CSTv –233-2026
Bogotá D.C., 23 de junio 2026

Doctor
FELIPE DÍAZ SUAZA
Director Ejecutivo
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Medidasantifraude@crcom.gov.co

Asunto: Comentarios al proyecto regulatorio “Medidas para Mitigar el Fraude Cibernético por Medio de Servicios Móviles”

Apreciado Dr. Felipe:

Reciba un cordial saludo de la Asociación Nacional de Empresas de Servicios Públicos y Comunicaciones en Colombia – ANDESCO.

En relación con el proyecto regulatorio de la referencia, previo a presentar nuestras consideraciones, debemos advertir que el término de publicación para comentarios no resulta suficiente para garantizar la participación ciudadana toda vez que en el presente caso la CRC publicó los documentos durante el tiempo mínimo previsto en el decreto 1078 de 2015 y no realizó durante este término ejercicios de socialización de las medidas propuestas, lo anterior no se compadece con la importancia del proyecto tanto para la industria como para la ciudadanía en general, los impactos que genera y la complejidad de los documentos publicados.

Si bien el 4 de julio de 2025 fue publicado el documento de formulación del problema de este proyecto y el 21 de noviembre de 2025 fue publicado para comentarios el documento de alternativas regulatorias, sólo hasta el pasado 5 de junio la CRC publicó la propuesta regulatoria como tal y dada la relevancia del problema que la CRC busca atender, consideramos que el término para revisar el documento soporte junto con las medidas propuestas y realizar los análisis de impacto por parte de los diferentes involucrados no es suficiente.

Sumado a esto, consideramos que la magnitud del proyecto, su alto componente técnico y los efectos de las medidas propuestas, ameritaban realizar espacios de socialización de la propuesta regulatoria en el término de participación ciudadana.

1. **Medidas de la propuesta regulatoria a resaltar**

Reconocemos, asimismo, que la creación de un ecosistema A2P trazable, basado en la identificación del originador real del mensaje, la diferenciación entre código corto A2P y Sender ID, la aplicación de procesos de conocimiento del cliente, y la existencia de un

mecanismo común de validación, constituye una línea regulatoria relevante para atacar una de las causas estructurales del fraude: la dificultad de atribuir responsabilidad sobre quien origina efectivamente el contenido enviado al usuario final.

En esa medida, nuestras observaciones no se dirigen a desmontar el modelo de trazabilidad A2P propuesto, sino a hacerlo idóneo, proporcional y sostenible. En particular, vemos con buenos ojos el proyecto y su objetivo de fortalecer la protección de los usuarios frente al fraude. No obstante, insistimos en que la desregulación de la tarifa mayorista del SMS A2P debe abordarse como una primera fase del proceso, o bien en que ambas medidas —el régimen antifraude y la definición o desregulación tarifaria del SMS A2P— se adopten de manera simultánea, de modo que las nuevas obligaciones cuenten con una fuente cierta de financiación y el modelo resulte sostenible. Consideramos además que la siguientes son herramientas razonables, proporcionales y potencialmente efectivas:

- **Estrategias de educación y concientización a usuarios**

Compartimos la importancia de fortalecer las estrategias de educación digital dirigidas a los usuarios finales, especialmente aquellas orientadas a incrementar el conocimiento sobre las modalidades de fraude más frecuentes, los mecanismos de suplantación de identidad y las recomendaciones para la protección de la información personal y financiera.

El fraude cibernético es un fenómeno que, en gran medida, explota factores asociados al comportamiento humano y a la ingeniería social. Por esta razón, las acciones de prevención y concientización constituyen herramientas complementarias fundamentales dentro de cualquier estrategia integral de mitigación del fraude.

En este sentido resaltamos la incorporación de medidas que promuevan campañas educativas, mecanismos de divulgación y acciones de sensibilización dirigidas a los usuarios.

- **Facultades para la suspensión preventiva de servicios asociados a posibles actividades fraudulentas**

Uno de los aspectos positivos de la propuesta es que fortalece las herramientas disponibles para que los PRST puedan adoptar medidas oportunas frente a situaciones en las cuales existan indicios razonables de utilización indebida de los servicios o de desarrollo de actividades potencialmente fraudulentas.

La posibilidad de suspender temporalmente la prestación de servicios asociados a campañas o actividades respecto de las cuales existan elementos objetivos que permitan inferir riesgos para los usuarios constituye una medida que puede generar efectos inmediatos en la contención del fraude y en la reducción de su impacto.

Adicionalmente, esta herramienta permite una actuación rápida frente a situaciones de riesgo, evitando que la materialización de los daños continúe mientras se realizan las verificaciones correspondientes.

Esta medida sumada con la suspensión provisional implementada por la CRC dentro del desarrollo de una actuación administrativa, y bajo una actuación expedita de la misma, logra mejores beneficios a favor de los usuarios.

- **Terminación de relaciones contractuales**

Consideramos igualmente adecuada la incorporación de mecanismos que permitan la terminación de relaciones contractuales cuando se acrediten incumplimientos graves asociados a actividades fraudulentas o al uso indebido de los servicios.

La posibilidad de excluir del ecosistema a actores que reiteradamente incumplen las condiciones regulatorias o contractuales constituye un incentivo importante para el cumplimiento y contribuye a preservar la confianza en los servicios de mensajería empresarial.

