

Rad. 2026819792
Cod. 11000
Bogotá, D.C.

Radicado:	2026529119
Fecha:	29/08/2026 6:52:13 P. M.
Proceso:	11000 PROSPECTIVA ESTRATÉGICA E INNOVACIÓN
Destino:	CONGRESO DE LA REPÚBLICA DE COLOMBIA
Asunto:	OBSERVACIONES AL PROYECTO DE LEY NO. 165 DE 2026

Honorable Representante

JULIO ROBERTO SALAZAR PERDOMO

Representante a la Cámara – Departamento de Cundinamarca

CONGRESO DE LA REPÚBLICA DE COLOMBIA

Correo electrónico: uti.julio-salazar@camara.gov.co; julio.salazar@camara.gov.co

Dirección: Carrera 7 No. 8 – 68 Oficinas 531 - 532 - Oficina Nuevo del Congreso

Bogotá

REF: Observaciones al Proyecto de Ley No. 165 de 2026 «por medio del cual se establecen disposiciones para la personalización obligatoria de las tarjetas SIM y se implementan medidas para fortalecer la seguridad en la venta y uso de servicios de telefonía móvil en Colombia».

Honorable Representante Salazar:

La Comisión de Regulación de Comunicaciones (CRC) recibió la solicitud formulada por su Despacho el 24 de agosto de 2026, mediante la cual requiere concepto técnico sobre el Proyecto de Ley No. 165 de 2026 Cámara (en adelante, el proyecto de ley). En atención a dicha solicitud y en el marco de las funciones previstas en la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, esta Comisión presenta las siguientes observaciones.

El Proyecto de Ley 165 de 2026¹ tiene como finalidad fortalecer la seguridad en la venta, activación y uso de los servicios móviles, mediante la identificación de los titulares de las tarjetas SIM, la creación de la Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS) y la implementación de mecanismos de verificación biométrica.

Al respecto, la CRC reconoce la importancia de esta iniciativa legislativa, en tanto busca fortalecer la seguridad de los usuarios de los servicios de telecomunicaciones móviles y contribuir con las autoridades en la prevención e investigación de conductas delictivas asociadas al uso indebido de líneas telefónicas. En particular, la Comisión destaca el interés del legislador en enfrentar fenómenos que afectan de manera relevante a la ciudadanía, como la extorsión, el secuestro extorsivo, el fraude financiero, la suplantación de identidad y otras modalidades delictivas que utilizan los servicios móviles como medio para su comisión o facilitación.

Sin embargo, resulta necesario que la exposición de motivos demuestre, con evidencia suficiente, cuáles son las insuficiencias concretas del marco normativo y regulatorio vigente y cuál sería el beneficio incremental atribuible a la creación de una base nacional centralizada y a la imposición general de mecanismos de verificación biométrica. En particular, se requiere acreditar la necesidad,

¹ Gaceta del Congreso No. 1088 del 21 de agosto de 2026.

idoneidad, proporcionalidad y viabilidad técnica y económica de estas medidas, así como valorar alternativas menos gravosas.

Adicionalmente, es necesario resaltar que la CRC se ha pronunciado anteriormente sobre iniciativas legislativas de objeto similar² al presente proyecto de ley, lo que permite evidenciar la continuidad de la posición institucional en la materia. Sin embargo, estos antecedentes no sustituyen el análisis particular del Proyecto de Ley No. 165 de 2026, cuyo contenido incorpora medidas y salvaguardas que deben ser examinadas específicamente. Por esta razón, las observaciones que se presentan a continuación se concentran en la justificación y el articulado de la iniciativa actualmente sometida a consideración.

1. Comentarios generales

1.1. Identificación del problema y beneficio incremental de las medidas

La exposición de motivos identifica como problemática el uso indebido de los servicios móviles para la comisión de actividades ilícitas y señala que la existencia de líneas anónimas o registradas de manera incorrecta facilitaría conductas como la extorsión, el fraude financiero, el secuestro y el robo de identidad. Para sustentar esta problemática, el Proyecto de Ley presenta cifras asociadas a la utilización de líneas móviles en determinados delitos y plantea la necesidad de fortalecer la identificación y trazabilidad de sus titulares.

No obstante, si bien la exposición de motivos evidencia la existencia de una problemática que se pretende atender, no desarrolla un diagnóstico suficientemente detallado que permita identificar cuál es la falla concreta que explica su ocurrencia y, por tanto, justificar la necesidad de las medidas propuestas. En particular, no permite establecer si el problema obedece principalmente a la ausencia de obligaciones de identificación, al incumplimiento de las existentes, a deficiencias en la calidad o actualización de los registros, a eventos de suplantación durante los procesos de validación, a dificultades o demoras en el acceso de las autoridades a la información, o a una combinación de estos factores.

