Bogotá D.C., diciembre 29 de 2025.

Ingeniera
Claudia Ximena Bustamante
Directora Ejecutiva
Comisión de Regulación de Comunicaciones – CRC
La ciudad

Asunto: Comentarios al documento *"Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles – Documento de Alternativas Regulatorias"*

Ingeniera Bustamante,

Desde la Asociación de la Industria Móvil de Colombia - Asomóvil, agradecemos la oportunidad de comentar el Documento de Alternativas Regulatorias - para la mitigación del fraude cibernético por medio de servicios móviles.

I. Consideraciones no incorporadas en las alternativas regulatorias del documento sobre mitigación del fraude cibernético mediante servicios móviles.

El pasado 4 de agosto con radicado **2025817801,** en el marco de los comentarios a la identificación "*de medidas para mitigar el fraude cibernético por medio de servicios móviles"*, presentando a la entidad una serie de consideraciones que son vitales para la mitigar el fraude cibernético pero que fueron omitidos por la CRC en el documento soporte, que sirve de fundamento para esta nueva etapa del proceso regulatorio.

Dentro de las sugerencias propuestas en esa comunicación, se planteó la necesidad de habilitar a los PRSTM la terminación de contratos con los PCA/IT reincidentes, la invitación construida desde Asomóvil en la que se solicitaba suspender o terminar los contratos comerciales con aquellos PCA o integradores tecnológicos (IT) que reincidan en fraudes a través de la red móvil, tiene por objeto pasar de un mecanismo meramente correctivo a uno que genere un desincentivo real a los agentes que permiten estos comportamientos, esto es, que el fraude comprobado tenga una consecuencia efectiva y no se agote en la simple recuperación del código corto, sin un impacto material en el eslabón de la cadena en la que se concreta la conducta, y se basaba en el principio fundamental de la Buena Fe, en su acápite contractual, en tanto ciertos PCAs e IT abusando de la regulación se han constituido en verdaderas redes criminales para la comisión de fraudes a través de los sistemas de envíos de SMSs.

Si bien en el documento de alternativas la CRC reconoce la reincidencia y la posibilidad de terminar relaciones comerciales con actores infractores[1], observamos que la medida contenida en la alternativa 2, temática 7.4.3 (TEMÁTICA 3: Suspensión del tráfico cursado a través de un código corto en el marco de una actuación administrativa) debe complementar las disposiciones ya existentes en la Resolución CRC 7811 de 2025, al tiempo que se garantice la celeridad en el bloqueo del tráfico fraudulento y evitar afectaciones masivas a los usuarios. Para alcanzar dicho propósito, se requiere una medida realmente disuasiva que permita **i)** la terminación del acceso de un PCA/IT reincidente, **ii)** sancione la reincidencia y **iii)** faculte a las autoridades para adoptar medidas que cierren el ciclo de fraude por esta vía.

De otra parte, resulta necesario fortalecer el componente sancionatorio aplicable a los reincidentes. En la actualidad, la CRC sanciona estos comportamientos principalmente con la recuperación del recurso de numeración (número o código), pero en la práctica dicha medida no ha generado el efecto disuasivo esperado: actores a quienes se les retiran los números o los códigos de manera reiterada, pueden asumir la pérdida de un código corto como un costo menor frente al beneficio obtenido del ilícito y continuar la conducta mediante la rotación de numeración o el cambio a otro operador. Por ello, respetuosamente insistimos a la CRC en la necesidad de incorporar explícitamente en las alternativas el diseño de un régimen contra reincidentes que contemple medidas escalonadas y efectivas, tales como multas proporcionales al daño causado, la prohibición temporal o definitiva de recibir nuevas asignaciones de numeración e, incluso, la pérdida del registro como proveedor de contenidos ante la persistencia en conductas fraudulentas.

En casos de reincidencia la CRC podría establecer un periodo de Mora para la entrega de nuevos códigos cortos al PCA y/o IT que ha defraudado la confianza regulatoria, y que con sus acciones ha permitido o accionado actividades ilegales.