Este tipo de medidas tienen la ventaja de actuar directamente sobre los agentes responsables de las conductas indebidas, sin imponer cargas indiscriminadas sobre la totalidad de los participantes del mercado.

2. Comentarios relacionados con AIN y modificaciones contractuales

El artículo 2.2.13.3.2 del Decreto 1078 de 2015 exige que los proyectos regulatorios vayan acompañados de documentos soporte que incluyan la evaluación de impactos económicos de las medidas propuestas. El numeral 3 del artículo 2 de la Ley 1341 de 2009 exige que la regulación sea eficiente. Una regulación sin modelo económico verificable no cumple ese requisito. El artículo 22 numeral 1 de la Ley 1341 exige que la CRC maximice el bienestar social de los usuarios; sin cuantificar costos y beneficios, ese mandato no puede acreditarse como cumplido.

La metodología AIN exige que la evaluación de alternativas incorpore simultáneamente los impactos técnicos, operativos y económicos de cada medida. Separar artificialmente el análisis técnico (Fase I) del análisis económico (Fase II) fragmenta la intervención regulatoria y elimina la posibilidad de hacer un genuino análisis costo-beneficio. Los costos de implementación del validador centralizado dependen del volumen de tráfico A2P, que a su vez depende del precio de terminación que resulte de la Fase II. Un precio de $0.03/SMS haría insostenible el modelo de validación para muchos asignatarios de código corto. La Fase II se convierte en una promesa sin fecha, mientras las obligaciones de la Fase I entran a regir inmediatamente.

La ausencia de análisis económico impide evaluar la viabilidad y sostenibilidad de las medidas propuestas, generando riesgos de insostenibilidad financiera del esquema de validación, posible desincentivo a la inversion, riesgo de concentración del mercado en grandes agentes que puedan absorber los costos y posible traslado de costos a usuarios finales.

Consideramos que la CRC debe publicar simultáneamente con la resolución definitiva (o con carácter previo a su entrada en vigor) el análisis económico del mercado de terminación de SMS A2P, incluyendo: (i) estructura de costos del validador centralizado; (ii) esquema de recuperación de costos para los asignatarios del código corto; (iii) análisis de impacto sobre PCA/IT por tamaño; (iv) proyección de traslado de costos a usuarios finales. Alternativamente, la entrada en vigor de los artículos 12, 13, 14 y 19 debe quedar explícitamente condicionada a la publicación de ese análisis, no solo a la expedición del acto de remuneración A2P.

Adicionalmente, la evaluación multicriterio no incluyó el fortalecimiento de mecanismos actuales como alternativa comparada con el validador centralizado. Omitir esa comparación afecta la conclusión de que el validador es la mejor alternativa.

Asimismo, el artículo 2.1.10.7.3.4 confiere carácter vinculante a las decisiones técnicas del Comité, mientras el artículo 11.1.1.2.6 exime de publicación previa a las resoluciones que las adopten. Esto crea un mecanismo de regulación de facto que elude los requisitos del proceso AIN establecidos en el Decreto 1078 de 2015 y vulnera el derecho de participación ciudadana.

Por otra parte, el proyecto de resolución incluye obligaciones relacionadas con la modificación de los contratos de los PRST con entidades del sector financiero para incorporar deberes derivados de la regulación, consideramos la obligación de registrar o reportar la información correspondiente recae directamente sobre la entidad financiera, en su calidad de titular de la relación contractual con el usuario y de sujeto obligado por la regulación que establezca dicho deber. En consecuencia, no resulta razonable ni jurídicamente adecuado exigir a los PRST que gestionen modificaciones contractuales con terceros para asegurar el cumplimiento de obligaciones que no les corresponden. La CRC ante la ausencia de facultades para imponer obligaciones a las entidades financieras, traslada a los PRST responsabilidades sobre actuaciones que dependen exclusivamente de la voluntad y gestión de terceros, generando obligaciones de imposible o difícil cumplimiento.

3. Comentarios frente a la proporcionalidad de las medidas

En cuanto a la aplicación de los criterios que conforman el test de proporcionalidad frente a las medidas propuestas.

Idoneidad: las medidas son potencialmente idóneas para reducir el fraude en el canal SMS/voz, pero la CRC no demuestra el grado de eficacia esperado ni cuantifica la reducción de fraude proyectada. La ausencia de análisis del efecto sustitución hacia canales OTT es especialmente grave.

Necesidad: la CRC no acredita que las medidas propuestas sean la alternativa menos gravosa. No se evalúa ex post la efectividad de herramientas vigentes (suspensión provisional de códigos cortos, monitoreo y bloqueo de tráfico). La creación de un validador centralizado no es la única forma de fortalecer el KYC sobre asignatarios de códigos cortos.

Proporcionalidad estricta: los costos de implementación no fueron cuantificados. Sin ese dato, es imposible verificar si los beneficios superan los costos. Cargar simultáneamente con validador centralizado, plantillas, KYC, CTLFSM y medidas educativas sobre los mismos agentes, sin modelo económico que los sostenga, puede generar inviabilidad financiera para operadores pequeños y medianos.

