Bogotá D.C., 17 de diciembre de 2025

Doctora
Claudia Ximena Bustamante
Directora Ejecutiva
Comisión de Regulación de Comunicaciones (CRC)
Bogotá D.C.

Ref. Comentarios al Documento de Alternativas del Proyecto Regulatorio "Identificación de medidas regulatorias para mitigar el fraude cibernético por medio de servicios móviles".

El presente documento contiene los comentarios y recomendaciones elaborados por el Departamento de Derecho, Comunicaciones y Tecnologías de la Información de la Universidad Externado de Col al Documento de Alternativas del Proyecto Regulatorio "Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles" de conformidad con la publicación oficial y la invitación a la ciudadanía en general a participar en el proceso de consulta pública abierta por la CRC.

La CRC ha incorporado en este proyecto como prioritario en su Agenda Regulatoria 2025–2026, explícitamente dentro del pilar de Bienestar y derechos de los usuarios, con inicio de actividades en el primer trimestre de 2025. Lo cual confirma la pertinencia del abordaje y su alineación con la defensa de la confianza y seguridad en el ecosistema de comunicaciones del país[1].

COMENTARIOS AL PROYECTO

En efecto, el Documento de Alternativas publicado por la CRC para comentarios evidencia una hoja de ruta que articula opciones regulatorias y no regulatorias para la prevención y mitigación del fraude, abarcando medidas de etiquetado de llamadas, bloqueo de tráfico anómalo y fortalecimiento de autenticación en el establecimiento de llamadas[2].

En ese sentido, la iniciativa debe integrarse con la Estrategia Nacional de Seguridad Digital 2025–2027[3], que fija acciones en gobernanza, ciber resiliencia y adecuación del marco normativo, además de impulsar alianzas público–privadas para la protección de infraestructuras y usuarios. [4] (DNP/MinTIC/Presidencia) garantizará que las medidas antifraude se inserten en el esfuerzo transversal de seguridad y confianza digital y en la ampliación de capacidades institucionales.

---

[1] https://www.crcom.gov.co/es/noticias/comunicado-prensa/crc-presenta-su-agenda-regulatoria-2025-2026

[2] https://www.crcom.gov.co/es/noticias/proyectos-regulatorios/publicado-documento-alternativas-regulatorias-identificacion-medidas-fraude%20cibernetico-servicios-moviles

[3] https://mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

[4] https://www.presidencia.gov.co/prensa/Paginas/Estrategia-Nacional-de-Seguridad-Digital-enfrentara-amenazas-ciberneticas-250624.aspx

Finalmente, en lo que corresponde a cualquier tratamiento de datos personales que se requiera para implementar las medidas propuestas debe ajustarse a la Ley Estatutaria 1581 de 2012, con énfasis en legalidad, finalidad, proporcionalidad y seguridad, y coordinarse con los lineamientos de elaborados por la Superintendencia de Industria y Comercio en materia responsabilidad demostrada[5] y privacidad desde el diseño.

Ahora bien, para robustecer el diagnóstico, conviene desagregar tipologías de fraude: (i) suplantación y *spoofing* de CLI (Calling Line Identification) en llamadas internacionales que aparentan números nacionales; (ii) SIM swap y port-out fraud, con toma de control de cuentas mediante cambio de SIM o portaciones maliciosas; (iii) campañas de smishing y robo de credenciales por SMS; y (iv) abusos en interconexión y señalización (SS7) que facilitan filtrado o manipulación de mensajes/llamadas. La literatura internacional[6] (ITU, CEPT/ECC, GSMA, FCC) ha documentado la erosión de confianza en el CLI y ha recomendado acciones de autenticación, bloqueo/supresión de CLI sospechoso y controles reforzados frente a SIM swap/port-out[7]. Asimismo, el diagnóstico debe incorporar cifras y trazabilidad de incidentes, con métricas de *call setup* y patrones de tráfico, tal como sugiere el Documento de Alternativas de la CRC, para fundamentar la proporcionalidad de las intervenciones[8].

Conviene desagregar las tipologías de fraude porque ello permite una caracterización más precisa de los vectores de ataque y sus impactos diferenciados. En efecto, cada modalidad —como el spoofing de identificadores de llamada (CLI), el SIM swap y las portaciones fraudulentas, el smishing mediante SMS, o la manipulación de señalización SS7— presenta mecanismos técnicos, actores involucrados y riesgos específicos que no pueden abordarse con medidas uniformes. Al segmentar estas tipologías, se facilita la adopción de soluciones regulatorias proporcionales y focalizadas, evitando respuestas genéricas que podrían resultar ineficaces o excesivamente restrictivas para la innovación.

