

Rad. 2026201760
Cod. 11000
Bogotá, D.C.

Radicado:	2026534711
Fecha:	15/10/2026 11:01:26 A. M.
Proceso:	11000 PROSPECTIVA ESTRATÉGICA E INNOVACIÓN
Destino:	CONGRESO DE LA REPÚBLICA DE COLOMBIA
Asunto:	OBSERVACIONES AL PROYECTO DE LEY NO. 204 DE 2026 SENADO «POR MEDIO DEL CUAL SE REGULA LA COMERCIALIZACIÓN, ACTIVACIÓN, REGISTRO Y USO DE TARJETAS SIM, FÍSICA O VIRTUAL O LA TECNOLOGÍA QUE LAS REMPLACE, Y SE DICTAN OTRAS DISPOSICIONES».

Honorable Senador
SANTIAGO BARRETO TRIANA
Senador de la República
CONGRESO DE LA REPÚBLICA DE COLOMBIA
Correo electrónico: santiago.barreto@senado.gov.co; comision.sexta@senado.gov.co
Dirección: Carrera 7 No. 8 – 68 Oficina 704 Edificio Nuevo del Congreso
Bogotá D.C.

REF: Observaciones al Proyecto de Ley No. 204 de 2026 Senado «por medio del cual se regula la comercialización, activación, registro y uso de tarjetas SIM, física o virtual o la tecnología que las remplace, y se dictan otras disposiciones».

Honorable Senador Barreto:

La Comisión de Regulación de Comunicaciones (CRC), en ejercicio de las funciones previstas en la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, presenta sus observaciones al Proyecto de Ley 204 de 2026 Senado¹, que propone crear una Base de Datos Nacional de Registro de Tarjetas SIM (BDNTS), establecer mecanismos de identificación y autenticación de usuarios y definir obligaciones y sanciones para los actores involucrados.

La CRC comparte el propósito de fortalecer la seguridad de los usuarios y facilitar la prevención e investigación de delitos como la extorsión, el secuestro y la suplantación de identidad. Sin embargo, la relevancia de estos objetivos no demuestra, por sí sola, que una base centralizada y la autenticación biométrica obligatoria sean las respuestas más adecuadas. La cuestión central es identificar qué deficiencias persisten en el régimen vigente, quién tiene capacidad efectiva para corregirlas y qué beneficios adicionales producirían las nuevas medidas frente a sus costos, riesgos y alternativas.

Este examen resulta especialmente importante porque el ordenamiento ya contempla obligaciones de identificación, validación y actualización de usuarios, así como instrumentos de prevención del fraude. Una dificultad originada en el incumplimiento de esas reglas no exige necesariamente la misma respuesta que otra derivada de registros deficientes, suplantaciones o demoras en el acceso a información. Además, mejorar la trazabilidad de una línea o la oportunidad de una consulta no equivale necesariamente a reducir la incidencia del delito; cada resultado requiere una justificación y una forma de verificación propias.

En esta línea, la CRC considera conveniente fortalecer la iniciativa en cuatro aspectos: (i) precisar la falla que se pretende corregir y el beneficio incremental de las medidas; (ii) comparar alternativas

¹ Gaceta del Congreso No. 1276 del 25 de agosto de 2026.

de identificación, autenticación y gestión de información, incluidas arquitecturas interoperables que no requieran centralizar todos los registros; (iii) asignar obligaciones, costos y responsabilidades conforme a la capacidad efectiva de control de cada actor, considerando sus efectos sobre la competencia y el acceso al servicio; y (iv) delimitar las competencias institucionales y las condiciones de protección de datos, financiación, supervisión e implementación.

Estas observaciones dan continuidad a los pronunciamientos de la CRC sobre los Proyectos de Ley 381 de 2024, 074, 038 y 535 de 2025, y 165 y 077 de 2026. En ellos, la Comisión ha recordado de manera consistente que el ordenamiento ya contempla medidas de identificación de usuarios móviles y prevención del fraude. Por ello, ha insistido en que cualquier nueva obligación se sustente en una identificación clara de la causa raíz del problema y en análisis de necesidad, proporcionalidad y viabilidad técnica, operativa y económica.