4. Comentarios respecto del validador centralizado

La CRC propone crear una persona jurídica privada — seleccionada por los propios PRSTM — que tiene a su cargo la expedición de certificaciones habilitantes para acceder a recursos de identificación administrados por el Estado, la aprobación de plantillas que condicionan el envío de todo el tráfico A2P del país, la administración del KYC de todos los agentes del ecosistema y la operación del registro de marcas, ninguno de estos elementos fue comparado rigurosamente con la alternativa de fortalecer las capacidades internas de la CRC como Administradora de Recursos de Identificación.

Técnicamente, el validador centralizado introduce tres riesgos graves: (i) Single Point of Failure (SPOF): si el validador falla, todos los PRST del país pierden simultáneamente la capacidad de validar y enrutar tráfico A2P, afectando OTP bancarios, alertas de seguridad, notificaciones de emergencia y mensajería crítica de IoT. El SLA del 99.5% mensual permite hasta 3.6 horas de caída al mes, período durante el cual el ecosistema quedaría bloqueado. (ii) Honeypot para ciberataques: concentrar en un solo nodo la base de datos de todos los remitentes autorizados, todas las plantillas activas y todos los dominios validados del país crea un objetivo de alto valor para actores maliciosos. Un hackeo exitoso permitiría inyectar smishing masivo desde plantillas aprobadas. (iii) Cuello de botella de capacidad: el validador debe procesar las consultas simultáneas de todos los PRST del país (4 operadores activos con volúmenes de 6,000-12,000 consultas/segundo en hora pico). Ningún sistema centralizado puede garantizar esa disponibilidad con los tiempos de respuesta exigidos sin inversiones de infraestructura que la resolución no cuantifica.

No obstante, en vez de descartar la figura del validador, consideramos que esta puede constituir un instrumento útil para dotar al ecosistema A2P de trazabilidad homogénea, neutralidad operativa y reglas comunes de validación, siempre que su diseño regulatorio

incorpore salvaguardas suficientes para evitar riesgos sistémicos, indisponibilidad del servicio, afectación de mensajes legítimos y concentración indebida de información sensible. Así, las advertencias técnicas anteriores (punto único de falla, valor del nodo como objetivo de ciberataques y límites de capacidad) no deben entenderse como un rechazo a la figura, sino como la exigencia de un diseño institucional robusto.

En consecuencia, solicitamos que la CRC precise en la resolución reglas mínimas sobre gobernanza, independencia funcional, neutralidad, acceso no discriminatorio, confidencialidad, protección de datos, minimización de información, trazabilidad de consultas, auditoría, ciberseguridad, niveles de servicio, disponibilidad, redundancia, continuidad operacional y manejo de incidentes, tomando como referencia la gobernanza de la base de datos administrativa de portabilidad numérica. El validador deberá contar además con un plan de contingencia aplicable ante indisponibilidad total o parcial, degradación de sus APIs, incumplimiento de tiempos de respuesta, incidentes de seguridad o fallas de interoperabilidad, que preserve la entrega de mensajes legítimos, en especial los asociados a autenticación, seguridad, alertas transaccionales, salud, servicios públicos, entidades financieras y comunicaciones críticas para el usuario.

En ningún caso debería atribuirse responsabilidad regulatoria al PRST por fallas, indisponibilidad, degradación o incidentes del validador centralizado que no sean imputables a su red, operación o conducta.

5. **Validación sincrónica del tráfico A2P: necesidad de especificaciones técnicas previas y de continuidad operativa**

El artículo 6.13.4.7.2 obliga a los PRST a verificar, 'previo al enrutamiento de CADA mensaje A2P', que este cuente con código corto A2P válido, Sender ID asignado e implementado y plantilla aprobada y vigente en el sistema del validador. Esta exigencia de validación síncrona por mensaje individual es técnicamente incompatible con la arquitectura y capacidad de procesamiento de los SMSC de los operadores móviles colombianos.

Desde el punto de vista técnico la propuesta presenta los siguientes problemas: (i) Los SMSC de los operadores procesan entre 2,000 y 3,000 mensajes por segundo en hora pico. (ii) La validación síncrona al validador introduce una latencia adicional mínima de 200 ms por mensaje (tiempo de respuesta normal según Art. 6.13.2.1.2). (iii) Con 2,000 msg/seg y 200 ms de latencia adicional, el throughput efectivo se reduciría a aproximadamente 340-510 msg/seg: pérdida del 83% de capacidad. (iv) En condiciones de alta demanda del validador (500 ms según la norma), la latencia total superaría 610-890 ms por mensaje, violando los SLA de mensajería transaccional (OTP bancarios exigen entrega < 500 ms). (v) El validador centralizado debe atender simultáneamente las consultas de todos los operadores del país: 6,000 a 12,000 consultas/segundo. Ningún sistema de un único nodo puede sostener ese volumen con los tiempos exigidos. (vi) Los mensajes que no se procesen en tiempo real se acumularán en cola, generando timeouts SMPP y colapso del

servicio en horas pico. Los más afectados serían los mensajes OTP de autenticación bancaria, que son los más críticos para el usuario final.