Asimismo, permitiría priorizar recursos en función del impacto económico y social de cada modalidad, armonizar las acciones con estándares internacionales (como STIR/SHAKEN para autenticación de llamadas o protocolos antifraude para portaciones), y establecer indicadores diferenciados para evaluar la efectividad de las medidas. En suma, una clasificación desagregada no solo fortalece la evidencia técnica del problema, sino que también contribuye a diseñar un marco regulatorio equilibrado, adaptable y alineado con las mejores prácticas globales.

Sobre las medidas regulatorias:

---

[5] https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

[6] ITU – TR.spoofing Countering spoofing: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-TRUST-2021-PDF-E.pdf

[7] CEPT/ECC – Recomendación (23)03: https://docdb.cept.org/download/4402

[8] GSMA – IR.82 SS7 Security Guidelines: https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/ir-82-ss7-security-network-implementation-guidelines-v5-0/

I. Etiquetado de llamadas "No verificada" / "Probable fraude"

En primer lugar, el etiquetado visible en el dispositivo del usuario para llamadas con CLI no verificable o patrones anómalos es una herramienta preventiva valiosa. No obstante, su eficacia exige estándares de interoperabilidad entre operadores (móviles/fijos/VoIP) y criterios homogéneos de activación para evitar falsos positivos y bloqueos de legítimos (por ejemplo, roaming o desvíos justificables). La experiencia europea (ECC Rec. 23/03) recomienda bloqueo o supresión del CLI en llamadas entrantes internacionales con números nacionales sospechosos, condicionando excepciones por casos de uso legítimos.

Por lo tanto, Colombia podría adoptar un enfoque equivalente, en armonía con ITU E.164 y mejores prácticas de autenticación[9]-[10]. Además, considerando el ecosistema STIR/SHAKEN (y su expansión hacia redes no-IP), el etiquetado debería consumir la información de autenticación cuando esté disponible, y degradarla cuando la cadena de confianza se pierda en segmentos no-IP (soluciones Out-of-Band SHAKEN ya normalizadas)[11].

II. Bloqueo de tráfico anómalo (rates, patrones y reputación)

A continuación, el bloqueo selectivo de tráfico con tasa de establecimiento y distribución de prefijos anómala debe basarse en reglas auditables, listas de reputación dinámicas y mecanismos de *traceback*; ello exige compartición segura de indicadores (con granularidad adecuada) y regímenes de exención para casos legítimos (por ejemplo, centros de contacto verificados). Las guías ITU/GSMA recomiendan contar con equipos antifraude con capacidad de análisis en tiempo real, y la normativa comparada (FCC) refuerza exigencias de autenticación/registro para proveedores que tercerizan el firmado de llamadas[12].

III.Autenticación de llamada y fortalecimiento del CLI (STIR/SHAKEN y verificación)

Seguidamente, la CRC debería fomentar (aunque sin imponer de manera inmediata) la adopción progresiva de STIR/SHAKEN en tramos IP y su extensión Out-of-Band en presencia de segmentos no-IP, de forma coordinada con los operadores y con pruebas piloto sobre roaming, OTT interconectado y call centers. La estandarización 3GPP y ATIS ya contempla APIs y perfiles operativos que facilitan interoperabilidad internacional, reduciendo el spoofing y elevando el grado de atestación[13]. En paralelo, debe mantenerse la armonización con ITU E.164 para integridad del plan de

---

[9] CEPT/ECC – Recomendación (23)03: https://docdb.cept.org/download/4402

[10] GSMA – IR.82 SS7 Security Guidelines: https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/ir-82-ss7-security-network-implementation-guidelines-v5-0/

[11] TransNexus – Nuevo estándar Out-of-Band SHAKEN (ATIS, 2025): https://transnexus.com/blog/2025/new-out-of-band-shaken-standard/

[12] FCC – Call Authentication Trust Anchor (prácticas de terceros): https://docs.fcc.gov/public/attachments/DOC-407144A1.pdf

[13] FCC – Call Authentication Trust Anchor (Final Rule 2025): https://www.federalregister.gov/documents/2025/08/19/2025-15809/call-authentication-trust-anchor

numeración, así como con recomendaciones ITU/ECC contra spoofing que habilitan acciones nacional-internacional[14].

IV. Mitigación de SIM swap y port-out fraud

De igual manera, resulta esencial reforzar la autenticación en cambios de SIM y portaciones, con notificación inmediata al usuario, métodos multifactor, biometría (cuando sea proporcional y conforme a Ley 1581) y ventanas de latencia antes de habilitar cambios sensibles. La regulación comparada de la FCC introduce requisitos concretos en CPNI/LNP para obligar a los operadores a verificar y alertar ante solicitudes de SIM swap/port-out. Colombia podría adaptar ese esquema, coordinándolo con la SIC en materia de protección de datos[15]. A su vez, las recomendaciones ITU sobre riesgos SIM sugieren controles como validación IMSI/ICCID en tiempo real, detección de cambio de dispositivo (device-binding) y notificación preventiva a Proveedores de Servicios Financieros para evitar fraude en autenticaciones basadas en SMS[16].