Esta distinción resulta relevante, en la medida en que cada una de estas causas podría requerir una respuesta normativa diferente: fortalecer el cumplimiento de las obligaciones existentes; mejorar los procedimientos de validación; establecer mecanismos de interoperabilidad; optimizar los canales de consulta de las autoridades; o, si la evidencia así lo demuestra, crear una nueva infraestructura centralizada. Sin una identificación precisa de la causa que se pretende corregir, no es posible determinar si la creación de la BDNTS y la implementación obligatoria de mecanismos biométricos constituyen las alternativas idóneas y necesarias para atender la problemática identificada, ni establecer si sus beneficios adicionales justifican los costos y riesgos asociados a su implementación.

² Entre otros, la CRC se pronunció sobre los proyectos de Ley 535 de 2025 Cámara y 038 de 2025 Cámara, mediante los oficios con radicados CRC 2025511445 del 14 de abril de 2025 y 2025531068 del 24 de septiembre de 2025. También se han identificado otras iniciativas de objeto semejante, entre ellas los proyectos de Ley 269 de 2024 Senado, 381 de 2024 Cámara, 074 de 2025 Senado y 077 de 2026 Cámara.

Por consiguiente, se recomienda complementar la exposición de motivos con información sobre: (i) la proporción de líneas activas cuyos titulares no se encuentran correctamente identificados; (ii) la calidad y actualización de los registros; (iii) los eventos de suplantación asociados a la activación de líneas; (iv) los tiempos actuales de respuesta a las autoridades; (v) las investigaciones afectadas por información fragmentada, incompleta o desactualizada; y (vi) la relación verificable entre esas deficiencias y los delitos que se pretende prevenir.

1.2. Alcance del marco normativo y regulatorio vigente

Para determinar en qué medida la problemática identificada en la exposición de motivos es atendida actualmente, resulta necesario examinar el marco normativo y regulatorio vigente. Para tal efecto, las disposiciones aplicables se presentan en tres grupos: (i) las obligaciones actuales de identificación y actualización de la información de los usuarios; (ii) las medidas complementarias de prevención del fraude y la extorsión; y (iii) aspectos que requieren evaluación frente al marco normativo vigente.

- Obligaciones actuales de identificación y actualización de la información

En primer lugar, los numerales 12 y 13 del artículo 95 de la Ley 1801 de 2016³ establecen que constituyen comportamientos que afectan la seguridad de las personas y sus bienes la activación de líneas telefónicas y tarjetas SIM sin que el usuario haya suministrado al prestador del servicio sus datos biográficos al momento de la activación. De esta manera, el ordenamiento jurídico ya contempla una prohibición expresa frente a la activación anónima de líneas y tarjetas SIM.

Por su parte, la Resolución 912 de 2008⁴, expedida por la Dirección de Investigación Criminal de la Policía Nacional (DIJIN), dispone que los proveedores de redes y servicios de telecomunicaciones, al activar una línea telefónica, deben registrar en sus respectivas bases de datos, entre otros, los nombres y apellidos del suscriptor o usuario, el tipo y número de documento de identificación, el número móvil o de la línea telefónica y la fecha de activación. Asimismo, contempla el registro posterior de otros datos de contacto y establece que la vigilancia del cumplimiento de estas obligaciones corresponde al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

En el ámbito regulatorio, la Resolución CRC 7684 de 2025⁵ modificó los artículos 2.1.3.3 y 2.1.3.4 de la Resolución CRC 5050 de 2016 y estableció obligaciones específicas para la activación de los servicios móviles en modalidad prepago y para la actualización de los datos de identificación de sus usuarios.

³ «Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana».

⁴ «Por la cual se reglamenta el suministro de información de suscriptores y usuarios autorizados para el uso de las telecomunicaciones al igual que las redes de los concesionarios y licenciarios».

⁵ «Por la cual se adoptan medidas para la promoción de la competencia, se modifican algunas disposiciones de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones».

En particular, la regulación dispone que, antes de activar el servicio, los proveedores deben recolectar y validar la información de identificación del usuario. También establece parámetros para la actualización de dicha información, define los medios de atención que deben estar disponibles para adelantar este procedimiento y prohíbe registrar como titular de una línea móvil prepago a quien adquiera tarjetas SIM físicas o virtuales con el propósito de distribuirlas o comercializarlas a terceros.