La propuesta de norma crea una obligación de resultado (validación previa a cada mensaje) sin valorar la viabilidad técnica de su cumplimiento. El artículo 19 de la Ley 1341 de 2009 exige que la regulación sea técnica y económicamente viable. Una obligación cuyo cumplimiento literal hace colapsar el servicio no cumple ese requisito. La CRC no realizó análisis de impacto sobre la viabilidad técnica de esta exigencia en plataformas de alto throughput, incumpliendo la metodología AIN.

La degradación del servicio SMS A2P generaría: (i) pérdida de ingresos para PRST y asignatarios de código corto durante los períodos de colapso; (ii) responsabilidades contractuales de los operadores frente a clientes corporativos cuyos SLA se incumplan; (iii) costos de rediseño arquitectural profundo de los SMSC, no incluidos en el AIN. (iv) Incumplimiento de SLA de OTP bancarios. (v) Afectación de mensajería crítica de IoT (rastreo vehicular, alarmas, sensores industriales). (vi) Costos de rediseño arquitectural no cuantificados. (vii). Responsabilidades contractuales de los operadores.

Más que descartar de plano la validación centralizada, solicitamos que la CRC defina su arquitectura técnica antes de imponer la obligación. La resolución debe precisar el flujo operativo de validación, las especificaciones de las APIs, los mecanismos de autenticación, los tiempos máximos de respuesta, los niveles de disponibilidad, los criterios de capacidad en transacciones por segundo (TPS), los esquemas de caché o validación local permitidos, las reglas aplicables al tráfico bidireccional y los protocolos de contingencia ante indisponibilidad o degradación del validador. Sin esas especificaciones, los PRST y demás agentes no pueden dimensionar adecuadamente las inversiones requeridas, evaluar impactos sobre SMSC y motores de enrutamiento, ni garantizar la continuidad de mensajes legítimos.

En consecuencia, la regulación debe evitar que la validación centralizada se traduzca en un cuello de botella operacional y debe permitir soluciones técnicas que preserven la continuidad del servicio, reduzcan latencias, eviten acumulación de colas, prevengan timeouts y aseguren que una falla del validador no bloquee injustificadamente tráfico legítimo, en especial el asociado a autenticación, seguridad, salud, servicios públicos, alertas transaccionales y comunicaciones críticas.

6. Sender id — restricción de asignación única y titularidad indirecta

El proyecto establece que a cada persona natural o jurídica le será asignado un único Sender ID (Art. 6.12.1.2, Parágrafo 2). Adicionalmente, la solicitud de asignación debe ser presentada por el asignatario del código corto A2P en nombre del solicitante (Art. 6.12.2.1), no directamente por el creador del contenido. Ambas restricciones generan problemas operativos graves.

Problemas técnicos del Sender ID único por empresa: (i) Grandes corporaciones (bancos, aseguradoras, retailers con múltiples marcas) necesitan Sender ID diferenciados por categoría de mensaje para que el usuario pueda priorizar e identificar visualmente el tipo de comunicación. Un banco con un único Sender ID 'BANCOX' mezclaría OTP de autenticación, avisos de transacciones, mensajes comerciales y alertas de seguridad en el mismo identificador, dificultando que el usuario distinga entre categorías críticas y no críticas. (ii) Grupos empresariales con múltiples personas jurídicas subsidiarias deben registrar Sender ID separados por NIT, multiplicando los trámites administrativos sin que la medida mejore la trazabilidad del fraude. (iii) El parágrafo del artículo 6.12.1.1 prohíbe identificadores que 'imiten nombres de entidades públicas, financieras u operadores de telecomunicaciones' pero no establece un mecanismo de verificación cruzada con el registro de marcas de la SIC ni con el RUES, dejando abierta la posibilidad de que actores maliciosos con empresa legalmente constituida soliciten Sender ID similares a marcas reconocidas (homóglifos, variaciones ortográficas).

Un único Sender ID por empresa genera: (i) costos de gestión documental elevados para corporaciones con múltiples marcas que deben crear personas jurídicas separadas para obtener Sender ID diferenciados; (ii) impacto negativo sobre la experiencia del usuario, que pierde la capacidad de identificar visualmente el tipo de mensaje; (iii) incentivo perverso a la fragmentación societaria para eludir la restricción.

En cuanto a la asignación, la resolución establece que el PCA debe solicitar a la CRC la asignación del SENDER ID a nombre del creador del contenido. Al respecto, es necesario que esta obligación en cabeza del PCA se modifique, y que la obligación de solicitar la asignación del SENDER ID recaiga directamente sobre el creador o responsable del contenido y no sobre el Proveedor de Contenidos y Aplicaciones (PCA). Lo anterior, en la medida en que el SENDER ID constituye un identificador asociado a la identidad, actividad y responsabilidad del remitente final de las comunicaciones, quien es el sujeto que conoce, controla y responde por el contenido de los mensajes enviados.

7. Plantillas a2p — rigidez operativa e impacto en servicios críticos

El régimen de plantillas establece que ningún mensaje A2P puede ser cursado si no está respaldado por una plantilla previamente aprobada y vigente. Las plantillas tienen vigencia mensual con renovación automática. El procedimiento de aprobación toma hasta 48 horas; sin embargo, el Proyecto no define la estructura, contenido mínimo, campos de información, reglas de intercambio ni especificaciones técnicas de la plantilla o formato mediante el cual se realizarían las consultas y respuestas entre los proveedores y dicho mecanismo.

