Bogotá D.C., agosto 4 de 2025.

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

Asunto: Comentarios al documento de formulación del problema *"Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles"*.

Ingeniera Bustamante,

Desde la Asociación de la Industria Móvil de Colombia – Asomóvil, y en atención al proceso de consulta pública del proyecto del asunto, presentamos a continuación una perspectiva complementaria a la expuesta en el documento de formulación del problema. En particular, deseamos hacer énfasis en los siguientes puntos que tuvimos la oportunidad de exponer el pasado julio 23 de 2025 en la Universidad Externado de Colombia.

1. **Omisión del internet móvil en el análisis y necesidad de incluirlo:** Notamos que el árbol de problema y el análisis regulatorio presentado por la CRC se centran en los servicios tradicionales de voz y mensajería SMS, al ser éstos los medios directamente vinculados al uso de recursos de identificación administrados por la Comisión. Sin embargo, consideramos que existe una omisión importante: el servicio de acceso a Internet móvil no ha sido incorporado explícitamente en la caracterización del problema, pese a ser parte esencial del ecosistema de comunicaciones y estar íntimamente ligado a la ejecución de muchos fraudes. Es cierto que las estafas objeto del proyecto suelen iniciarse mediante una llamada o SMS, pero a menudo se concretan o amplifican a través del internet móvil. Por ejemplo, un mensaje de smishing típicamente contiene un enlace malicioso; el usuario, al hacer clic, es dirigido mediante su conexión de datos móviles a un sitio web fraudulento donde puede entregar sus credenciales o información sensible. De igual forma, muchas modalidades de engaño utilizan aplicaciones de mensajería OTT (WhatsApp, Telegram) o correos electrónicos, los cuales operan sobre la red de internet móvil. Ignorar esta realidad implicaría asumir que el fraude termina en el SMS o la llamada, cuando en realidad la red de datos es el siguiente eslabón explotado por los atacantes para culminar la estafa.

Por lo tanto, sugerimos que el análisis regulatorio considere al internet móvil dentro del entorno del problema, al menos de forma transversal.

2. **Incremento de fraude por smishing y spoofing:** Coincidimos con la CRC en que las modalidades de fraude como el *smishing* (mediante SMS) y el *vishing* o suplantación vía llamadas de voz (*caller ID spoofing*) se han incrementado de forma alarmante en los últimos años. Estos fraudes, afectan gravemente a los usuarios al engañarlos para obtener sus datos o dinero, pero también tienen consecuencias directas sobre los operadores móviles, en la medida que, de una parte estas prácticas generan un daño reputacional: los clientes comienzan a desconfiar de los mensajes y llamadas legítimas, debilitando la percepción de seguridad de nuestros servicios y por otro lado, generan impactos operativos en la medida que los PRSTM se incrementa el volumen de PQR relacionadas con fraudes. En paralelo, aunque el tráfico de voz y SMS tradicionales ha tendido a disminuir (mientras aumenta el uso de datos y aplicaciones de mensajería instantánea), los incidentes de fraude asociados a estos canales han crecido de forma sostenida, evidenciando que la reducción en el uso no conlleva una disminución del riesgo. Esto indica que, los delincuentes concentran sus esfuerzos en explotar vulnerabilidades de estos canales.

   Desde las revisiones que se han adelantado desde la industria, se ha detectado un auge en la práctica de suplantar números telefónicos en llamadas: se enmascaran llamadas internacionales con numeración nacional para inducir a error al usuario, logrando que atienda comunicaciones fraudulentas. A través de esta técnica de *spoofing* se realizan robo de datos personales, fraudes financieros y otros delitos, terminando de minar la confianza del público en los canales de comunicación.

3. **Reincidencia de ciertos PCA e integradores tecnológicos en usos fraudulentos de numeración:**

   En los análisis realizados por los operadores, se ha identificado la reincidencia de algunos Proveedores de Contenido y Aplicaciones (PCA) e Integradores Tecnológicos (IT) en el uso indebido de recursos de numeración, tanto códigos cortos como numeración nacional. En múltiples ocasiones, se han detectado los mismos actores vinculados a campañas fraudulentas reiteradas a pesar de los esfuerzos realizados por los operadores ante las autoridades administrativas y de justicia para contrarrestar estas conductas. Se documentó que ciertos códigos cortos (como 890087, 85999, *85617*, *890133, 890176, 899773* y *893184*) asignados a distintos PCA fueron utilizados para fraudes (ofertas falsas de descuentos en

facturas de operadores, suplantación de entidades como Netflix, DIAN, entre otros), repitiéndose estas situaciones con un mismo integrador, HABLAME, que actuaba en la cadena como IT de varios PCA involucrados. Esto pone en evidencia, la existencia de fallas en los filtros y controles de dichos intermediarios.

