SENDER ID

El artículo 1 del Proyecto de Resolución define el SENDER ID como un recurso de identificación administrado por la CRC que identifica al responsable del contenido enviado por SMS y USSD. Por su parte, el Capítulo 12 (artículos 6.12.1.1 y siguientes) regula su asignación, condicionando la tenencia de SENDER ID a la posibilidad de cursar tráfico A2P.

Resulta preocupante que la figura del SENDER ID se utilice como mecanismo para imponer un régimen de habilitación previa a los generadores de contenido, condicionando la posibilidad misma de comunicación con usuarios. Aunque la CRC administra legítimamente ciertos recursos de identificación, esa competencia debe ejercerse dentro de los límites propios de la administración técnica, eficiente y segura de tales recursos, sin convertirlos en un instrumento de autorización previa de actividades económicas o de comunicaciones legítimas.

Ahora bien, se reconoce la importancia del SENDER ID como herramienta para identificar con mayor claridad al originador de comunicaciones A2P, reducir la suplantación y mejorar la confianza del usuario. Sin embargo, convertirlo en requisito administrativo previo, con asignación única por entidad, exigencias de validación, causales de recuperación y dependencia del validador centralizado, puede transformarlo en una barrera de acceso y permanencia en el mercado.

Un régimen de asignación previa, con tiempos administrativos y causales de recuperación, resulta incompatible con la velocidad operativa de los servicios digitales y con la incorporación ágil de nuevos remitentes legítimos. La consecuencia práctica es la imposición de barreras de entrada para startups, comercios digitales y desarrolladores, y de demoras para proveedores de mayor escala, con el riesgo de que servicios de seguridad no puedan operar en Colombia.

1.1. Establecimiento de una sucursal en Colombia

De otro lado, el Parágrafo 2 del artículo 6.12.1.2 dispone que “a cada persona natural o jurídica le será asignado un único SENDER ID”; solo se asignará “un SENDER ID por NIT o por cédula”; y los solicitantes extranjeros podrán ser asignatarios “siempre que hayan establecido una sucursal en Colombia”. La exigencia de sucursal se reitera en el numeral 6.12.2.1.1 del Proyecto de Resolución.

La exigencia de establecer una sucursal en el país como condición para enviar mensajes de autenticación y seguridad a usuarios en Colombia resulta desproporcionada y potencialmente discriminatoria frente a los proveedores extranjeros. Obligar a una presencia local permanente para el ejercicio de una función puramente técnica de identificación no es una medida proporcional y, de hecho, impone una carga estructural gravosa que no guarda relación de necesidad ni con el fin de identificar al remitente.

Adicionalmente, esta obligación puede generar tensiones con los compromisos internacionales asumidos por Colombia en materia de comercio transfronterizo de servicios. En particular, el TLC con Estados Unidos contempla disciplinas orientadas a evitar que la prestación transfronteriza de servicios sea condicionada a la obligación de establecer presencia local en el territorio de la otra parte. Por ello, una medida que exige a proveedores extranjeros constituir una sucursal en Colombia como condición para acceder al SENDER ID y cursar mensajes A2P podría ser incompatible con dichos compromisos.

Finalmente, la exigencia de una sucursal obligatoria puede desincentivar la prestación de servicios de seguridad desde el exterior y podría impedir o desincentivar que ciertos proveedores globales mantengan el SMS como canal de autenticación en Colombia, llevando a los usuarios a alternativas menos seguras o reduciendo la disponibilidad de mecanismos de autenticación robusta en el país. Ello afectaría la seguridad del ecosistema digital, que el propio Proyecto pretende proteger.

Adicionalmente, la exigencia de establecer una sucursal en Colombia debe analizarse junto con las cargas operativas que se derivan del modelo de validación propuesto. Aunque el Proyecto no lo señala expresamente, la obligación de gestionar plantillas con vigencia mensual, atender eventuales rechazos en plazos de 24 a 48 horas, interactuar con el validador centralizado y mantener actualizados los registros asociados al SENDER ID puede generar, en la práctica, la necesidad de contar con una estructura operativa local o dedicada para cumplir con el régimen.