Esta ausencia limita la capacidad de los PRST para evaluar de manera integral la viabilidad técnica, operativa y económica de la medida propuesta, así como para identificar los desarrollos tecnológicos, adecuaciones de sistemas, tiempos de implementación y eventuales impactos sobre sus procesos.

En consecuencia, es necesario que la CRC incorpore dentro de la propuesta regulatoria un modelo de plantilla o especificación funcional detallada y la someta a comentarios de la industria, con el fin de garantizar un análisis adecuado de su factibilidad y de los costos asociados a su implementación.

Sin conocer la información que deberá intercambiarse, los tiempos de respuesta exigidos y los mecanismos de integración, resulta imposible estimar con precisión los impactos regulatorios y la carga operativa que asumirían los PRST. Lo anterior, en atención a los principios de transparencia, participación y análisis de impacto normativo.

Adicionalmente, la obligación de que 'ningún mensaje A2P podrá ser cursado sin plantilla aprobada y vigente' (Art. 6.13.4.1) es una restricción absoluta sin excepciones para situaciones de emergencia o falla del validador. El Código de Procedimiento Administrativo establece que las restricciones absolutas sobre actividades lícitas requieren justificación de proporcionalidad. La norma tampoco establece qué ocurre si el validador demora más de 48 horas en resolver una solicitud de plantilla urgente: el agente queda bloqueado sin recurso inmediato.

Finalmente, se solicita que la regulación establezca que la validación y aprobación de plantillas por parte del validador centralizado se realice en un plazo máximo de veinticuatro (24) horas. Un término superior podría generar impactos significativos sobre la operación de los agentes que utilizan servicios de mensajería para el desarrollo de su actividad económica, especialmente en aquellos casos en los que la creación o modificación de plantillas responde a necesidades comerciales, operativas o de atención a los usuarios que requieren una implementación ágil.

En efecto, numerosos sectores económicos, entre ellos el financiero, asegurador, comercio electrónico, transporte, salud y telecomunicaciones, utilizan la mensajería para enviar comunicaciones asociadas a procesos transaccionales, campañas temporales, validaciones de identidad, recuperación de credenciales, notificaciones de seguridad y atención de contingencias operativas. En estos escenarios, imponer tiempos de aprobación superiores a veinticuatro (24) horas podría retrasar la puesta en marcha de nuevos servicios, afectar la continuidad de procesos críticos y generar perjuicios económicos tanto para los remitentes como para los usuarios finales. Por esta razón, cualquier esquema de validación debe procurar un equilibrio entre los controles destinados a prevenir el fraude y la necesidad de garantizar la agilidad que demandan las dinámicas propias del mercado y de los servicios digitales.

8. Comentarios sobre el plazo para la implementación de sistemas de monitoreo

El artículo **2.1.10.7.2.1.5.** señala que los PRST tienen TRES MESES a partir de la expedición de la resolución para implementar los sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P) orientados a identificar:

- La detección oportuna de patrones de uso atípico que sean indicativos de un posible uso fraudulento del servicio.
- Patrones asociados al uso masivo de planes con SMS ilimitados o con alto saldo para cursar el tráfico de naturaleza A2P simulado como P2P.
- el funcionamiento de granjas de SIM o a la comercialización del saldo de mensajes de texto entre usuarios.
- Volumen inusual de mensajes salientes por usuario.
- Alta dispersión de destinatarios.
- Homogeneidad del contenido.

Con independencia del plazo, las obligaciones de monitoreo de tráfico P2P y voz deben preservar la flexibilidad técnica de los PRST. La regulación puede definir criterios de referencia, pero no debería imponer una metodología cerrada ni exigir la concurrencia acumulativa de todos los patrones previstos al mismo tiempo para habilitar la actuación del operador. Cada PRST debe poder definir, según la arquitectura de su red, la información disponible y sus capacidades operativas, los criterios más adecuados para identificar riesgos, bastando contar con herramientas tecnológicas razonables y verificables basadas en al menos uno o varios criterios de análisis. Este enfoque conserva el objetivo de prevención del fraude, reduce el riesgo de falsos positivos, evita costos desproporcionados y permite que los operadores innoven en sus metodologías de detección.

El plazo de tres (3) meses previsto en el artículo mencionado, para la implementación de sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P), resulta insuficiente para garantizar una implementación adecuada, segura y efectiva de las capacidades exigidas por la regulación.

Las funcionalidades requeridas por la propuesta regulatoria exceden la simple incorporación de herramientas de monitoreo, pues implican el diseño, desarrollo, adquisición o adaptación de sistemas especializados capaces de identificar patrones complejos de comportamiento asociados a fraude, tales como detección de tráfico A2P simulado como P2P, identificación de granjas de SIM, análisis de volúmenes inusuales de tráfico, dispersión de destinatarios y homogeneidad de contenido. Estas actividades requieren procesos de análisis, parametrización, integración con plataformas existentes, definición de reglas de negocio, pruebas técnicas y ajustes operativos que difícilmente pueden completarse dentro del plazo propuesto.