La Resolución CRC 7684 de 2025 constituye, por tanto, el antecedente regulatorio con mayor relación al objeto del Proyecto de Ley, dado que establece obligaciones específicas para la identificación, validación y actualización de los datos de los usuarios de servicios móviles en modalidad prepago. Por su parte, en los servicios pospago la información de identificación es obtenida por los proveedores en el marco de la relación contractual con el usuario.

Las disposiciones descritas permiten concluir que el ordenamiento jurídico y regulatorio vigente ya contempla obligaciones de identificación, validación y actualización de la información de los usuarios de servicios móviles. Sin embargo, la existencia de estas obligaciones no permite afirmar, por sí sola, que el problema identificado por el proyecto de ley se encuentre solucionado. Para llegar a esa conclusión sería necesario contar con información sobre su implementación, nivel de cumplimiento y resultados.

- Medidas complementarias de prevención del fraude y la extorsión

Además de las obligaciones directamente relacionadas con la identificación de los usuarios, el ordenamiento jurídico y la regulación sectorial contienen medidas complementarias dirigidas a prevenir el fraude, la extorsión y otras conductas ilícitas realizadas mediante servicios móviles.

En este sentido, el artículo 2.1.10.7 de la Resolución CRC 5050 de 2016 establece que los proveedores tienen la obligación de utilizar herramientas tecnológicas adecuadas para prevenir la comisión de fraudes al interior de sus redes y realizar controles periódicos sobre la efectividad de dichos mecanismos. También les impone el deber de investigar las causas de las PQR relacionadas con posibles eventos de fraude y de demostrar al usuario las razones de su decisión cuando concluyan que el fraude no existió.

De otra parte, el Decreto 4768 de 2011⁶ adoptó medidas para restringir la utilización de dispositivos de telecomunicaciones en establecimientos penitenciarios y carcelarios. En desarrollo de estas medidas, MinTIC puede autorizar la inhibición o el bloqueo de señales, o requerir a los proveedores la restricción o eliminación de estas, cuando existan motivos fundados para considerar que desde dichos establecimientos se realizan amenazas, estafas, extorsiones u otros hechos delictivos mediante dispositivos de telecomunicaciones.

⁶ «por medio del cual se adoptan medidas para restringir la utilización de dispositivos de telecomunicaciones en los establecimientos penitenciarios y carcelarios y se dictan otras disposiciones».

En la misma línea, el Decreto 851 de 2024⁷ estableció mecanismos de articulación entre el sector justicia, MinTIC y los proveedores de redes y servicios de telecomunicaciones móviles para fortalecer las estrategias de prevención de la extorsión originada desde establecimientos de reclusión. Entre otras medidas, contempla la posibilidad de solicitar el bloqueo del IMEI de los equipos terminales móviles y del IMSI asociado a las tarjetas SIM identificadas en comunicaciones no autorizadas.

Adicionalmente, mediante la Resolución CRC 8308 de 2026⁸, la Comisión adoptó medidas orientadas a mitigar el fraude cibernético por medio de los servicios móviles. Estas disposiciones incluyen mecanismos para detectar patrones atípicos o sospechosos en llamadas y mensajes de texto, identificar de manera más clara a determinados remitentes, bloquear llamadas que presenten irregularidades en la numeración y fortalecer la coordinación entre operadores, empresas y autoridades a través del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles.

Por su parte, la Ley 2573 de 2026⁹ prevé medidas para proteger a las personas afectadas por eventos de suplantación de identidad frente a reportes negativos y al cobro de obligaciones adquiridas fraudulentamente ante operadores de telecomunicaciones, entidades financieras, crediticias y demás establecimientos comerciales comprendidos en su ámbito de aplicación. No obstante, su objeto principal no consiste en regular la identificación previa a la activación de tarjetas SIM ni en crear un registro nacional de sus titulares. Adicionalmente, debe tenerse en cuenta que la regla general de vigencia de esta ley opera seis meses después de su promulgación, con las excepciones previstas en su artículo 13.

Las medidas descritas atienden manifestaciones específicas del fraude, la extorsión y la suplantación de identidad en diferentes puntos de la cadena. Por tanto, complementan las obligaciones de identificación de los usuarios, pero no equivalen a la creación de un registro nacional de tarjetas SIM ni permiten concluir, por sí solas, que exista una duplicidad con la BDNTS propuesta por el proyecto de ley.