Esta carga resulta especialmente gravosa para proveedores de servicios digitales transfronterizos que operan bajo modelos globales de seguridad, autenticación y mensajería transaccional. En estos casos, las comunicaciones de seguridad, OTP, 2FA, alertas de fraude y verificación de identidad suelen gestionarse mediante infraestructuras automatizadas, centralizadas o distribuidas internacionalmente, diseñadas para operar de manera continua y con altos niveles de disponibilidad. Someter estos flujos a trámites locales, revisión periódica de plantillas y eventuales procesos de subsanación ante un validador puede introducir fricciones operativas que no guardan una relación directa con la mejora técnica de la seguridad.

En la práctica, la combinación entre presencia local obligatoria, validación mensual de plantillas, interacción permanente con un tercero privado y posibles bloqueos por ausencia de aprobación vigente puede desincentivar que proveedores globales mantengan el SMS o el USSD como canales de autenticación segura para usuarios en Colombia. Esto podría generar un efecto contrario al buscado por la regulación, pues los usuarios colombianos podrían enfrentar menor disponibilidad de mecanismos de autenticación, recuperación de cuenta, verificación de identidad o alertas de seguridad utilizados bajo estándares globales.

Por lo anterior, el Proyecto debería evitar trasladar a los proveedores de servicios digitales cargas operativas locales que no sean estrictamente necesarias, idóneas y proporcionales para prevenir el fraude. En particular, debería contemplar esquemas diferenciados para comunicaciones críticas de seguridad y autenticación, así como mecanismos automatizados, interoperables y basados en riesgo que permitan preservar la disponibilidad continua de servicios digitales sin imponer estructuras locales o trámites recurrentes que puedan afectar la operación transfronteriza.

En consecuencia, se recomienda eliminar la exigencia de sucursal en Colombia para proveedores extranjeros y sustituirla por mecanismos menos restrictivos de identificación, trazabilidad, representación para efectos de notificación, interoperabilidad técnica y cooperación frente a incidentes de seguridad, sin condicionar la prestación de servicios digitales transfronterizos a una presencia local permanente.

1.2. Mensajes de autenticación y seguridad (Artículos 6.12.1.3.1, 6.13.4.1 y 6.13.4.7.2)

El artículo 6.12.1.3.1 establece que los mensajes de autenticación y seguridad (OTP, alertas de inicio de sesión, confirmaciones) se generan a solicitud del usuario y no requieren consentimiento adicional. No obstante, los artículos 6.13.4.1 y 6.13.4.7.2 exigen que todo mensaje A2P, incluida la autenticación, cuente con plantilla aprobada y vigente, y disponen que en su ausencia el PRST podrá bloquear el mensaje o marcarlo como “sin verificar”.

Al respecto, se considera que el Proyecto incurre en una contradicción pues en principio reconoce la naturaleza especial de los mensajes de autenticación y luego los somete al mismo control previo de contenido y a la misma posibilidad de bloqueo que la mensajería comercial o publicitaria. Estos mensajes son generados a solicitud activa del propio usuario en un momento específico, lo que descarta que se trate de comunicaciones imprevistas o no deseadas que por sí solas puedan generar casos de fraude.

Las características técnicas de estos mensajes hacen de difícil cumplimiento algunas de las medidas propuestas por la CRC. Los OTP contienen variables dinámicas, son sensibles al tiempo y se cursan en volúmenes elevados con exigencias de disponibilidad casi absoluta. Aunque el Proyecto no necesariamente exige aprobar el valor exacto de cada OTP, sí somete la plantilla, el contenido estático, el sentido del contenido dinámico y el enrutamiento del mensaje a un esquema de validación previa y consulta operativa que puede generar falsos bloqueos, latencia o indisponibilidad.

La aprobación previa, la vigencia mensual de la plantilla, incluso si es de renovación automática, y la consulta en tiempo real al validador antes de enrutar cada mensaje añaden latencia y barreras para su adecuado funcionamiento. De hecho, cualquier interrupción en la entrega de un OTP impide, por ejemplo, el inicio de sesión o la recuperación de cuenta. Entonces, el costo de un falso bloqueo de un mensaje de seguridad es muy superior al de un mensaje comercial no entregado. El efecto de la propuesta sería desconocer la importancia de la herramienta que mejor protege a los usuarios, en contra del propio objetivo del Proyecto de Resolución.