Adicionalmente, la implementación de estos mecanismos demanda inversiones en infraestructura tecnológica, desarrollo de capacidades analíticas, procesamiento de grandes volúmenes de información y, en algunos casos, la contratación o adquisición de soluciones de terceros. Lo anterior debe estar acompañado de procesos internos de evaluación, contratación, desarrollo, pruebas de aceptación y puesta en producción, los cuales suelen requerir varios meses para su ejecución adecuada.

Debe considerarse además que la efectividad de los sistemas de detección depende de la construcción y calibración de modelos de comportamiento y umbrales de alerta, actividad que exige recopilar información histórica, analizar patrones de tráfico y validar la precisión de las alertas generadas con el fin de minimizar falsos positivos que puedan afectar usuarios legítimos o generar bloqueos injustificados.

Por otra parte, el proyecto regulatorio no incorpora evidencia que demuestre que un plazo de tres meses sea técnica y operativamente suficiente para implementar las capacidades exigidas por todos los PRST, ni presenta un análisis de impacto que considere las diferencias existentes entre operadores en cuanto a infraestructura, arquitectura tecnológica y niveles de madurez de sus sistemas antifraude.

En consecuencia, se solicita ampliar el plazo de implementación a un mínimo de seis (6) meses contados a partir de la entrada en vigencia de la resolución. Este término permitiría a los PRST desarrollar e implementar soluciones robustas, realizar las pruebas necesarias, capacitar al personal involucrado y garantizar que los mecanismos de monitoreo entren en operación con niveles adecuados de precisión, estabilidad y efectividad, contribuyendo así al cumplimiento de los objetivos perseguidos por la regulación sin comprometer la continuidad y calidad de los servicios. En consecuencia, el reporte del cumplimiento de dicha obligación debería realizarse a los doce (12) meses desde la expedición de la norma.

9. **Lista DNO y prohibición CLI spoofing — ausencia de excepciones técnicas necesarias**

El artículo 2.1.10.7.2.2.1 prohíbe absolutamente las llamadas internacionales entrantes que presenten CLI colombiano, salvo roaming identificado. El artículo 2.1.10.7.2.2.3 obliga a bloquear todas las llamadas que presenten numeración incluida en la Lista DNO. Ambas prohibiciones carecen de excepciones para casos de uso legítimos.

Una prohibición absoluta sin excepciones puede afectar actividades lícitas garantizadas por la libertad de empresa (Art. 333 CP). Las restricciones deben ser proporcionales y prever mecanismos de excepción para casos justificados. La ausencia de un marco de attestation previo a la prohibición (equivalente a STIR/SHAKEN) significa que se prohíbe una conducta sin primero crear las herramientas técnicas para distinguir entre CLI legítimo y CLI suplantado en el tráfico internacional.

Se recomienda establecer un procedimiento de inscripción voluntaria para clientes corporativos que usen numeración colombiana desde el exterior con fines legítimos (análogo al etiquetado de llamadas publicitarias), un proceso expedito de revisión para titulares de numeración bloqueados erróneamente por la Lista DNO, con resolución en máximo 48 horas y un plazo de 18 meses para desarrollar un marco de attestation de llamadas (STIR/SHAKEN adaptado al contexto colombiano) que permita a futuro distinguir técnicamente entre CLI legítimo y suplantado, antes de implementar la prohibición absoluta.

10. Etiquetado de llamadas — inviabilidad técnica en redes 2G/3G

El artículo 3 de la norma obliga a los PRST a etiquetar llamadas sospechosas con la indicación 'Alerta de llamada sospechosa' visible en el dispositivo del usuario receptor. Esta función no es implementable en todos los segmentos de la red colombiana.

El etiquetado de llamadas visible en el terminal del usuario requiere: (i) soporte de la red en el nivel de señalización (4G/VoLTE o 5G); (ii) soporte del sistema operativo del terminal (Android/iOS con versión reciente); (iii) APIs del fabricante del terminal que permitan mostrar metadatos de la llamada en la pantalla de identificación. Las redes 2G y 3G no soportan esta funcionalidad de señalización.

En Colombia, una proporción significativa de usuarios aún opera en redes 2G/3G (especialmente en zonas rurales y población de menores ingresos). Para esos usuarios, el etiquetado es técnicamente imposible independientemente de lo que haga el operador. La responsabilidad de mostrar la etiqueta recae sobre el sistema operativo del terminal y el fabricante, no sobre el PRST, quien solo puede enviar la señalización. Si el teléfono no la interpreta, la etiqueta no se muestra.

Imponer una obligación cuyo cumplimiento depende de terceros no regulados genera inseguridad jurídica para los PRST, quienes quedarían expuestos a sanciones por incumplimiento de una obligación que no está bajo su control completo.

A esto se suma que el costo de implementar sistemas de señalización de etiquetado de llamadas en infraestructura 4G/VoLTE es significativo y no fue cuantificado en el AIN. Para las redes 2G/3G, el costo es prácticamente ilimitado (requeriría migración completa a 4G, que es un proceso de varios años).