- Aspectos que requieren evaluación frente al marco normativo vigente

A partir del marco normativo y regulatorio expuesto, se observa que actualmente existen obligaciones dirigidas a identificar a los usuarios de los servicios móviles, mantener actualizada su información y prevenir la utilización de las redes para la comisión de fraudes y otras conductas ilícitas. No obstante, para determinar si se requiere una intervención legislativa adicional, resulta

⁷ «Por el cual se dictan disposiciones relacionadas con la restricción de comunicaciones no autorizadas al interior de Establecimientos de Reclusión del Orden Nacional (ERON), se adicionan unos artículos al Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1069 de 2015, y se modifican y derogan algunas disposiciones del Título 11 de la Parte 2 del Libro 2 del Decreto 1078 de 2015».

⁸ «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones».

⁹ «Por medio del cual se establecen medidas para proteger a las personas del reporte negativo ante operadores de información y el cobro de obligaciones en casos de suplantación de identidad ante los operadores de telecomunicaciones, las entidades financieras - crediticias y demás establecimientos comerciales con esta competencia y se dictan otras disposiciones»

necesario establecer, a partir de información verificable, cuáles aspectos de la problemática permanecen sin ser atendidos suficientemente por las medidas vigentes.

En particular, como se expuso previamente, la exposición de motivos no presenta información que permita determinar si las dificultades identificadas obedecen al incumplimiento de las obligaciones existentes, a problemas en la calidad o actualización de la información suministrada por los usuarios, a eventos de suplantación durante los procesos de activación, a la dispersión de los registros entre los diferentes proveedores, a los tiempos requeridos para atender las solicitudes de las autoridades o a una combinación de estos factores.

Esta precisión resulta especialmente relevante frente a la Resolución CRC 7684 de 2025, por ser el antecedente regulatorio que se relaciona con la identificación y actualización de los datos de los usuarios de servicios móviles prepago. Teniendo en cuenta su reciente expedición e implementación, resulta necesario considerar la información disponible sobre su aplicación y, en la medida en que transcurra un periodo suficiente para su evaluación, los resultados obtenidos con las obligaciones de identificación, validación previa y actualización de datos allí establecidas. En ese contexto, no es posible concluir, con fundamento en la información contenida en la exposición de motivos, que el régimen vigente haya solucionado integralmente la problemática.

Tampoco se encuentra acreditado en la exposición de motivos que la creación de la BDNTS y la imposición general de mecanismos biométricos constituyan las alternativas más adecuadas para atenderla.

En consecuencia, se recomienda complementar la justificación de la iniciativa con información que permita determinar: (i) qué componentes de la problemática son atendidos por las obligaciones vigentes; (ii) cuáles dificultades persisten en su aplicación; (iii) cuál es su magnitud; y (iv) de qué manera las nuevas medidas producirían un beneficio adicional y verificable frente al régimen actual.

Este análisis permitiría valorar si los beneficios esperados de la BDNTS y de la verificación biométrica obligatoria justifican sus costos, riesgos y cargas de implementación, así como comparar estas medidas con otras alternativas que permitan alcanzar la misma finalidad.

1.3. Calidad y trazabilidad de la evidencia presentada

La exposición de motivos incorpora diferentes cifras con las que se busca acreditar la magnitud de la problemática y la efectividad de las medidas propuestas. Entre ellas, señala que un porcentaje significativo de los casos de extorsión y secuestro extorsivo reportados entre 2020 y 2023 habría involucrado líneas móviles mal registradas o anónimas; atribuye a Asobancaria una estimación de pérdidas anuales superiores a quinientos mil millones de pesos por fraudes cibernéticos derivados del uso de líneas móviles no registradas; y presenta cifras sobre la reducción de delitos y el mejoramiento de las capacidades investigativas que habrían experimentado España, México y Alemania después de implementar mecanismos de identificación de usuarios, registros de tarjetas SIM o sistemas de verificación biométrica.

Sin perjuicio de la relevancia de esta información para dimensionar la problemática, las cifras presentadas no permiten establecer, por sí solas, una relación causal entre la falta de identificación de los titulares de las tarjetas SIM y la ocurrencia de los delitos mencionados. Tampoco demuestran que la creación de una base nacional centralizada o la imposición general de mecanismos biométricos produzcan necesariamente una reducción de estas conductas o una mejora de las capacidades investigativas.