La reincidencia de estos agentes en actividades fraudulentas sugiere que las sanciones actuales no están generando el efecto disuasivo esperado. Si un asignatario de numeración –sea PCA o integrador– *recupera rápidamente su acceso a nuevos recursos o a las redes pese a haber incurrido en fraude*, el círculo de abuso continúa. Desde la perspectiva de los PRSTM, esta situación es sumamente grave porque erosiona la integridad del sistema de numeración y pone en entredicho la eficacia de la regulación vigente. Un actor recurrente en malas prácticas representa un riesgo elevado de nuevos engaños masivos a los usuarios, comprometiendo también la relación de confianza entre operadores y abonados (por ejemplo, cuando mensajes con códigos oficiales del operador son explotados para estafar).

Por ello, consideramos esencial reconocer en el diagnóstico del problema la existencia de actores reincidentes específicos, e implementar mecanismos que *eviten que un mismo sujeto pueda seguir reutilizando numeración o infraestructura de otro operador tras sanciones leves*. La trazabilidad total de quién está detrás de cada campaña y la publicidad de los infractores reiterativos son elementos clave para romper ese ciclo de fraude.

4. Insuficiencia de las medidas regulatorias actuales de la CRC:

Si bien la CRC ha ejercido sus funciones en materia de administración de recursos de identificación *–principalmente a través de la recuperación de códigos cortos utilizados indebidamente–*, los PRSTM percibimos que estas medidas resultan insuficientes para frenar el fraude cibernético móvil en su conjunto. Actualmente, ante un caso comprobado de uso fraudulento de numeración, la acción típica es que la CRC inicia un proceso administrativo y finalmente revoca o recupera el número o código corto involucrado para retirarlo del tráfico. Esta medida, si bien necesaria, se queda corta en efectividad por varias razones:

- La empresa infractora (PCA o integrador) pierde el código corto específico, pero *su vínculo contractual con el operador de red puede permanecer intacto*. De hecho, la CRC ha manifestado que no tiene competencia para pronunciarse sobre el incumplimiento del contrato comercial o regulado entre el PRSTM y el asignatario. Esto implica que, tras la recuperación del recurso, no hay una

consecuencia directa sobre la continuidad de la conexión o del acuerdo comercial o contrato de acceso, uso e interconexión del actor sancionado, quien podría intentar obtener nuevos recursos numéricos, utilizar otros códigos que tenga asignados para reiterar la práctica fraudulenta o continuar operando a través de otros medios.

- **Vacío en la sanción a reincidentes:** Como se mencionó, existen casos donde la misma entidad incurre en fraudes reiterados con distintos recursos. La acción de recuperar la numeración cada vez no conlleva una penalidad acumulativa (agravación por reiteración de la conducta) ni una inhabilitación explícita para el agresor. En la práctica, el impacto para el infractor es menor *(pierde un código, pero podría solicitar otro)*, mientras que el impacto para los usuarios y operadores ya se materializó en forma de fraude consumado y pérdida de confianza.

- **Respuesta limitada de otras autoridades:** Como se manifestó en el evento realizado en la Universidad Externado de Colombia, es preocupante que frente a estos hechos, ninguna autoridad adicional a la CRC está llenando este vacío. El Ministerio TIC, por ejemplo, ante consultas de los operadores, ha indicado que su rol se limita a reconocer las acciones tomadas por la CRC sobre la numeración fraudulenta, inhibiéndose de actuar adicionalmente por tratarse de competencias de la CRC en administración de numeración. De igual modo, entidades como la Superintendencia de Industria y Comercio (SIC) o la Fiscalía, aunque competentes en protección de datos o delitos informáticos, no reaccionan con la celeridad que estos eventos requieren para prevenir daños mayores. En resumen, el marco actual deja un área gris donde el fraude operativo no recibe una sanción integral: se corta el *medio* (el número), pero no se imposibilita al *actor* malicioso ni se mitiga rápidamente el efecto sobre las víctimas.