[1] Adicional a lo anterior, es importante aclarar que, la regulación vigente ya establece obligaciones claras para PCA y PRST en materia de seguridad, prevención de fraude y monitoreo de tráfico, de modo que no es cierto que se carezca de lineamientos por efecto del desconocimiento del ecosistema de mensajería. El hecho de que existan múltiples intermediarios o rutas internacionales no exime a los asignatarios de su deber de implementar controles eficaces que aseguren el uso legítimo de los códigos cortos. De hecho, en otros mercados internacionales con condiciones similares de complejidad, los operadores y asignatarios han demostrado que sí es posible aplicar mecanismos de trazabilidad, filtrado y monitoreo con resultados tangibles en la reducción del fraude. https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-alternativas-regulatorias-identificacion-medida-fraude-cibernetico-servicios-moviles.pdf p. 32.

En la misma línea, y en relación con los controles para la asignación de numeración (códigos cortos y numeración A2P), la restricción vigente resulta insuficiente, dado que los actores reincidentes pueden "volver a operar" una vez termine el plazo del cumplimiento de la sanción o acceder a nueva numeración mediante filiales o intermediarios. De ahí la necesidad de que se adopte un enfoque más robusto, basado en una evaluación de riesgo del solicitante (antecedentes de cumplimiento y vínculos relevantes), que cierre la puerta al fraude desde el origen y complemente la suspensión de tráfico con consecuencias realmente efectivas frente a la reincidencia, enviando un mensaje inequívoco: el fraude reiterado conlleva la salida del ecosistema.

De otra parte, observamos que las diferentes alternativas del proyecto regulatorio contempla la implementación de una serie de desarrollos tecnológicos que deberán adoptar los PRSTM, sin embargo, en el documento no se advierte un análisis de impacto (AIN) que justifiquen estas medidas: Algunas de las alternativas contenidas en el documento imponen obligaciones técnicas y operativas a los PRSTM (monitoreo y filtrado), pese a que estos no controlan el origen último de muchas prácticas fraudulentas. Medidas como la implementación obligatoria de nuevos sistemas *(p. ej., autenticación de llamadas STIR/SHAKEN propuesta como Alternativa 4 en la temática "Mecanismos de verificación, autenticación e identificación del originador de la llamada de voz", o limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) -(Spoofing)-)* implican no solo una carga regulatoria adicional para los PRSTM, sino un impacto económico en la operación de estos. Si bien la industria está comprometida trabajar de manera conjunta en la lucha contra el ciberdelito, es imperativo que cada nueva exigencia esté soportada en un Análisis de Impacto Normativo (AIN). En el documento no se advierte la evaluación de las medidas propuestas; por ejemplo, no se cuantifican los costos de desplegar STIR/SHAKEN a nivel nacional ni se contrastan con los beneficios esperados en reducción de fraude. Esta ausencia de AIN contrasta con los lineamientos de mejora regulatoria que exigen identificar la viabilidad técnica, legal y económica antes de imponer nuevas obligaciones.

Adicionalmente, es importante advertir que los servicios sobre los que se pretende imponer estas obligaciones técnicas —principalmente voz móvil y mensajes SMS— **corresponden a productos de telecomunicaciones en declive**, cuya demanda y relevancia relativa disminuye año a año debido a la migración de los usuarios hacia servicios avanzados basados en datos, aplicaciones OTT y comunicaciones IP. En este contexto, exigir inversiones de alto costo en plataformas y sistemas aplicables a tecnologías en proceso de obsolescencia podría generar una asignación ineficiente de recursos, obligando a los operadores a desplazar inversiones desde tecnologías en

crecimiento, necesarias para la expansión de redes, innovación y modernización, hacia tecnologías que ya no constituyen el núcleo del ecosistema digital actual.

De otra parte, preocupa que estas cargas se impongan principalmente a los PRSTM, cuando el origen de buena parte de las prácticas fraudulentas se encuentra en los PCA y en otros generadores de contenido que no están bajo el control directo del proveedor de red. En ese escenario, existe el riesgo de que la regulación termine trasladando costos altos a quienes tienen capacidades limitadas para intervenir en el origen del problema, sin atacar de manera equivalente al eslabón en el que se origina el problema. Adicionalmente, como lo señaló la Universidad Externado de Colombia, medidas excesivamente gravosas o focalizadas solo en la red pueden incentivar que los actores y modelos de negocio vinculados al fraude se desplacen hacia canales no regulados o menos supervisados, con lo cual se reduciría la eficacia de las obligaciones técnicas propuestas y se debilitaría la relación costo–beneficio que precisamente debe sustentar el AIN.

Revisión de las temáticas y las alternativas regulatorias.

