



Bogotá, D.C., 23 de junio de 2026

Señores

COMISIÓN DE REGULACIÓN DE COMUNICACIONES – CRC Dirección Ejecutiva

medidasantifraude@crcom.gov.co

atencioncliente@crcom.gov.co.

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:

TransUnion® agradece la oportunidad de presentar comentarios sobre el proyecto regulatorio de la Comisión de Regulación de Comunicaciones (en adelante “CRC”) para mitigar el fraude cibernético a través de servicios móviles. El proyecto de regulación representa un esfuerzo significativo y con visión de futuro para abordar el smishing, vishing, suplantación (spoofing), uso indebido de recursos de identificación y la erosión general de la confianza del consumidor en los canales de telecomunicaciones.

Con base en nuestra revisión del proyecto regulatorio, TransUnion® observa respetuosamente que la CRC está desarrollando algo más que establecer reglas puntuales contra el fraude; la propuesta crea la base para un marco nacional de confianza para la mensajería A2P y voz.

La protección del consumidor y la integridad de los canales de comunicación constituyen prioridades compartidas por todos los actores del ecosistema. Por esta razón, TransUnion® considera que la implementación del nuevo régimen debe procurar, simultáneamente, efectividad en la prevención del fraude, continuidad operacional, protección de la información, competencia efectiva y condiciones objetivas de acceso para diversos participantes del ecosistema.

TransUnion® cuenta con experiencia en soluciones de identidad, prevención y detección de fraude, analítica, verificación y gestión de riesgos aplicables a ecosistemas de telecomunicaciones y comunicaciones digitales. A través de nuestro negocio denominado “Trusted Communications Solutions”, TransUnion® trabaja con operadores, empresas, organismos de la industria y actores del ecosistema para restaurar la confianza en los canales afectados por suplantación.

Asimismo, cuenta con conocimiento profundo del mercado colombiano, y de los retos asociados a la prestación y protección de canales de contacto seguros que habilitan confianza y desarrollo.

La experiencia internacional demuestra que restaurar la confianza requiere más que bloquear actores maliciosos. Se necesitan validación de identidad, analítica, controles anti-spoofing, gobernanza y transparencia hacia el consumidor.



En ese contexto, TransUnion® manifiesta su interés en contribuir al diseño y en participar en la implementación del esquema propuesto. Para tal efecto, respetuosamente presentamos las siguientes observaciones:

1. Proceso de Selección de Validador Centralizado

Se considera imperativo que el proceso de selección del Validador Centralizado definido en el artículo 18 del Proyecto Reglamentario se ajuste a estándares rigurosos de transparencia, objetividad y concurrencia, incorporando, como mínimo las siguientes salvaguardas:

- a. Una convocatoria abierta que permita la participación de terceros neutrales, especializados e idóneos.
- b. La publicación previa de criterios técnicos, operativos, de seguridad, independencia, gobernanza y experiencia relevante.
- c. La documentación objetiva de los criterios de elegibilidad, metodologías de evaluación, puntajes y razones que fundamenten la decisión de selección.
- d. Mecanismos claros para que la CRC pueda revisar la conformidad del proceso con los principios de transparencia, competencia, independencia, imparcialidad y no discriminación.
- e. La incorporación de criterios que evalúen experiencia en validación de identidad, gestión de riesgo de fraude, procesamiento transaccional de alta disponibilidad, seguridad de la información y gobernanza de ecosistemas de telecomunicaciones.
- f. Un plan documentado de transición, continuidad operacional y entrega ordenada de información en caso de sustitución del validador luego del período inicial de operación.

2. Claridad sobre independencia y conflictos de interés

El numeral 6.13.1.3.4 propone que el validador centralizado no tenga vínculos accionarios, contractuales o de control con los PRSTM, asignatarios de código corto A2P o sus respectivos grupos empresariales, cuando tales vínculos puedan comprometer su independencia e imparcialidad.

TransUnion® comparte la importancia de preservar la autonomía, objetividad e imparcialidad del validador. No obstante, se considera necesario precisar los criterios para identificar cuándo un vínculo contractual, accionario o de control compromete efectivamente dicha independencia.

Una interpretación amplia o absoluta podría restringir injustificadamente el universo de posibles participantes, especialmente en un mercado especializado donde los proveedores con experiencia relevante pueden mantener relaciones comerciales legítimas con actores del ecosistema de telecomunicaciones.