  Por otra parte, la regulación actual no contempla ninguna medida para abordar la modalidad de fraude Spoofing. Consideramos que la principal responsabilidad recae en los Carrier internacionales, los cuales deben velar por la seguridad de los usuarios y minimizar el impacto de estos riesgos. Este tipo de proveedor no cuenta con una regulación más allá de fijar condiciones para el acceso y remuneración, no existen obligaciones ni condiciones para prevenir el fraude cibernético, así como sus consecuencias en caso de incumplimiento.

5. **Necesidad de medidas regulatorias concretas para disuadir y prevenir el fraude:** Con base en lo expuesto, proponemos a la CRC la adopción de medidas específicas en el marco normativo, orientadas a cerrar las brechas aprovechadas por delincuente y elevar los estándares de seguridad en la cadena de valor:

    - **Suspensión de contratos por reincidencia:** Establecer la facultad (y el deber) de los operadores de suspender o terminar la relación contractual con aquellos PCA o integradores tecnológicos que incurran repetidamente en prácticas fraudulentas a través de la red móvil. Actualmente, cuando se detectan fraudes, el recurso sancionatorio efectivo es prácticamente inexistente más allá del retiro del código corto; por ello, dotar a los PRSTM de herramientas contractuales claras para cesar servicios a infractores reincidentes crearía un fuerte incentivo de cumplimiento. La reincidencia debería conllevar sanciones ejemplares, acorde con la gravedad de exponer a miles de usuarios al fraude.

    - **Auditorías periódicas a integradores tecnológicos:** Reforzar la supervisión sobre los integradores asignatarios de códigos cortos mediante auditorías regulares de sus sistemas y protocolos de prevención de fraude. Proponemos que la CRC, en ejercicio de sus funciones de vigilancia, realice (o exija a terceros independientes) realizar evaluaciones periódicas a los integradores, para verificar que estén aplicando filtros robustos de seguridad, actualizando sus mecanismos frente a nuevas modalidades de fraude y cumpliendo con las mejores prácticas de la industria.

    - **Inclusión Obligatoria de Generadores de Contenido en la Cadena Antifraude:** En la cadena de valor del fraude cibernético por servicios móviles, los generadores de contenido juegan un papel crítico al ser quienes efectivamente crean y dirigen las campañas de SMS y llamadas. Aunque tradicionalmente la regulación se ha centrado en operadores y proveedores de conectividad, es indispensable reconocer que sin el control de los contenidos maliciosos desde su origen—ya sea un PCA, un integrador o una aplicación de terceros—ninguna medida técnica de bloqueo o autenticación resultará plenamente eficaz. Por ello, la CRC debe incluir a los generadores de contenido en sus obligaciones regulatorias. Solo integrando a estos actores en los mecanismos de identificación, reporte y sanción de fraudes se podrá cerrar la brecha que actualmente permite que mensajes engañosos se filtren al usuario final y perpetúen el ciclo delictivo.

- **Establecimiento de obligaciones sobre fraude cibernético a los Carrier internacionales:** Para combatir el Spoofing, el que origina el tráfico y el Carrier internacional deben tener la obligación de garantizar que el tráfico que trae hacia Colombia está plenamente identificado con la numeración de origen y debe corresponder a dicho país (puede influir en controlar el fraude de bypass), y no debe venir enmascarado ni alterado (como incluir un numero adicional al inicio o al final, así como que no esté alterado o en desorden).

  Asimismo, el generador de tráfico (caso de algunos Carrier internacionales) tenga la obligación de no cursar tráfico local o nacional como si fuera internacional. Para ello, tendría la obligación de garantizar el correcto enrutamiento de ese tráfico de acuerdo con su origen y con las rutas establecidas para ello.

Agradecemos el espacio que la Comisión habilitó para recibir estos comentarios y quedamos atentos a apoyar en el proceso de construcción de la solución.

Cordialmente,

Samuel Hoyos Mejía.
Presidente de ASOMÓVIL.