El documento de la CRC agrupa las alternativas regulatorias en cuatro grandes temáticas: (1) mitigación del fraude vía SMS (mensajes de texto), (2) mitigación del fraude vía llamadas de voz, (3) educación al usuario, y (4) mejoras al régimen de administración de numeración (simplificación y control)

En ese sentido, una primera consideración es que el diseño regulatorio debe estructurarse desde la proporcionalidad y sostenibilidad del ecosistema, evitando trasladar a los PRSTM cargas tecnológicas y operativas que no guarden relación con la estructura de ingresos del servicio ni con el control efectivo que tienen sobre el origen del fraude. La mayoría de las alternativas descritas en el documento, suponen inversiones y ajustes técnicos importantes (plataformas, monitoreo en tiempo real, mecanismos de autenticación/verificación, integraciones y reportes), que generarían ineficiencias y distorsiones si se imponen de manera homogénea sin diferenciar el rol de cada actor en la cadena (PRSTM, PCA/IT).

Asimismo, resulta indispensable que cualquier obligación regulatoria se asigne a los actores de la cadena de valor que realmente tienen control sobre el contenido y la generación de las comunicaciones, y no a los PRSTM, cuya función en muchos casos se limita al transporte y enrutamiento del tráfico. Los operadores no originan los mensajes ni determinan su contenido, por lo que imponerles cargas de monitoreo, filtrado o verificación implica trasladarles responsabilidades que exceden su ámbito de control y

que, en la práctica, deberían recaer sobre quienes gestionan, producen o habilitan los servicios donde se origina el fraude.

En materia de mitigación del fraude vía SMS, consideramos que el hecho de fortalecer la identificación y trazabilidad del tráfico A2P desde el origen, evitando que el ecosistema continúe operando sobre esquemas de remitencia compartida que favorecen el smishing.

Para la mitigación del fraude vía llamadas de voz, a partir de las alternativas propuestas advertimos que las medidas evaluadas pueden tener impactos económicos relevantes para los PRSTM, en tanto exigen capacidades técnicas adicionales de monitoreo, filtrado, analítica, etiquetado o bloqueo, y coordinación operativa permanente. Además, resulta determinante reconocer que una porción importante del riesgo proviene de los carries internacionales con caller ID spoofing o tráfico que aparenta origen local. Por ello, más allá de las medidas internas de red propuestas en las propuestas regulatorias, es fundamental que la CRC incorpore un componente de corresponsabilidad en la cadena internacional, promoviendo acuerdos y exigencias a carriers internacionales y de tránsito para que el tráfico hacia Colombia ingrese con numeración auténtica y sin manipulación, y bajo estándares verificables de procedencia. Sin estas regulaciones con agentes internacionales, parte de la carga operativa puede recaer desproporcionadamente en los PRSTM, aun cuando el origen del problema se encuentre fuera de su control directo.

En cuanto a la educación al usuario, compartimos la relevancia de fortalecer capacidades de prevención, alfabetización digital y mecanismos de reporte. Programas educativos o campañas informativas, sin embargo, el diseño de esta política debe involucrar a todos los actores a través de una coordinación interinstitucional (*público-privados* - esfuerzos conjuntos con autoridades, entidades financieras y canales de denuncia) que maximice el impacto, y debe estar acompañada de consecuencias efectivas para los actores que habilitan el fraude.

En ese sentido, antes de avanzar en la adopción de la totalidad de las alternativas regulatorias, es importante que la CRC desarrolle un AIN respecto de las alternativas presentadas, en las que se garantice su viabilidad técnica, su proporcionalidad económica y su sostenibilidad para el ecosistema y para los usuarios.

Finalmente, es fundamental que los próximos proyectos de esta naturaleza incluyan a las **OTTs**, dado el hecho que hoy gran parte de las prácticas fraudulentas se originan y distribuyen a través de **plataformas de mensajería y comunicaciones IP**, no mediante

los servicios tradicionales de voz y SMS. Cualquier marco regulatorio que pretenda ser efectivo debe incorporar a estos actores, que son quienes concentran el tráfico y los mecanismos de comunicación usados actualmente por los defraudadores.

Cordialmente,

Samuel Hoyos Mejía.
Presidente de ASOMÓVIL.

Calle 81 N° 11 – 55 Piso 9, Bogotá D.C – Colombia
Teléfono +57 (1) 6500075 presidencia@asomovil.org