Por tanto, se solicita que la CRC precise que la incompatibilidad debe originarse exclusivamente en vínculos que, por su naturaleza, alcance, duración o efecto económico, generen un conflicto de interés real, actual y verificable frente al ejercicio de las funciones de validación.

Asimismo, se propone que la regulación permita acreditar la independencia mediante medidas de mitigación tales como segregación funcional, gobierno corporativo, controles de acceso, murallas de información, auditorías independientes, declaración y administración de conflictos de interés, y mecanismos de supervisión por parte de la CRC.



Se solicita aclarar expresamente que la prohibición no incluye los contratos de operación o prestación de servicios, siempre que estén sujetos a condiciones objetivas, transparentes y no discriminatorias.

3. Interoperabilidad, modularidad y uso de proveedores especializados

El esquema propuesto exige capacidades tecnológicas diversas, incluyendo procesos de KYC, validación documental, verificación de marcas y plantillas, administración de registros, gestión de URLs y dominios, análisis de incidentes, interfaces de consulta en tiempo real, seguridad de la información y reportes regulatorios.

Por tal razón, se considera conveniente que la regulación permita que la persona jurídica seleccionada como validador centralizado actúe como responsable integral frente a la CRC, aun cuando para determinados componentes tecnológicos, operativos o de ciberseguridad pueda apoyarse en proveedores especializados.

Este modelo permitiría mantener un único responsable frente al cumplimiento de las obligaciones regulatorias, sin impedir el aprovechamiento de capacidades complementarias de terceros. La posibilidad de integrar soluciones interoperables y especializadas puede fortalecer la innovación, la resiliencia tecnológica, la seguridad y la capacidad de respuesta del modelo.

En consecuencia, se solicita precisar que la prohibición de delegar funciones de verificación documental y KYC no impide el uso de herramientas tecnológicas, infraestructura, analítica, ciberseguridad o proveedores especializados, siempre que el validador conserve la dirección, control, responsabilidad y trazabilidad integral de dichas funciones.

Respecto de aquellas actividades que requieran autorización expresa de la CRC, se solicita establecer un procedimiento claro, objetivo y oportuno para obtener dicha autorización, evitando que la operación del sistema dependa de decisiones discrecionales o de trámites que puedan afectar la continuidad del servicio.

4. Neutralidad tecnológica y requerimientos técnicos

La regulación debería evitar imponer arquitecturas cerradas, herramientas específicas o soluciones propietarias que limiten la participación de proveedores con capacidades equivalentes o superiores. Los requisitos técnicos deben permitir que los participantes propongan soluciones innovadoras, siempre que acrediten el cumplimiento de los niveles mínimos de desempeño, seguridad y continuidad exigidos por la CRC y formularse bajo un enfoque de neutralidad tecnológica basado en resultados.

5. Sostenibilidad económica y Fase II de remuneración



La efectividad del modelo de validación centralizada dependerá, en buena medida, de la definición que adopte la CRC en la Fase II del proyecto, relativa a la remuneración e incentivos aplicables al ecosistema A2P.

TransUnion® considera importante que el modelo económico permita inversiones sostenibles en validación, seguridad, monitoreo, reportes, gestión de incidentes y protección del consumidor. Un esquema que imponga obligaciones operativas relevantes sin mecanismos económicos viables puede generar barreras de implementación o incentivos no deseados.

Por lo anterior, se solicita que la CRC considere desde la Fase I mecanismos que contemplen la recuperación razonable de costos asociados a la validación e infraestructura de confianza; una distribución clara de responsabilidades económicas entre los actores beneficiados por el sistema; incentivos para procesos robustos de KYC, gestión de plantillas y monitoreo antifraude; criterios de asequibilidad que prevengan el abuso de los canales; y tratamientos diferenciados para casos de uso de mayor o menor riesgo, con base en parámetros objetivos.

6. Autorregulación sectorial

TransUnion® considera conveniente que la CRC promueva, bajo su supervisión y en coordinación con los actores del ecosistema, una hoja de ruta de autorregulación sectorial dirigida a recuperar la confianza.