En efecto, la participación de una línea mal registrada o anónima en una conducta delictiva permite identificar una asociación entre ambos fenómenos, pero no demuestra que la ausencia de registro sea la causa determinante del delito ni que su adecuada identificación hubiera impedido su comisión. Para establecer dicha relación resulta necesario determinar, entre otros aspectos, de qué manera la falta o incorrección del registro obstaculizó la investigación, si la persona identificada como titular correspondía al usuario real de la línea y en qué medida una base centralizada o una validación biométrica habría modificado el resultado.

En el ámbito nacional, la información presentada tampoco permite establecer si los porcentajes reportados corresponden al total de denuncias, investigaciones, casos esclarecidos, capturas, imputaciones o condenas. Esta distinción resulta relevante, pues cada una de estas categorías mide un aspecto diferente de la problemática y no permite inferir automáticamente la efectividad que tendría una medida de identificación o centralización de datos.

En relación con la cifra atribuida a Asobancaria, aun si esta correspondiera a pérdidas por fraudes cibernéticos en los que fueron utilizadas comunicaciones móviles, ello no permitiría concluir que la totalidad de dichas pérdidas sea atribuible a líneas no registradas ni que pudiera evitarse mediante la BDNTS o la biometría obligatoria. Para sustentar esa conclusión sería necesario establecer qué proporción de los eventos estuvo asociada específicamente a deficiencias en la identificación de los titulares y de qué manera las medidas propuestas habrían prevenido o mitigado el fraude.

De igual forma, aunque la exposición de motivos identifica las medidas adoptadas en España, México y Alemania y presenta separadamente los resultados atribuidos a cada experiencia, no explica la metodología con fundamento en la cual establece una relación causal entre su implementación y la reducción de los índices delictivos o el mejoramiento de las capacidades investigativas. La circunstancia de que determinados resultados se hayan observado después de la adopción de una medida de identificación, registro o verificación biométrica evidencia una relación temporal, pero no permite concluir, por sí sola, que tales resultados hayan sido producidos por dicha intervención.

Para sustentar esa relación causal resulta necesario considerar otros factores concurrentes que también podrían haber incidido en los resultados, como modificaciones en la legislación penal, cambios en las capacidades de investigación y judicialización, variaciones en los niveles de denuncia, implementación simultánea de otras herramientas antifraude y evolución general de las

conductas delictivas. Asimismo, debería precisarse si los resultados presentados corresponden a evaluaciones específicas de impacto de las medidas o a variaciones generales en los indicadores de criminalidad observadas durante el mismo periodo.

Además, deben examinarse tanto los resultados favorables como las dificultades de implementación. Esto resulta particularmente relevante respecto de México, dado que el propio proyecto de ley reconoce que el Registro Nacional de Usuarios de Telefonía Móvil fue descontinuado por problemas administrativos y de control. Esta experiencia, por tanto, no solo aporta elementos sobre los beneficios esperados, sino también sobre los riesgos de calidad de la información, seguridad, sostenibilidad y gobernanza de un registro centralizado.

Por lo anterior, se recomienda fortalecer la exposición de motivos explicando la relación existente entre la evidencia presentada, las causas específicas del problema y cada una de las medidas propuestas. En particular, debería demostrarse: (i) en qué medida la falta o incorrección de los registros facilita la comisión de los delitos o afecta su investigación; (ii) cuál sería el beneficio adicional de centralizar información que actualmente administran los operadores; y (iii) qué resultado incremental produciría la biometría frente a otros mecanismos de verificación de identidad.

En consecuencia, la información presentada puede contribuir a evidenciar la existencia y relevancia de la problemática, pero no resulta suficiente para demostrar que la BDNTS y la biometría obligatoria sean las medidas idóneas, necesarias y proporcionales para atenderla. Para sustentar la intervención propuesta se requiere establecer un vínculo más preciso entre las causas identificadas, las medidas seleccionadas y los resultados que se espera obtener.

1.4. Creación de la Base de Datos Nacional de Registro de Tarjetas SIM

El hecho de que los PRSTM administren actualmente información de sus usuarios no permite concluir, por sí solo, que una base centralizada carezca de utilidad. La centralización podría generar beneficios relacionados con la oportunidad, uniformidad y trazabilidad de las consultas, facilitar la identificación de líneas asociadas a una misma persona y reducir cargas derivadas de solicitudes dirigidas a múltiples operadores.