2. Validador centralizado (Artículos 6.13.1.1 a 6.13.1.6 y 18)

Los artículos 6.13.1.1 a 6.13.1.6 y 18 crean un validador centralizado, entendido como una persona jurídica única seleccionada por los PRST móviles y financiada por los asignatarios de código corto A2P, encargado de la verificación del KYC, de la aprobación de plantillas y de la emisión de certificaciones, sin cuyo aval no es posible acceder a los recursos ni cursar tráfico.

Esta configuración impone una arquitectura compleja que puede entorpecer la operación técnica y generar distorsiones en el mercado, al superponer un intermediario obligatorio en la cadena de valor de la mensajería A2P. Resulta especialmente preocupante que el Proyecto concentre en un actor privado único funciones que condicionan el acceso al mercado, la asignación de recursos y el flujo de comunicaciones.

La delegación en un particular de funciones que condicionan el ejercicio de una actividad económica y el flujo de comunicaciones exige una base legal clara. La ausencia de una habilitación legal expresa sobre el validador central plantea problemas de legalidad y proporcionalidad. Además, aunque el Proyecto prevé supervisión por parte de la CRC o del Administrador de Recursos de Identificación, no establece salvaguardas suficientes de debido

proceso, auditoría, responsabilidad, transparencia, no discriminación y mecanismos de revisión frente a decisiones del validador.

Por otra parte, la creación de un validador único introduce riesgos sistémicos y de eficiencia para el ecosistema. En primer lugar, un validador único constituye un punto de falla que podría afectar masivamente la entrega de mensajes críticos, salvo que se incorporen mecanismos robustos de contingencia, validación diferida o reglas de continuidad para comunicaciones de seguridad. En segundo lugar, al carecer de presión competitiva, este modelo puede desincentivar la innovación tecnológica en soluciones de validación. Por último, el esquema traslada el costo financiero de esta infraestructura a los asignatarios de código corto A2P, obligándolos a financiar un actor privado cuya gobernanza y estructura deben estar sometidas a controles estrictos.

Adicionalmente, el Proyecto parte de una premisa institucional y técnica discutible al concentrar la validación del ecosistema en un único validador centralizado, operado por un tercero privado. En lugar de promover una arquitectura flexible, interoperable y basada en estándares técnicos, la propuesta crea un intermediario obligatorio que se convierte en punto único de falla, añade costos, introduce latencia y puede limitar la integración de soluciones tecnológicas ya existentes en el mercado.

Una alternativa menos restrictiva y más compatible con la innovación sería adoptar un enfoque basado en interoperabilidad, estándares abiertos y protocolos técnicos comunes. Bajo este modelo, los distintos actores del ecosistema podrían intercambiar información relevante para la prevención del fraude, la verificación del remitente, el reporte de incidentes y la trazabilidad de mensajes, sin necesidad de someter todo el flujo operativo a la autorización de un único tercero privado.

En particular, la CRC podría promover la adopción de estándares técnicos de intercambio de información para procesos de KYC, reportes de fraude, validación de remitentes, señales de riesgo y mecanismos de respuesta ante incidentes. Este enfoque permitiría que proveedores nacionales y globales integren sus propios sistemas de verificación y monitoreo con el ecosistema colombiano de forma automatizada, segura y auditable, sin sacrificar continuidad operativa ni imponer una barrera de acceso al mercado.

Este tipo de arquitectura también permitiría una reacción más ágil y coordinada entre PRST, asignatarios de códigos cortos A2P, proveedores de contenidos y aplicaciones, plataformas tecnológicas, comercios electrónicos y autoridades competentes frente a amenazas de seguridad. En lugar de depender de una validación previa centralizada para cada elemento operativo, el sistema podría apoyarse en trazabilidad, reportes oportunos, intercambio de señales de riesgo, auditorías posteriores y controles reforzados frente a actores o patrones de comportamiento de alto riesgo.

Por lo anterior, se recomienda reconsiderar la creación de un validador centralizado único y evaluar esquemas alternativos basados en interoperabilidad, estándares técnicos abiertos, APIs seguras, validación descentralizada y supervisión regulatoria ex post. Esta aproximación permitiría cumplir el objetivo de prevención del fraude de manera menos restrictiva, más resiliente y más alineada con la neutralidad tecnológica.