Respecto de la biometría, ha advertido que se trata de datos sensibles y que su uso obligatorio implica costos significativos para los PRST y los usuarios. Su efectividad, además, se ve limitada por brechas de conectividad y de acceso a dispositivos, y depende de la capacidad de la Registraduría. Frente a las bases de datos centralizadas y los esquemas de interoperabilidad, ha pedido precisar su valor agregado, diseño, financiación y gobernanza. Ha recomendado también que cada actor asuma los costos de sus propios sistemas y que su administración recaiga en una entidad con competencias en investigación criminal, como la DIJIN. Por último, ha señalado que la intervención de la CRC debe circunscribirse a la definición de condiciones técnicas y operativas, sin abarcar funciones de financiación, administración de infraestructura ni inspección, vigilancia y control. En el caso de las llamadas desde centros penitenciarios, ha indicado que la solución corresponde al fortalecimiento del control del INPEC.

Teniendo en cuenta lo anterior, se presentan las siguientes consideraciones sobre la justificación y el articulado del Proyecto.

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 facilita conductas como la extorsión, el secuestro y la suplantación 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.

Sin embargo, la información presentada no permite establecer con suficiente precisión cuál es la falla que se pretende corregir. Identificar la causa es determinante, pues las deficiencias en el diseño o cumplimiento de las obligaciones de identificación, la calidad de los registros y el acceso de las autoridades a la información pueden requerir respuestas distintas. No todas estas dificultades se resuelven necesariamente mediante una base centralizada o mecanismos de autenticación biométrica. Además, mejorar la calidad de los registros, facilitar la investigación y prevenir delitos

son resultados relacionados, pero distintos, cuya efectividad debe evaluarse de manera diferenciada.

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 pretenden 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 2016² 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 2008³, 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 2025⁴ 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

² «Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana».

³ «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».

⁴ «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».

servicios móviles en modalidad prepago y para la actualización de los datos de identificación de sus usuarios.

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 distribuir las 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.

- 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, existen otras normas que 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 2011⁵ 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.

En la misma línea, el Decreto 851 de 2024⁶ 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

⁵ «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».

⁶ «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».

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 2026⁷, 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.

La Resolución CRC 8308 de 2026 interviene sobre riesgos asociados al fraude mediante llamadas y mensajes, distintos de los problemas de identificación de titulares que aborda el Proyecto. Por ello, ambas iniciativas deben examinarse como instrumentos potencialmente complementarios, identificando qué riesgo atiende cada una y qué beneficios adicionales se esperan de las nuevas obligaciones.

Por su parte, la Ley 2573 de 2026⁸ 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

El marco normativo y regulatorio descrito evidencia que ya existen obligaciones de identificación, validación y actualización de la información de los usuarios, así como instrumentos para prevenir el fraude y otras conductas ilícitas. Sin embargo, la existencia de estas medidas no permite concluir que la problemática esté solucionada. Para valorar la necesidad de una intervención legislativa

⁷ «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones».

⁸ «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».

adicional, convendría establecer qué dificultades persisten, cuál es su magnitud y en qué medida obedecen al diseño de las obligaciones vigentes, a su cumplimiento o a necesidades adicionales de información e interoperabilidad.

Esta evaluación resulta especialmente relevante frente a la Resolución CRC 7684 de 2025, por tratarse de una intervención reciente sobre la identificación y actualización de los usuarios prepago. Su implementación requiere un periodo suficiente de observación para valorar sus resultados, sin que ello impida examinar la información actualmente disponible. En consecuencia, convendría determinar qué beneficios adicionales y verificables producirían las medidas propuestas frente al régimen vigente, y si estos justifican sus costos y riesgos en comparación con otras alternativas de intervención.

1.3. Pertinencia y suficiencia de la evidencia presentada

La exposición de motivos presenta cifras sobre extorsión y secuestro por departamento durante 2025 y el primer semestre de 2026, así como información sobre ingresos del sector, líneas móviles prepago sin compra y tráfico mensual de voz. También examina experiencias regulatorias de Alemania, México, Brasil, Chile y la Unión Europea. Esta información permite dimensionar la problemática y caracterizar el mercado, pero su capacidad para justificar las medidas propuestas depende de la relación que pueda establecerse entre los indicadores, las causas identificadas y los resultados esperados.