No obstante, la exposición de motivos no presenta un diagnóstico que permita establecer si esos beneficios responden a fallas verificadas del modelo actual ni si superan los costos y riesgos derivados de crear una nueva infraestructura. Antes de adoptar la BDNTS se requiere información sobre la calidad y actualización de los registros existentes, los tiempos de respuesta a las autoridades, las investigaciones afectadas por la fragmentación, los requerimientos de interoperabilidad y los costos de construcción, migración, operación, mantenimiento y seguridad.

También deben definirse el modelo de gobierno de datos, las responsabilidades por errores, indisponibilidad o incidentes, los niveles de servicio, los mecanismos de corrección de información y la justificación de cada categoría de datos que se pretende centralizar. En particular, debe

evaluarse si campos como dirección de residencia, correo electrónico e historial de cambios son estrictamente necesarios para las finalidades de la ley.

La concentración de información personal en una infraestructura nacional puede crear un objetivo de alto valor para ataques y un punto único de falla. La evaluación debe comparar la creación de una base centralizada con otras alternativas que permitan atender las necesidades de acceso, oportunidad, uniformidad y trazabilidad de la información, considerando sus respectivos costos, riesgos, beneficios y condiciones de implementación.

El proyecto de ley incorpora salvaguardas relevantes: limita la retención de información, restringe el acceso a autoridades en el marco de investigaciones, ordena registrar las consultas, prohíbe el almacenamiento de biometría en bruto en la BDNTS y exige medidas de seguridad. Estas garantías reducen algunos riesgos, pero no sustituyen la demostración de la necesidad y proporcionalidad de centralizar la información.

1.5. Verificación biométrica obligatoria

Los datos biométricos tienen la condición de datos personales sensibles y su tratamiento exige una justificación reforzada en atención a los riesgos que puede representar para los derechos de sus titulares. El Proyecto de Ley incorpora salvaguardas relevantes al disponer que la biometría se utilice exclusivamente para el cotejo de identidad al momento de la activación; prohibir el almacenamiento del dato biométrico en bruto en la BDNTS; limitar la conservación de las plantillas biométricas; restringir las finalidades de su tratamiento; contemplar mecanismos alternativos de identificación; y establecer que la imposibilidad de utilizar la biometría no puede traducirse en la negación del servicio. Estas previsiones contribuyen a reducir algunos de los riesgos asociados a la privacidad y a la exclusión de determinados usuarios.

En particular, la exposición de motivos no contiene información sobre los costos de implementación y operación; las tasas de falsos rechazos; los riesgos de suplantación biométrica; la cobertura territorial; la capacidad y disponibilidad de los servicios de identificación de la Registraduría Nacional del Estado Civil; el funcionamiento de los mecanismos en zonas sin conectividad; la utilización de pruebas de vida; ni los procedimientos de atención aplicables cuando la biometría de una persona no pueda ser utilizada. Estos elementos resultan necesarios para evaluar la viabilidad técnica, operativa y económica de la medida y sus posibles efectos sobre el acceso a los servicios móviles.

En consecuencia, la información presentada no permite concluir que la imposición general de la biometría constituya una medida necesaria y proporcional, aunque tampoco aporta elementos suficientes para descartar definitivamente la utilización de esta tecnología. Por ello, se recomienda evaluar comparativamente la efectividad, los costos y los riesgos de las diferentes alternativas de verificación de identidad.

Dentro de esta evaluación debería considerarse la posibilidad de mantener como mecanismo general la constatación de documentos oficiales de identidad antes de la activación del servicio, de conformidad con las obligaciones regulatorias vigentes, sin perjuicio de que los PRST puedan

implementar mecanismos biométricos de acuerdo con sus capacidades, condiciones de operación y niveles de riesgo. Esta alternativa deberá compararse con la imposición general de la biometría y con los mecanismos alternativos contemplados en el propio Proyecto de Ley, a fin de determinar cuál ofrece una respuesta más eficiente y proporcional.

Solo a partir de este análisis sería posible establecer si la biometría debe imponerse con carácter obligatorio y general, aplicarse de manera focalizada o permanecer como una herramienta que los proveedores puedan utilizar dentro de sus procesos de validación, con sujeción a las garantías aplicables al tratamiento de datos sensibles.

2. Comentarios específicos sobre el articulado propuesto

2.1. Identificación del titular — artículo 3

Las obligaciones de identificación y validación de los usuarios de servicios móviles ya son objeto de regulación sectorial, como se expuso en los comentarios generales. En particular, el artículo 4 de la Resolución CRC 7684 de 2025 adicionó el artículo 2.1.3.3 a la Resolución CRC 5050 de 2016 y estableció el procedimiento que deben observar los proveedores para la activación de servicios móviles en modalidad prepago.