En consecuencia, se solicita a la CRC evaluar alternativas menos restrictivas al validador centralizado, incluyendo modelos de validación descentralizada, interoperabilidad técnica, APIs seguras, estándares comunes de intercambio de información y mecanismos de supervisión posterior, de manera que la prevención del fraude no dependa de un único intermediario privado ni genere barreras innecesarias para la operación de servicios digitales legítimos.

3. Plantillas de contenido obligatorias, aprobación previa y vigencia mensual (Artículos 6.13.4.1 a 6.13.4.3)

Los artículos 6.13.4.1 a 6.13.4.3, junto con la definición de Plantilla de contenido A2P, disponen que ningún mensaje A2P puede cursarse sin una plantilla aprobada y vigente; que el validador revisa el contenido estático y el sentido del contenido dinámico; que las plantillas tienen vigencia mensual renovable; y que la aprobación o el rechazo se resuelven en plazos de 24 a 48 horas.

El Proyecto instaura un mecanismo de aprobación previa de plantillas como condición para cursar comunicaciones A2P. Este esquema debe analizarse con especial cuidado, pues puede operar como un control previo sobre comunicaciones legítimas y generar restricciones desproporcionadas a la libertad de empresa, la libre competencia y la continuidad de servicios digitales.

Aunque la renovación sea automática, mantener una vigencia mensual y causales amplias de desactivación introduce incertidumbre operativa para servicios críticos. En particular, si la plantilla puede ser suspendida, rechazada o desactivada por criterios amplios o poco determinados, como los establece el Proyecto de Resolución, los remitentes legítimos enfrentan un riesgo operativo permanente que puede afectar comunicaciones de seguridad, autenticación, alertas de fraude o mensajes transaccionales necesarios para la prestación de servicios digitales.

Además, los servicios digitales modifican textos, idiomas, variables y enlaces de manera continua y a gran escala. Exigir una plantilla aprobada por mensaje o campaña, con vigencia mensual y revisión del contenido dinámico, es incompatible con flujos automatizados y con la personalización legítima. En el caso de los OTP, el contenido dinámico es, por diseño, impredecible. El esquema introduce latencia, costos y fragilidad operativa, y traslada al validador decisiones que afectan la entrega de mensajes legítimos, con un incentivo estructural a la sobre-restricción para evitar responsabilidad.

Adicionalmente, el esquema de plantillas obligatorias y aprobación previa de contenido introduce una visión estática de la seguridad digital que puede resultar incompatible con la evolución tecnológica de las herramientas de prevención del fraude. El fraude cibernético, particularmente mediante técnicas de ingeniería social, suplantación y smishing, evoluciona de manera rápida y dinámica, por lo que su mitigación no depende únicamente de la revisión previa de textos o contenidos predeterminados.

En la actualidad, buena parte de las soluciones de seguridad digital se orientan hacia modelos basados en análisis de riesgo, inteligencia artificial y aprendizaje automático, que permiten identificar patrones anómalos de tráfico, comportamientos sospechosos, intentos de suplantación o variaciones inusuales en tiempo real. Estos mecanismos requieren flexibilidad

para ajustar mensajes de alerta, autenticación o verificación según el contexto de riesgo, el tipo de amenaza detectada y las características del usuario o de la transacción.

Por ello, condicionar el envío de mensajes A2P a una plantilla previamente aprobada y vigente puede limitar la capacidad de los sistemas de seguridad para responder de manera inmediata ante amenazas emergentes. En particular, un modelo rígido de contenido puede impedir que proveedores de servicios digitales, comercios electrónicos, entidades financieras, plataformas tecnológicas y demás actores del ecosistema ajusten oportunamente sus comunicaciones de seguridad, alertas de fraude o factores de autenticación cuando una amenaza sea detectada por herramientas automatizadas o sistemas de inteligencia artificial.

Esta rigidez puede generar un efecto contrario al buscado por el Proyecto de Resolución: en lugar de fortalecer la seguridad del usuario, podría retrasar la respuesta frente al fraude, reducir la efectividad de mecanismos de prevención y desincentivar la adopción de tecnologías más avanzadas de detección y mitigación. En esa medida, el Proyecto debería evitar que la regulación de SMS y USSD se convierta en una barrera para el uso de soluciones dinámicas, automatizadas y basadas en riesgo.