11. Proporcionalidad de las medidas de voz, capa de aplicación y asignación de cargas al originador

Las medidas asociadas al tráfico de voz deben replantearse bajo criterios estrictos de proporcionalidad y costo-eficiencia. El servicio de voz móvil se encuentra en una fase de declive estructural por la sustitución hacia servicios de datos y aplicaciones OTT, por lo que imponer inversiones significativas en plataformas, señalización, monitoreo y etiquetado sobre un canal decreciente puede generar ineficiencias económicas y destrucción de valor sectorial. Cualquier obligación en materia de voz debería limitarse a variables de señalización técnica y transporte que estén bajo control razonable del operador.

La presentación visual de etiquetas como “Alerta de llamada sospechosa” o “Llamada con fines publicitarios” en el terminal del usuario depende de la capa de aplicación, del sistema operativo, del fabricante del dispositivo y de aplicaciones de terceros, no del core de red del PRST. Por tanto, la regulación no debería imponer al PRST una obligación de resultado sobre elementos que no controla, ni hacerlo responsable de la visualización efectiva de la

etiqueta. En materia de llamadas internacionales con CLI colombiano, la carga regulatoria debe asignarse principalmente a los originadores del tráfico y a los carriers internacionales que transportan o entregan llamadas con información irregular de origen, sin recargar al PRST terminante con obligaciones que no puede controlar integralmente.

En la misma línea, la obligación de consultar el Registro de Números Excluidos (RNE) y abstenerse de contactar a usuarios inscritos debe recaer sobre el originador de la comunicación publicitaria o comercial, en tanto es quien conoce la finalidad de la campaña, la base de datos utilizada, las autorizaciones otorgadas por el usuario y la eventual aplicación de excepciones legales. Trasladar al PRST la obligación de verificar y bloquear llamada a llamada frente al RNE implica imponerle una función de calificación jurídica y vigilancia material que excede su rol de proveedor de infraestructura y transporte, pues no cuenta con información suficiente para determinar si una llamada es publicitaria, transaccional, de servicio, solicitada por el usuario o amparada por una excepción legal. En consecuencia, la regulación debería promover reglas claras aplicables a los originadores, bajo la vigilancia de las autoridades competentes, en lugar de una obligación de validación y bloqueo en tiempo real a cargo del PRST.

12. Respecto del periodo de transición y plazo de implementación

El artículo 2.1.10.7.2.1.5 otorga tres meses para implementar sistemas de monitoreo y control de tráfico P2P. El período de transición del artículo 19 es de seis meses contados desde la publicación de la resolución de remuneración A2P (Fase II), cuya fecha es incierta.

La implementación de sistemas de monitoreo P2P capaces de detectar los seis patrones descritos en el artículo 2.1.10.7.2.1.1 (volumen inusual, alta dispersión de destinatarios, homogeneidad de contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado, concentración geográfica) requiere: (i) diseño de la arquitectura del sistema; (ii) selección o desarrollo de modelos de machine learning; (iii) integración con los sistemas de gestión de red del PRST; (iv) calibración de umbrales con datos históricos de tráfico; (v) pruebas en entorno no productivo; (vi) ajustes y corrección de falsos positivos; (vii) capacitación del personal. Ese proceso toma entre 6 y 12 meses en operadores con infraestructura tecnológica madura, y potencialmente más en operadores con arquitecturas más antiguas. El plazo de 3 meses es técnicamente inviable para implementar un sistema robusto; puede ser suficiente para implementar uno rudimentario que genere altas tasas de falsos positivos, afectando usuarios legítimos.

La norma no presentó un análisis técnico de viabilidad del plazo de 3 meses. La imposición de plazos técnicamente insuficientes genera el riesgo de que los operadores implementen soluciones superficiales de cumplimiento formal sin efectividad real en la prevención del fraude.

Ampliar el plazo de implementación de sistemas de monitoreo P2P a 6 meses desde la publicación en Diario Oficial, con el primer informe de acreditación a los 7 meses y el informe

de resultados a los 13 meses. Para el período de transición del sistema A2P (Art. 19), establecer un cronograma mínimo garantizado de 6 meses contados desde la publicación de la presente resolución para que los agentes puedan iniciar los procesos internos de preparación, independientemente de la fecha de la Fase II.

13. Efecto de sustitución hacia canales OTT — vacío analítico fundamental

El proyecto regulatorio no analiza el efecto de sustitución del fraude hacia canales no cubiertos por la regulación (WhatsApp, Telegram, Instagram, correo electrónico, llamadas VoIP). Sin este análisis no es válida la conclusión de que las medidas propuestas generarán una reducción del fraude.

El fraude cibernético es un fenómeno dinámico que migra hacia los canales con menor costo de operación y menor nivel de control regulatorio. Si la regulación propuesta eleva significativamente los costos y riesgos del fraude vía SMS/voz, los defraudadores migrarán hacia WhatsApp Business API, canales de mensajería OTT, correo electrónico y llamadas VoIP sobre internet. Estos canales tienen alcance equivalente o mayor al SMS para la mayoría de la población colombiana con smartphone. No existe evidencia empírica en la regulación de que el fraude en canales OTT sea menor que el del SMS; de hecho, la evidencia anecdótica sugiere que el phishing vía WhatsApp ha crecido significativamente en los últimos dos años.