De acuerdo con esta disposición, antes de la activación del servicio, los proveedores deben recolectar y validar la información de identificación del usuario. Asimismo, la regulación prohíbe registrar como titular de una línea móvil prepago a quien adquiera tarjetas SIM físicas o virtuales con el propósito de distribuir las o comercializarlas a terceros.

Por su parte, el artículo 2.1.3.4 de la Resolución CRC 5050 de 2016 establece los parámetros aplicables a la actualización de los datos de identificación de los usuarios de servicios móviles en modalidad prepago. En cuanto a los servicios pospago, la información de identificación del usuario es obtenida por los proveedores en el marco de la relación contractual.

En consecuencia, se recomienda tener en cuenta las obligaciones regulatorias vigentes al evaluar el contenido y alcance del artículo 3 del Proyecto de Ley.

2.2. BDNTS — artículos 4 a 8

Sin perjuicio de las consideraciones generales expuestas sobre la necesidad y proporcionalidad de la BDNTS, se recomienda revisar los artículos 4 a 8 para delimitar con precisión la responsabilidad de MinTIC como responsable del tratamiento, la calidad en la que actuarían los operadores respecto de la información reportada y la intervención de la CRC exclusivamente dentro del ámbito de sus competencias regulatorias.

En relación con el artículo 5, debe justificarse la necesidad de cada una de las categorías de información que integrarían la BDNTS. En particular, se recomienda eliminar la expresión abierta «otros datos relevantes» o delimitarla mediante criterios estrictos de necesidad, finalidad y

minimización, teniendo en cuenta que una habilitación indeterminada podría permitir la incorporación posterior de información no indispensable para los objetivos de la ley.

Se valora positivamente que los artículos 6 y 8 establezcan periodos limitados de retención, condiciones de acceso restringido y el registro de las consultas. No obstante, deben precisarse los responsables y procedimientos de supresión, anonimización, auditoría y control.

Asimismo, se valora positivamente el párrafo 1 del artículo 7, que exige notificación previa, al menos dos avisos efectivos, suspensión reversible, acceso a números de emergencia y consideración de poblaciones vulnerables. Sin perjuicio de ello, estas disposiciones deben armonizarse con el régimen de protección de los usuarios y delimitar cuáles datos requieren actualización para evitar que cualquier modificación en información accesorio pueda dar lugar a la suspensión del servicio.

2.3. Verificación biométrica e interoperabilidad — artículos 12 y 13

Sin perjuicio del análisis general sobre la necesidad y proporcionalidad de la biometría, se reconocen las salvaguardas previstas en los párrafos del artículo 12, relacionadas con la limitación de la finalidad, la prohibición de almacenar el dato biométrico en bruto, la supresión de las plantillas y la disponibilidad de mecanismos alternativos cuando no pueda realizarse la verificación biométrica.

No obstante, debe aclararse la relación entre el carácter obligatorio de la verificación biométrica previsto en el artículo 12 y la expresión «podrán interoperar» contenida en el artículo 13. La redacción propuesta no permite establecer cuál sería el mecanismo obligatorio de cotejo cuando no se utilicen los servicios de identificación de la Registraduría Nacional del Estado Civil.

Asimismo, la implementación de la interoperabilidad requiere determinar previamente las capacidades institucionales, condiciones técnicas, niveles de servicio, requisitos de seguridad, costos y responsabilidades de los participantes.

2.4. Comercialización, activación y regímenes especiales — artículos 14 y 15

La comercialización, la activación y el uso son actividades diferentes y pueden involucrar responsables distintos. La obligación de asegurar que una línea no sea activada sin identificación debe recaer principalmente en el PRSTM que controla técnicamente la activación. La entrega o comercialización de una SIM no activada no produce, por sí sola, el mismo riesgo que su activación anónima.

Se recomienda revisar la prohibición del artículo 14 para diferenciar la venta de una SIM inactiva de la activación y prestación del servicio sin registro. Asimismo, debe armonizarse el régimen de los puntos de venta con la prohibición del artículo 2.1.3.3.7 de la Resolución CRC 5050 de 2016, según la cual el operador no puede registrar como titular de una línea prepago a quien adquiere SIM para distribuir las o comercializarlas a terceros.

Se valora que el artículo 15 contemple reglas diferenciadas para líneas M2M/IoT, SIM corporativas, eSIM y roaming, pues estos casos no responden necesariamente al esquema de una persona natural identificada biométricamente por cada dispositivo. No obstante, conviene precisar las responsabilidades de las personas jurídicas y el alcance del inventario de asignaciones.