En línea con el principio de neutralidad tecnológica, la regulación no debería privilegiar un único modelo de control basado en revisión previa de contenido, sino permitir esquemas alternativos y más flexibles de mitigación del fraude, tales como monitoreo posterior, validación basada en riesgo, auditorías selectivas, trazabilidad del remitente, mecanismos de reporte y controles reforzados únicamente frente a patrones o agentes de alto riesgo.

Por lo anterior, se recomienda que el Proyecto excluya expresamente de la obligación de aprobación previa de plantillas a los mensajes de autenticación, seguridad, verificación de identidad, alertas de fraude y comunicaciones transaccionales críticas, o que, como mínimo, permita para estos casos un esquema diferenciado basado en riesgo, trazabilidad y monitoreo posterior, que no impida la respuesta inmediata frente a amenazas cibernéticas.

4. Bloqueo o etiquetado de mensajes sin plantilla por el PRST (Artículo 6.13.4.7.2)

El artículo 6.13.4.7.2 obliga al PRST a verificar, antes de enrutar cada mensaje A2P, la existencia de código corto A2P, SENDER ID y plantilla vigentes en el sistema validador, y dispone que, en ausencia de alguno de estos elementos, el PRST deberá bloquear el mensaje impidiendo su entrega al usuario final o, alternativamente, a su elección, marcarlo con la etiqueta de no verificado.

Al respecto, condicionar el enrutamiento de cada comunicación a una consulta de verificación genera una dependencia operativa y añade una latencia inadmisible a la red. Bajo esta arquitectura, cualquier retraso técnico en la consulta o un falso negativo en el sistema central se traducirá en el bloqueo automático de interacciones críticas que requieren inmediatez, tales como las alertas de fraude o los códigos de autenticación, lo cual perjudicará gravemente a los usuarios y a los remitentes globales.

Además, la alternativa de marcar un mensaje de seguridad legítimo con la etiqueta de “sin verificar” resulta ser una medida equívoca y contraproducente. En lugar de alertar eficazmente, esta señalización induce a error al usuario y mina su confianza en las comunicaciones que son, precisamente, las que buscan proteger su identidad y su patrimonio. El costo económico y reputacional de un falso bloqueo o de una mala catalogación sobre una

comunicación crítica es desproporcionadamente elevado y asimétrico frente al beneficio marginal que el Proyecto pretende obtener mediante una exigencia procedimental.

En consecuencia, se recomienda que los mensajes de autenticación, seguridad, recuperación de cuenta, verificación de identidad, alertas de fraude y demás comunicaciones transaccionales críticas no sean objeto de bloqueo automático por falta de plantilla vigente o por fallas de consulta al validador. En su lugar, el Proyecto debería contemplar mecanismos de continuidad operativa, validación diferida, monitoreo posterior y gestión basada en riesgo, con el fin de evitar que un falso negativo o una falla técnica afecte la seguridad y el acceso de los usuarios a servicios digitales.

5. KYC, identificación del beneficiario final y conservación por cinco años (Artículos 6.13.3.1 y 6.13.3.2)

De acuerdo con el Proyecto de Resolución, los asignatarios de SENDER ID iniciarán ante los asignatarios de código corto A2P el proceso de KYC como clientes, obtendrán la certificación correspondiente y formalizarán los contratos requeridos. Frente a este modelo es importante señalar que el PCA asume la posición de cliente y debe ser examinado y certificado.

Al respecto, el Proyecto de Resolución incluye cargas administrativas desproporcionadas y obligatorias para los PCA que no aportan seguridad al ecosistema y sí generan costos y demoras injustificadas para el PCA. Antes de acceder al SENDER ID, el PCA queda sujeto a un trámite de habilitación ante un particular y a la obtención de una certificación. El resultado es trámites excesivos sobre el mismo sujeto dado que el asignatario del código corto A2P examina al PCA y el validador vuelve a revisar ese examen.