Las cifras de ingresos, líneas prepago sin compra y tráfico de voz permiten caracterizar la dinámica del mercado móvil, pero no constituyen, por sí solas, indicadores de la ocurrencia de delitos como la extorsión o el secuestro. Los ingresos responden a condiciones de consumo, competencia y evolución tecnológica; las líneas prepago sin actividad comercial reciente pueden corresponder a usos legítimos y no permiten establecer la finalidad de su utilización; y las variaciones en el tráfico de voz pueden explicarse por cambios en los hábitos de consumo o procesos de sustitución tecnológica. En consecuencia, estos indicadores no permiten establecer una relación causal entre las condiciones del mercado y las conductas delictivas que el Proyecto pretende combatir.

Las experiencias internacionales citadas tampoco permiten concluir, por su sola adopción, que los mecanismos de identificación o registro hayan reducido la incidencia delictiva o mejorado las capacidades investigativas. Para valorar sus resultados convendría contar con evidencia que permita distinguir los efectos de estas medidas de otros factores, como el fortalecimiento institucional, las estrategias de investigación criminal y las variaciones en las dinámicas de denuncia. La existencia de un mecanismo en otra jurisdicción no acredita, por sí misma, su efectividad ni su conveniencia para Colombia.

Adicionalmente, la revisión de las experiencias internacionales tampoco revela un modelo uniforme de identificación. Por el contrario, muestra distintas combinaciones de verificación documental, controles sobre equipos y sistemas de registro. En particular, el caso mexicano ofrece una referencia relevante, pues la Suprema Corte de Justicia de la Nación invalidó en 2022 el Padrón

Nacional de Usuarios de Telefonía Móvil⁹, que contemplaba la recopilación de datos biométricos. Esta experiencia refuerza la importancia de examinar la justificación, proporcionalidad y condiciones de implementación de cada alternativa, en lugar de asumir que la existencia de registros en otras jurisdicciones acredita la conveniencia de un modelo específico para Colombia..

Lo anterior no desconoce la importancia de mantener actualizados los registros de usuarios ni de fortalecer su identificación y trazabilidad. Por el contrario, para justificar las medidas propuestas resultarían más pertinentes indicadores directamente relacionados con las deficiencias que se pretende corregir, como la proporción de registros incompletos o no verificables, las activaciones fraudulentas, los eventos de suplantación, los tiempos de respuesta a las autoridades y las investigaciones afectadas por información incorrecta o fragmentada. Esta evidencia permitiría evaluar con mayor precisión la necesidad de la intervención y el beneficio adicional que podría producir frente al régimen vigente.

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 mejoras verificables ofrecería la biometría frente a otros mecanismos de verificación de identidad.

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 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.

9

La concentración de información personal en una infraestructura nacional puede aumentar el impacto de incidentes de seguridad o indisponibilidad. Por ello, convendría comparar la centralización de registros con una arquitectura federada que permita consultas unificadas, autenticadas y trazables, conservando la información en los sistemas de los proveedores. Esta comparación debería considerar los costos, la calidad de los datos, los tiempos de respuesta, la seguridad y la continuidad operativa, sin asumir que alguna de las arquitecturas resulta necesariamente superior en todas estas dimensiones.

1.5. Verificación biométrica

Los datos biométricos son datos personales sensibles y su utilización exige una justificación específica. Aunque el Proyecto propone fortalecer la identificación de los usuarios mediante estos mecanismos, la exposición de motivos no desarrolla suficientemente sus costos de implementación y operación, los riesgos de suplantación biométrica, la disponibilidad de los servicios de contraste de identidad ni las condiciones de funcionamiento en zonas con conectividad limitada. Estos elementos son determinantes para valorar la viabilidad de la medida y sus efectos sobre el acceso al servicio.

También convendría distinguir entre la autenticación de una persona frente a una identidad previamente declarada y su identificación dentro de una base de registros. Estas operaciones tienen requerimientos diferentes de arquitectura, precisión y seguridad. Su evaluación debería considerar las tasas de falsos positivos y negativos, los mecanismos de prueba de vida, la disponibilidad de las fuentes de contraste y las alternativas de validación cuando el procedimiento falle, para evitar que los controles contra la suplantación terminen excluyendo a usuarios legítimos.