14. Liberalización del mercado A2P

El proyecto regulatorio fue planteado inicialmente sin incluir un análisis económico sobre la tarifa de terminación de mensajes SMS, a pesar de que este es un elemento clave para el adecuado funcionamiento del mercado. Paralelamente, la CRC desarrollaba otro proceso en el que definió un valor de referencia de $0,03 para la terminación de SMS.

Sin embargo, en esta etapa la CRC nuevamente omite analizar la tarifa de terminación de SMS A2P y los aspectos económicos del servicio, mientras propone medidas mucho más exigentes en lo técnico, operativo y económico. Estas incluyen nuevas obligaciones como validación de remitentes, autenticación, trazabilidad, mayores controles al tráfico, intercambios de información mediante plataformas tecnológicas, entre otras, que implican inversiones importantes, ajustes operativos y mayores cargas administrativas para los agentes.

Este enfoque desconoce que las obligaciones regulatorias deben ir acompañadas de mecanismos que permitan recuperar los costos asociados, garantizando su sostenibilidad. La falta de un análisis económico integral puede desincentivar la inversión, generar barreras a la participación de algunos actores, afectar la competencia en mercados relacionados y trasladar costos a los usuarios o clientes empresariales.

Además, al posponer nuevamente el análisis económico para una etapa posterior, se fragmenta la regulación, se generan riesgos de inconsistencias y se limita una evaluación completa de los impactos de las medidas. En estas condiciones, no es posible determinar si las obligaciones propuestas son proporcionales, eficientes y sostenibles.

Finalmente, resulta contradictorio que la propia CRC reconozca que aún necesita profundizar en el análisis del servicio de mensajería SMS A2P —incluyendo sus condiciones operativas, económicas y comerciales— y que haya solicitado información adicional a los agentes. Si no se cuenta con un entendimiento completo del mercado, resulta prematuro avanzar en la adopción de obligaciones que lo impactan directamente.

En conjunto, el proyecto presenta un desequilibrio entre la imposición de nuevas obligaciones y la ausencia de un análisis económico que garantice su viabilidad. Avanzar en exigencias técnicas y operativas sin definir las condiciones económicas del servicio genera incertidumbre y riesgos para la sostenibilidad del mercado.

Por ello, resulta necesario que la CRC aborde de manera integral y previa los aspectos económicos de la mensajería SMS A2P, de modo que las medidas regulatorias sean proporcionales, consistentes y basadas en un entendimiento completo del mercado, permitiendo así promover la inversión, la competencia y la prestación eficiente del servicio.

PROPUESTAS ALTERNATIVAS

Como complemento a los comentarios específicos por artículo, proponemos las siguientes medidas alternativas de carácter sistémico que, podrían evaluarse para el diseño del sistema:

Fortalecer las herramientas regulatorias existentes

La CRC ya dispone de mecanismos potencialmente efectivos que no han sido evaluados ex post: suspensión provisional de códigos cortos en actuaciones administrativas, recuperación expedita de recursos de identificación, monitoreo de tráfico por los propios PRST, coordinación con COLCERT y Fiscalía.

Modelo distribuido de KYC con auditoría centralizada

En lugar de un validador centralizado con posición monopólica, establecer un modelo en el que cada asignatario de código corto realice KYC bajo estándares regulatorios mínimos definidos por la CRC, con auditorías periódicas de la Comisión. Este modelo mantiene la responsabilidad en los agentes privados que tienen la relación contractual con los PCA, elimina el SPOF, reduce costos y no requiere crear un nuevo actor regulatorio.

Registro público de Sender IDs con validación cruzada

La CRC puede administrar directamente el registro de Sender IDs en el SIGRI, con validación cruzada automática contra el registro de marcas de la SIC y el RUES. Este modelo es técnicamente más sencillo que el validador centralizado, menos costoso y elimina el riesgo de monopolio privado.

Hoja de ruta para implementación de STIR/SHAKEN adaptado

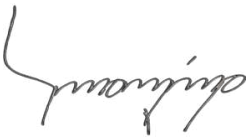
En lugar de prohibir el CLI spoofing de forma absoluta sin herramientas técnicas de distinción, la CRC debe liderar el desarrollo de un marco de attestation de llamadas (equivalente al STIR/SHAKEN norteamericano adaptado al contexto colombiano) en un plazo de 18-24 meses, con los PRST y la industria de carriers internacionales. Este marco permitiría a futuro distinguir técnicamente entre llamadas con CLI legítimo y llamadas con CLI suplantado, haciendo la prohibición más efectiva y menos propensa a falsos positivos.

Coordinación regulatoria interinstitucional para cubrir canales OTT

La CRC debe iniciar coordinación formal con el MinTIC, la Superintendencia Financiera, la SIC y el COLCERT para desarrollar un marco regulatorio que extienda las obligaciones de prevención del fraude a los canales OTT más utilizados para el fraude (WhatsApp, Telegram, plataformas de correo electrónico). Sin esa extensión, las medidas del presente proyecto pueden generar desplazamiento sin reducción del fraude.

Agradecemos tener en cuenta estas observaciones y quedamos atentos a resolver cualquier inquietud al respecto.

Cordialmente,



GABRIEL ADOLFO JURADO PARRA
Director Cámara TIC y TV