Además, la habilitación previa del PCA implica la imposición de barreras de acceso al mercado, que además depende de la decisión de un tercero particular. Esta subordinación operativa no solo restringe injustificadamente la libre entrada de nuevos competidores, sino que carece de control estatal directo, lo que incrementa el riesgo de conductas discriminatorias. Al condicionar la viabilidad comercial de un PCA a la discrecionalidad de un tercero independiente, se desincentiva la inversión en el sector y se ralentiza la adopción de innovaciones tecnológicas, perjudicando la eficiencia general del mercado de mensajería A2P.

El Proyecto define el KYC como un proceso de debida diligencia mediante el cual los asignatarios de código corto A2P deben verificar identidad, legitimidad y perfil de riesgo de los agentes con quienes contratan, con el propósito de prevenir el uso indebido de recursos de identificación para la comisión de fraudes por SMS. Resulta preocupante que el Proyecto exija la identificación del beneficiario final y disponga que el formato correspondiente sea elaborado con base en criterios de prevención del lavado de activos y financiación del terrorismo. La incorporación de estándares LA/FT en una regulación cuyo objeto es mitigar fraude por SMS puede generar ambigüedad jurídica, duplicidad regulatoria y cargas desproporcionadas para empresas que no son sujetos obligados bajo el régimen colombiano de prevención de LA/FT. Esto teniendo en cuenta que la debida diligencia LA/FT corresponde a un régimen legal especializado, con autoridades, sujetos obligados, metodologías y consecuencias propias.

Adicionalmente, es necesario evaluar la proporcionalidad de condicionar la asignación del SENDER ID a una certificación de KYC emitida dentro de un modelo centralizado. El Proyecto establece que el KYC es condición necesaria para que el validador centralizado expida la certificación requerida para la asignación del SENDER ID. Este diseño puede convertirse en una barrera para el acceso al mercado, especialmente para pequeñas empresas, desarrolladores, comercios electrónicos, startups y proveedores globales que operan con múltiples intermediarios o modelos de mensajería transaccional.

Finalmente, la redacción actual del artículo 6.13.3.1.7 resulta excesivamente amplia porque exige conservar la totalidad de la información KYC por cinco años después de la terminación del contrato, sin diferenciar entre tipos de datos, niveles de riesgo, existencia de incidentes, obligaciones legales específicas o necesidad probatoria. Ello puede implicar la retención prolongada de datos personales y empresariales sensibles, incluyendo información de representantes legales, documentos de identidad, beneficiarios finales, antecedentes, perfil de riesgo, información contractual y datos comerciales. Esta retención generalizada incrementa los riesgos de seguridad, acceso no autorizado, usos secundarios, duplicidad de bases de datos y exposición innecesaria de titulares y empresas a riesgos de seguridad.

En consecuencia, se recomienda que el Proyecto adopte un enfoque de KYC proporcional y basado en riesgo, que diferencie entre tipos de agentes, niveles de exposición, volumen de tráfico, antecedentes de incidentes y naturaleza de las comunicaciones. Asimismo, se recomienda eliminar la duplicidad de revisiones entre asignatarios de código corto A2P y validador centralizado, limitar la exigencia de información de beneficiario final a supuestos estrictamente necesarios y revisar el plazo de conservación de información para ajustarlo a criterios de necesidad, finalidad, proporcionalidad y seguridad de la información.

6. Atribución de responsabilidad por mal uso potencial de plantillas (Artículos 6.13.4.4 y 6.12.3.2.12)

El artículo 6.13.4.4 regula la atribución de responsabilidad por el mal uso de plantillas, y el numeral 6.12.3.2.12 establece como causal de recuperación del SENDER ID el envío de mensajes que potencialmente pueden ser atribuibles al mal uso de las plantillas y que sea imputable al asignatario.

Una causal de recuperación basada en lo potencialmente atribuible al mal uso de las plantillas introduce un estándar indeterminado y cercano a la responsabilidad objetiva, con la consecuencia gravísima de la pérdida del recurso y la desactivación de todas las plantillas del asignatario. La indeterminación afecta la tipicidad, la seguridad jurídica y el debido proceso protegidos en el artículo 29 de la Constitución Política. La responsabilidad debe fundarse en conocimiento efectivo, control real y una conducta verificable, y no en una simple potencialidad.