Las medidas previstas en el proyecto sobre suplantación de CLI, etiquetado de llamadas sospechosas o publicitarias, monitoreo de tráfico y controles de no originación constituyen avances importantes. Sin embargo, el diseño de mecanismos de confianza en voz puede requerir una evolución gradual, flexible y coordinada que permita al ecosistema adaptar estándares y prácticas a los cambios tecnológicos y a las modalidades de fraude.

Esta hoja de ruta podría considerar, entre otros aspectos, mecanismos de verificación de identidad de organizaciones legítimas, etiquetas positivas, información contextual sobre la finalidad de la llamada, controles antisuplantación, métricas de reducción de fraude y falsos positivos, así como prácticas consistentes entre operadores.

7. Convergencia futura entre voz, mensajería y otros canales

El proyecto incorpora elementos relevantes para fortalecer la confianza tanto en mensajería como en voz. TransUnion® considera importante que el diseño regulatorio preserve flexibilidad para una convergencia futura entre los mecanismos de validación de identidad empresarial, KYC, SENDER ID, validación de marcas, gobierno de plantillas, identidad de llamadas, inteligencia antifraude y educación al consumidor.

Los esquemas de fraude no se presentan de manera aislada. Los actores maliciosos pueden alternar entre SMS, llamadas de voz, mensajería por aplicaciones, correo electrónico y otros canales digitales. Por esta razón, resulta conveniente evitar que el desarrollo regulatorio genere silos rígidos entre voz y mensajería que impidan el intercambio de aprendizajes, capacidades de verificación o mecanismos de confianza.

Una lección clave: los beneficios son mayores cuando las soluciones se ofrecen nativamente en la red, sin depender de aplicaciones Over the Top (OTT).



Esta recomendación no implica adoptar una única tecnología ni imponer una plataforma común para todos los canales. Busca que el marco regulatorio actual no impida la evolución futura hacia arquitecturas interoperables, modulares y adaptables a las necesidades del ecosistema.

8. Implementación y transición

El proyecto contempla un período de transición de seis meses, dentro del cual se concentrarían la selección del Validador Centralizado, la habilitación de su infraestructura, y la integración con los PRST.

Aunque se comprende la necesidad de implementar oportunamente medidas de prevención del fraude, los plazos en el cronograma propuesto pueden resultar insuficientes frente a la complejidad técnica, contractual y operativa del modelo. El proceso para la selección de un proveedor, la suscripción de contratos, la implementación, las pruebas no productivas y el despliegue controlado de una plataforma crítica para el ecosistema requieren tiempos suficientes para asegurar calidad, seguridad y continuidad del servicio.

En consecuencia, se solicita a la CRC evaluar la ampliación del cronograma propuesto y establecer un esquema de implementación gradual. Este esquema debería supeditar la entrada en operación plena del régimen a la verificación de hitos objetivos de preparación técnica, pruebas de interoperabilidad, continuidad operacional, seguridad de la información y capacidad de atención de incidentes.

9. Aprendizajes internacionales para Colombia

La experiencia internacional muestra que diversos ecosistemas de comunicaciones han desarrollado marcos colaborativos para reducir la suplantación, el fraude, las robo llamadas, el phishing y otras formas de abuso, al tiempo que buscan recuperar la confianza de los consumidores en los canales de voz y mensajería.

- Brasil constituye un referente relevante para Colombia por las características de su mercado y por el desarrollo de iniciativas lideradas por ANATEL y ABR Telecom, orientadas a la autenticación de llamadas, mitigación de robo llamadas e identificación de organizaciones. La experiencia brasileña muestra la importancia de combinar liderazgo regulatorio, coordinación con operadores, gobernanza del ecosistema y transparencia frente a los usuarios.
- En Estados Unidos, las iniciativas de autenticación de llamadas y mitigación de robo llamadas han contado con la participación de la “Federal Communications Commission” y de actores sectoriales como la “Alliance for Telecommunications Industry Solutions”. Estas experiencias resaltan la necesidad de complementar los mecanismos técnicos de autenticación con validación de identidad empresarial, analítica, controles antifraude, gobernanza y transparencia al consumidor.
- Canadá también ofrece elementos de referencia a partir de los esfuerzos desarrollados por la “Canadian Radio-television and Telecommunications Commission”, los proveedores de telecomunicaciones y organismos de gobernanza relacionados con la autenticación de llamadas y controles antisuplantación. Esta experiencia evidencia la importancia de una colaboración sostenida entre reguladores, operadores, instancias de gobernanza y demás participantes del ecosistema.
- India es un punto de referencia importante porque demuestra cómo las comunicaciones confiables pueden evolucionar desde la prevención del fraude hasta una plataforma de confianza empresarial y de interacción con el cliente a gran escala. JioCX (PRST en India)