2.5. Sanciones, vigilancia y control — artículos 16 y 17

El artículo 16 reconoce competencias diferenciadas de MinTIC y la SIC. Esta distribución debe mantenerse y armonizarse con el artículo 17. En particular, el segundo inciso del artículo 17 debería ajustarse para evitar que la referencia general a inspecciones, auditorías, verificaciones y sanciones sea interpretada como una atribución indistinta a todas las entidades, incluida la CRC.

También se recomienda revisar la responsabilidad solidaria de los puntos de venta. La solidaridad sancionatoria requiere una definición clara de las conductas, sujetos responsables y criterios de imputación. No debería derivarse automáticamente de cualquier incumplimiento del operador cuando el punto de venta no tenga control material sobre la activación o el funcionamiento de la BDNTS.

2.6. Reglamentación — artículo 18

El artículo 18 debe diferenciar la potestad reglamentaria del Gobierno Nacional de las competencias regulatorias de la CRC y de las funciones de la SIC. La coordinación institucional no debe traducirse en una atribución conjunta e indistinta para expedir todas las disposiciones de implementación.

La ley puede fijar los límites y elementos esenciales, mientras que cada autoridad debería desarrollar los asuntos comprendidos en sus competencias mediante el instrumento jurídico correspondiente. En ningún caso la reglamentación puede crear conductas sancionables, sujetos responsables o sanciones no definidos por el legislador.

2.7. Régimen de transición — artículos 19 y 20

El régimen de transición incorpora avisos previos, campañas gratuitas, suspensión reversible y acceso a números de emergencia, elementos que reducen los riesgos para los usuarios. No obstante, el plazo y las condiciones de regularización deberían definirse a partir de información sobre el universo de líneas, la capacidad operativa de los canales de actualización y las necesidades de poblaciones vulnerables o ubicadas en zonas con conectividad limitada.

Además, la exigibilidad de la biometría y de las obligaciones dependientes de la BDNTS debería condicionarse no solo a la entrada en operación formal de la base, sino a la verificación de condiciones mínimas de disponibilidad, seguridad, interoperabilidad y cobertura, con planes de contingencia que eviten afectaciones masivas al servicio.

3. Consideraciones finales

La CRC comparte la finalidad de fortalecer la seguridad de los servicios móviles y de mejorar las capacidades institucionales para prevenir e investigar conductas ilícitas. El Proyecto de Ley, además, incorpora salvaguardas relevantes en materia de tratamiento biométrico, mecanismos alternativos de identificación, retención temporal, registro de consultas, acceso restringido y distribución inicial de funciones.

Sin embargo, la exposición de motivos no acredita todavía, de manera suficiente, el valor añadido, los costos, la viabilidad ni la proporcionalidad de la BDNTS y de la biometría obligatoria frente al régimen vigente. Tampoco permite establecer si la problemática obedece a la ausencia de obligaciones normativas, al incumplimiento de las existentes, a dificultades en la calidad o actualización de los registros, a la fragmentación de la información, a condiciones operativas de acceso o a una combinación de estos factores.

Por ello, se recomienda fortalecer el diagnóstico; verificar y documentar las fuentes nacionales e internacionales; establecer una línea base posterior a la Resolución CRC 7684 de 2025; comparar alternativas; cuantificar costos y responsables; definir indicadores de resultado; y delimitar claramente las competencias de MinTIC, la SIC y la CRC. Con esta información será posible determinar si las medidas propuestas generan beneficios incrementales suficientes y si constituyen la intervención más adecuada para alcanzar la finalidad perseguida.

En los anteriores términos damos respuesta a su consulta y quedamos atentos a cualquier aclaración adicional que requiera.

Cordial saludo,

DIAZ SUAZA

FELIPE

AUGUSTO

FELIPE AUGUSTO DÍAZ SUAZA

Director Ejecutivo

Firmado digitalmente
por DIAZ SUAZA
FELIPE AUGUSTO
Fecha: 2026.08.29
18:53:37 -05'00'

Proyectado por: Amparo Cubillos Vargas

Revisado por: Víctor Baldrich



SC 1390-1



@CRCCol



/CRCCol



/CRCCol



CRCCOL



@CRCCol

Calle 59A BIS No. 5-53, Edificio Link Siete Sesenta, piso 9 Bogotá, D.C.
Código postal 110231 - Teléfono +57 601 319 8300
Línea gratuita nacional 018000 919278