Adicionalmente, la recuperación del SENDER ID y la desactivación de plantillas pueden tener efectos operativos severos sobre comunicaciones legítimas, incluidas aquellas de autenticación, recuperación de cuenta, alertas de fraude, verificación de identidad y mensajes transaccionales. Por ello, una medida de esta naturaleza no debería proceder de manera automática ni con base en criterios amplios o indeterminados.

En consecuencia, se recomienda que el Proyecto precise los supuestos de responsabilidad, elimine referencias a conductas “potencialmente atribuibles” y establezca criterios claros de imputación, conocimiento efectivo, control material, gradualidad y debido proceso. Asimismo, antes de aplicar medidas como la recuperación del SENDER ID o la desactivación de plantillas, deberían preverse mecanismos de requerimiento previo, subsanación, contradicción, revisión de la decisión y proporcionalidad de la medida frente a la gravedad del incumplimiento.

III. Recomendaciones generales

Con fundamento en los comentarios anteriores, se recomienda a la CRC revisar integralmente el diseño regulatorio propuesto, con el fin de evitar que una medida orientada a prevenir el fraude termine afectando la seguridad digital, la continuidad de servicios críticos, la innovación tecnológica, la libre competencia y la operación transfronteriza de servicios digitales legítimos.

En particular, se recomienda:

1. Precisar el alcance de las competencias legales de la CRC frente a los PCA y evitar que la administración de recursos de identificación se convierta en un régimen de habilitación previa para actores que no tienen la calidad de PRST.
2. Excluir expresamente de la aprobación previa de plantillas y del bloqueo automático a los mensajes de autenticación, OTP, 2FA, recuperación de cuenta, verificación de identidad, alertas de fraude y demás comunicaciones transaccionales críticas.
3. Eliminar la exigencia de sucursal en Colombia para proveedores extranjeros y sustituirla por mecanismos menos restrictivos de identificación, trazabilidad, notificación, interoperabilidad y cooperación frente a incidentes de seguridad.
4. Reconsiderar la creación de un validador centralizado único y evaluar esquemas alternativos basados en interoperabilidad técnica, estándares abiertos, APIs seguras, validación descentralizada, intercambio de señales de riesgo y supervisión posterior.
5. Adoptar un enfoque de validación basado en riesgo, con controles reforzados para agentes, patrones o contenidos de alto riesgo, en lugar de imponer un régimen uniforme de validación previa para todo tipo de mensajes A2P.
6. Permitir el uso de soluciones tecnológicas dinámicas, automatizadas y basadas en inteligencia artificial o aprendizaje automático para la detección y mitigación del fraude, evitando que el esquema de plantillas limite la capacidad de respuesta frente a amenazas emergentes.
7. Revisar las obligaciones de KYC para asegurar que sean proporcionales, no dupliquen cargas existentes, no incorporen indebidamente estándares LA/FT a sujetos no obligados y no generen barreras innecesarias para startups, comercios electrónicos, desarrolladores y proveedores globales.
8. Ajustar las reglas de conservación de información KYC para que respondan a criterios de finalidad, necesidad, proporcionalidad, seguridad y minimización de datos.

9. Precisar las causales de recuperación del SENDER ID y de desactivación de plantillas, eliminando estándares indeterminados como el mal uso “potencialmente atribuible” y garantizando reglas claras de imputación, gradualidad, contradicción y debido proceso.

10. Incorporar mecanismos de continuidad operativa, validación diferida, contingencia y monitoreo posterior para evitar que fallas técnicas del validador, retrasos administrativos o falsos negativos afecten la entrega de comunicaciones críticas para la seguridad de los usuarios.

En conclusión, se comparte el objetivo de fortalecer la protección de los usuarios frente al fraude cibernético. No obstante, dicho propósito debe alcanzarse mediante medidas proporcionadas, técnicamente viables, compatibles con la innovación y respetuosas de los límites legales de la intervención regulatoria. Un enfoque basado en riesgo, interoperabilidad, trazabilidad, cooperación público-privada y supervisión posterior permitiría mitigar el fraude de manera más efectiva, sin afectar la disponibilidad de servicios digitales críticos ni imponer barreras desproporcionadas al ecosistema digital.