Sobre las medidas no regulatorias:

Por todo lo anterior, nos parece acertado complementar el andamiaje regulatorio con medidas no regulatorias: (i) campañas de educación digital que habiliten a los usuarios a reconocer llamadas y mensajes maliciosos; (ii) protocolos de cooperación intersectorial y traceback con autoridades (Policía Judicial, MinTIC) y sector financiero, bajo MOU y mesas técnicas; y (iii) sandboxes regulatorios para pilotar soluciones innovadoras (analítica de tráfico, reputación, etiquetado enriquecido, autenticación por RCD), con evaluación en entorno controlado. En el plano internacional, la GSMA Fraud[17] & Security Group (FASG)[18] promueve justamente esquemas de cooperación e intercambio de señales y estándares mínimos de seguridad para operadores, su adopción en Colombia facilitaría convergencia técnica y buenas prácticas.

CONCLUSIONES

En conclusión, cumplir la Ley 1581 de 2012 y los principios de legalidad, finalidad específica, proporcionalidad y seguridad, evitando tratamientos excesivos o innecesarios de datos sensibles (por ejemplo, biometría) sin un DPIA/EIPD previo.

---

[14] ITU – Recomendación E.164 (plan de numeración): https://www.itu.int/rec/T-REC-E.164/en

[15] FCC – Regla final SIM-Swap y Port-Out (2023): https://www.federalregister.gov/documents/2023/12/08/2023-26338/protecting-consumers-from-sim-swap-and-port-out-fraud

[16] ITU – Recomendaciones DFS contra SIM swap y vulnerabilidades: https://www.itu.int/en/ITU-T/webinars/dfs/sc/20241105/Documents/02%20ITU%20DFS%20recommendations%20to%20address%20SIM%20swap%20fraud%20and%20related%20risks.pdf

[17] GSMA – Fraud and Security Group (FASG): https://www.gsma.com/get-involved/working-groups/fraud-security-group/

[18] GSMA – Ponencia FASG sobre fraude (BEREC, 2025): https://www.berec.europa.eu/system/files/2025-05/2.%20GSMA.pdf

La SIC ha desarrollado guías de responsabilidad demostrada (*accountability*) y lineamientos de privacidad desde el diseño y por defecto que se deben incorporar en el ciclo de vida de soluciones antifraude (diseño, prueba, despliegue y monitoreo), lo que le permitiría a la CRC requerir a los operadores, para que estos documenten controles, auditen algoritmos de detección y publiquen resúmenes no técnicos de impacto en privacidad para reforzar la legitimidad y confianza social[19].

En ese sentido, es aconsejable que las medidas se alineen con estándares ITU (E.164 numeración y reportes contra spoofing) y ECC (23/03 sobre manejo de llamadas entrantes internacionales con CLI nacional sospechoso), así como con avances del STIR/SHAKEN (3GPP/ATIS) y su extensión a redes no-IP. Esta armonización reduce brechas de implementación, facilita economías de escala y contribuye a la cooperación transfronteriza frente al fraude.

Sumado a esto, la iniciativa debería articular mesas permanentes entre CRC, MinTIC, Policía Judicial, SIC y sector financiero, usando como marco la Estrategia Nacional de Seguridad Digital 2025–2027 y los comités nacionales allí previstos. En esas mesas se definirán indicadores, intercambio de información (con protocolos de minimización/anonimización) y acuerdos de frontera con países vecinos para coordinación ante spoofing internacional y traceback.

De manera complementaria, se sugiere fijar KPIs verificables: (a) reducción trimestral del volumen de llamadas/SMS maliciosos detectados; (b) tiempo medio de respuesta a incidentes (detección–mitigación–alerta al usuario); (c) porcentaje de llamadas con autenticación (IP y out-of-band) en redes móviles; (d) disminución de reclamaciones por SIM swap/port-out; y (e) satisfacción del usuario (percepción de confianza). Estos KPI pueden integrarse en el tablero de control del proyecto y publicarse en informes periódicos de transparencia.

En suma, la iniciativa de la CRC es necesaria y oportuna para enfrentar el fraude cibernético en servicios móviles. Sin embargo, su efectividad dependerá de:

(i) la precisión técnica de las medidas (etiquetado, bloqueo y autenticación),
(ii) la proporcionalidad y respeto por los derechos fundamentales,
(iii) la interoperabilidad con estándares internacionales, y
(iv) la coordinación institucional sostenida bajo la Estrategia Nacional de Seguridad Digital.

Cordialmente,

Departamento de Derecho, Comunicaciones y Tecnologías de la Información
Facultad de Derecho - Universidad Externado de Colombia

[19] Ley 1581 de 2012 (Función Pública): https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981