En consecuencia, la implementación general de mecanismos biométricos debería compararse con la validación documental prevista en el régimen vigente y con otras alternativas de identificación, considerando su efectividad, costos, riesgos y condiciones de operación. Esta evaluación permitiría determinar si resulta justificada una exigencia general, una aplicación focalizada según el riesgo o un esquema que admita distintos mecanismos de validación.

Si bien el proyecto no establece de manera expresa si la recolección de datos biométricos tendrá carácter obligatorio, se recomienda evaluar si la incorporación de dicha exigencia podría incidir en el núcleo esencial del derecho fundamental a la protección de datos personales, en la medida en que supondría otorgar el dato en escenarios distintos a los previstos actualmente en el artículo 6 de la Ley 1581 de 2012 y, en consecuencia, analizar la necesidad de un trámite estatutario.

2. Comentarios específicos sobre el articulado propuesto

Los comentarios al articulado siguen el criterio común de asignar las obligaciones y responsabilidades conforme a las funciones y capacidades de control de cada actor, de manera que los incentivos de cumplimiento correspondan a los riesgos que efectivamente puede gestionar.

2.1. Sobre las definiciones — artículo 2

Las definiciones de los literales g), i), j) y k) del artículo 2 deberían armonizarse con las categorías previstas en la Ley 1581 de 2012 y distinguir entre la tarjeta SIM o elemento seguro, el perfil electrónico, la suscripción, el número asignado, el titular contractual y el usuario efectivo. Estas categorías no necesariamente coinciden, particularmente en el caso de las eSIM, cuya provisión puede realizarse de forma remota. Su diferenciación permitiría precisar qué información debe registrarse, cuándo nace cada obligación y qué actor responde por su cumplimiento.

2.2. BDNTS — artículo 4

La implementación de la BDNTS requiere definir qué entidad administra y opera la plataforma, quién responde por el tratamiento de los datos y qué obligaciones conservan los proveedores sobre la calidad y actualización de la información. Esta distribución debería contemplar las responsabilidades por errores, incidentes de seguridad e indisponibilidad, así como los mecanismos de corrección y rendición de cuentas. Sin una delimitación de funciones, podrían presentarse dificultades para establecer qué actor responde por cada incumplimiento.

La intervención de la CRC en la implementación de la BDNTS debería circunscribirse a las competencias previstas en la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, particularmente en la definición de las condiciones técnicas y operativas exigibles a los proveedores de redes y servicios de telecomunicaciones móviles. Estas podrían comprender aspectos de interoperabilidad, protocolos y formatos de intercambio, autenticación, seguridad, trazabilidad y disponibilidad de la información. Ello no supone atribuirle la administración, custodia, operación o gestión de la BDNTS, ni facultades para determinar las autoridades habilitadas para consultar la información, las finalidades de acceso o los requisitos jurídicos para obtenerla, materias que deben sujetarse al marco legal aplicable y a las competencias de las autoridades correspondientes.

Finalmente, convendría considerar la articulación entre las competencias de la Superintendencia de Industria y Comercio, las autoridades encargadas de la investigación de conductas delictivas y la entidad responsable de la BDNTS. Esta coordinación facilitaría la gestión y protección de la información, así como el seguimiento de las obligaciones previstas en el Proyecto, respetando las funciones legalmente asignadas a cada entidad.

2.3. Estructura de la BDNTS — artículo 5

Módulo 5.1: Se recomienda desarrollar con mayor detalle la forma en que operará el proceso de identificación y validación de los usuarios. En particular, resulta necesario precisar aspectos esenciales relacionados con el tratamiento de los datos biométricos, tales como las condiciones de captura, procesamiento, almacenamiento, conservación, acceso, obligatoriedad y eventual eliminación de la información recolectada.

También, se recomienda aclarar el alcance y la interacción de los literales c) y d), en tanto no resulta claro cómo se articulan con el proceso de identificación del usuario ni cuáles son los efectos jurídicos y operativos derivados de cada uno de ellos. Una redacción más precisa permitiría determinar si se trata de mecanismos complementarios, alternativos o sucesivos de validación.