introdujo JioCX Verify, una solución de llamadas de marca verificadas destinada a permitir que las empresas se comuniquen con los consumidores utilizando identidad verificada, garantía de marca y capacidades mejoradas de interacción. Esta iniciativa resalta el valor comercial y de protección al consumidor del servicio de llamadas de marca nativas de red: las empresas verificadas pueden presentar información de identidad a los consumidores, los consumidores obtienen claridad y confianza, y los operadores pueden restaurar el valor del canal de voz. También ilustra el valor de la incorporación de empresas, el KYB (Conoce a tu negocio), la validación de activos y la gestión del ciclo de vida como capacidades fundamentales para las comunicaciones confiables.

- Las iniciativas de la GSMA (Asociación de PRST que representa más de mil operadores móviles, fabricantes y empresas afines) también apuntan hacia una dirección más amplia de la industria. GSMA Open Verifiable Calling explora un marco para construir confianza verificable directamente en las llamadas de voz mediante identidades verificadas, autorización de números telefónicos, nombres, logotipos, garantías criptográficas y la visualización en el dispositivo de la información del llamante verificado. GSMA Open Gateway también refleja el movimiento de la industria hacia APIs de red estandarizadas, incluidas capacidades relacionadas con la identidad como APIs de “Conoce a tu cliente” (KYC). Estas iniciativas refuerzan la importancia de servicios de confianza armonizados, reutilizables y basados en la red.

De estas experiencias se desprenden lecciones relevantes para Colombia:

- a. Las comunicaciones confiables requieren validación de identidad empresarial y no únicamente monitoreo de tráfico.
- b. Los modelos duraderos requieren reglas neutrales, transparentes, auditables y sujetas a una adecuada gobernanza.
- c. Los mecanismos de confianza prestados de manera nativa sobre las redes pueden alcanzar una mayor cobertura, sin depender de la adopción de aplicaciones externas por parte de los usuarios.
- d. La verificación positiva de organizaciones legítimas complementa las alertas y bloqueos frente a comunicaciones sospechosas.
- e. La colaboración entre reguladores, operadores, empresas y demás participantes resulta esencial para definir estándares, reglas de gobernanza y prácticas operativas consistentes.
- f. La sostenibilidad económica es determinante para la continuidad de las inversiones en confianza, seguridad y protección al consumidor.

Si bien las referencias internacionales no deben trasladarse de forma automática al contexto colombiano, su valor radica en aportar aprendizajes que puedan ser adaptados a las condiciones jurídicas, técnicas, competitivas y de mercado del país.

10. Conclusión

El proyecto de resolución constituye un avance relevante para fortalecer la confianza en el ecosistema colombiano de comunicaciones, reducir el fraude, mejorar la trazabilidad y aumentar la protección de los consumidores.



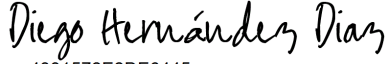
TransUnion® respalda la dirección propuesta por la CRC y considera que el validador centralizado, dadas las funciones que se le asignan, debe operar como un componente neutral de infraestructura de confianza para el ecosistema nacional de comunicaciones, y no únicamente como una herramienta administrativa de cumplimiento.

Para ello, resulta fundamental que el proceso de selección sea abierto, transparente, competitivo y objetivo; que las reglas de independencia se apliquen de manera clara y proporcional; que el modelo preserve la competencia, la interoperabilidad y la innovación; y que las fases posteriores promuevan una evolución sectorial hacia comunicaciones confiables prestadas de manera nativa sobre las redes de telecomunicaciones.

TransUnion® agradece a la CRC la oportunidad de presentar estos comentarios y manifiesta su disposición para participar en los espacios técnicos que se estimen pertinentes durante la evolución e implementación del proyecto regulatorio.

Cordialmente,

DocuSigned by:


4331572E2DE6445...

DIEGO ORLANDO HERNÁNDEZ DÍAZ

Representante Legal Suplente

dhernan@transunion.com

CIFIN S.A.S. - TransUnion®

Calle 100 No. 7a-81 Piso 8

Bogotá D.C.