Módulo 5.4: Se sugiere revisar el esquema de interoperabilidad propuesto, toda vez que no define con suficiente claridad las entidades que podrán acceder a la información, los niveles de acceso que tendrá cada una, los fines específicos de las consultas ni los mecanismos de control.

Asimismo, la propuesta no delimita adecuadamente las responsabilidades de los distintos actores que participarían en el intercambio de información ni el detalle de la operación. En consecuencia, se recomienda definir expresamente la entidad responsable de la administración del esquema, los protocolos de intercambio de información y los mecanismos de supervisión.

Frente al parágrafo 2, se recomienda examinar si la prohibición de adquisición de tarjetas SIM por menores de edad introduce una restricción adicional necesaria frente a las reglas de capacidad previstas en el Código Civil. Para ello, resulta importante distinguir entre la adquisición de la tarjeta, la contratación del servicio, la activación de la línea y su uso efectivo. La prohibición de adquisición no impide que un menor utilice una línea registrada por su representante legal ni garantiza, por sí sola, una mayor trazabilidad. En consecuencia, se sugiere precisar las condiciones de contratación, identificación y registro cuando intervengan menores de edad, así como el alcance de la responsabilidad que podría corresponder a sus representantes legales, conforme al régimen civil y demás disposiciones aplicables, sin que la sola titularidad de la línea permita atribuirles automáticamente responsabilidad por las conductas realizadas mediante ella.

En ese sentido, se recomienda armonizar la disposición con las normas civiles y penales establecidas en el ordenamiento jurídico colombiano.

2.4. Responsabilidad única del titular de la línea — artículo 6

La identificación del titular acredita una relación de registro con la línea, pero no demuestra la autoría de las conductas realizadas mediante ella. Convertir esa asociación en responsabilidad exclusiva podría trasladar al usuario riesgos de suplantación, pérdida o fraude en la activación y, simultáneamente, debilitar los incentivos de los proveedores para prevenir dichas situaciones. En consecuencia, se recomienda revisar esta disposición de manera que la información de la BDNTS contribuya a la individualización e investigación de posibles conductas delictivas, sin sustituir las reglas ordinarias de prueba, imputación, debido proceso y responsabilidad personal.

2.5. Responsabilidad del Proveedor de la Red de Telecomunicaciones — artículo 7

Frente al literal c) del artículo 7, convendría establecer en la ley la obligación general de mantener actualizada la información registrada y reservar al desarrollo reglamentario los aspectos operativos de su cumplimiento, como los eventos que exigen actualización, los plazos, los canales disponibles y los mecanismos de verificación. Esta distribución permitiría preservar la obligación legal y adaptar sus procedimientos a la evolución tecnológica.

2.6. Prohibición del uso y comercialización de Tarjetas SIM, física o virtual — artículo 9

La comercialización de una SIM, la activación de la línea y el uso del servicio son actividades distintas que pueden involucrar responsables diferentes. La obligación de verificar la identidad antes de la activación debería recaer principalmente en el proveedor que controla técnicamente ese proceso, sin perjuicio de las obligaciones propias de los comercializadores. Esta distinción cobra especial importancia frente a las eSIM, cuya provisión puede efectuarse remotamente, sin entrega de una tarjeta física. Por ello, la regulación debería diferenciar las obligaciones asociadas a la comercialización de aquellas vinculadas a la activación efectiva del servicio.

2.7. Costos de Infraestructura — artículo 5 y 10

El numeral 5.5 y el artículo 10 deberían analizarse conjuntamente, pues la implementación de la BDNTS supone inversiones tanto en la infraestructura común como en los sistemas de los proveedores y las entidades que deban interactuar con ella. Sin embargo, la exposición de motivos no presenta estimaciones de los costos de desarrollo, integración, almacenamiento, procesamiento de consultas, seguridad, operación y mantenimiento del sistema, ni distingue las inversiones que ya exige el régimen vigente de aquellas que generaría el nuevo esquema. Esta diferenciación resulta importante para determinar el costo incremental de la intervención y valorar su viabilidad económica.

Desde una perspectiva de eficiencia, la distribución de estos costos debería responder a criterios de causación y control. Para esa distribución, convendría que cada actor asumiera los costos de las adecuaciones, sistemas e interfaces bajo su administración, mientras que la infraestructura común requeriría una regla específica de financiación y asignación de responsabilidades. Esta distinción permitiría alinear los costos con las decisiones que los generan y los incentivos para gestionarlos. Adicionalmente, convendría considerar las diferencias de escala y modelo de operación entre proveedores, pues las inversiones fijas de cumplimiento pueden representar una carga proporcionalmente mayor para los operadores de menor tamaño y, dependiendo de su magnitud, elevar las barreras de entrada o expansión. En consecuencia, la evaluación económica debería considerar no solo el costo agregado del sistema, sino también su distribución y los posibles efectos sobre la competencia.

Finalmente, convendría precisar la afirmación de la exposición de motivos sobre la ausencia de impacto fiscal, dado que el Proyecto contempla obligaciones de infraestructura para entidades públicas cuya implementación podría requerir recursos de adecuación tecnológica, integración, seguridad y operación. Si bien estas obligaciones no implican necesariamente nuevas apropiaciones presupuestales, resulta pertinente establecer si pueden atenderse con los recursos existentes o si requieren financiación adicional. Esta evaluación permitiría distinguir los eventuales costos para las entidades públicas de las cargas regulatorias impuestas a los proveedores, identificar sus fuentes de financiación y valorar la sostenibilidad económica del sistema.

2.8. Sanciones, vigilancia y control — artículos 11 y 12

Se recomienda precisar la distribución de competencias entre las autoridades involucradas en la supervisión y aplicación del régimen propuesto, distinguiendo las funciones de regulación técnica, protección de datos personales e inspección, vigilancia y control. La coordinación necesaria para

implementar la BDNTS debería desarrollarse dentro de las atribuciones legalmente asignadas a cada entidad, sin que implique su ampliación o modificación. En materia sancionatoria, convendría delimitar las conductas constitutivas de infracción, los sujetos obligados y las autoridades competentes para conocer de su incumplimiento, de manera que las responsabilidades y consecuencias jurídicas sean previsibles.

Asimismo, la responsabilidad por los incumplimientos debería corresponder a las obligaciones y actuaciones que cada sujeto tenga capacidad efectiva de controlar. Así, los puntos de venta podrían responder por las verificaciones y procedimientos de comercialización a su cargo, pero no por fallas de disponibilidad de la BDNTS, errores de activación imputables al proveedor o deficiencias de sistemas ajenos a su administración, sin perjuicio de la responsabilidad derivada de sus propias actuaciones. Esta delimitación permitiría que cada actor responda por obligaciones que está en capacidad de cumplir, fortaleciendo los incentivos de prevención sin trasladar responsabilidades por fallas ajenas a su control

2.9. Implementación y régimen de transición

La entrada en operación de la BDNTS requiere una transición que permita depurar y conciliar los registros existentes, probar la interoperabilidad y seguridad del sistema y establecer mecanismos de contingencia y corrección de información. Estas etapas deberían contemplar la migración y deduplicación de registros, así como garantías para evitar suspensiones indebidas del servicio por inconsistencias históricas. Por esto, el inicio de las obligaciones que dependan de la plataforma debería sujetarse a condiciones verificables de funcionamiento y no únicamente al vencimiento de un plazo legal.

3. Consideraciones finales

La CRC comparte el objetivo de fortalecer la seguridad de los usuarios de los servicios de telecomunicaciones y de apoyar las capacidades institucionales para la prevención, investigación y judicialización de conductas delictivas asociadas al uso de líneas y servicios móviles. Asimismo, reconoce la importancia de adoptar medidas que contribuyan a combatir fenómenos como la extorsión, el secuestro, la suplantación de identidad y otras modalidades delictivas que afectan de manera significativa a la ciudadanía.

La relevancia del objetivo perseguido no sustituye la necesidad de establecer qué falla concreta permanece sin resolver, cuál es su magnitud y qué resultado adicional se espera alcanzar mediante la creación de la BDNTS y la utilización de mecanismos biométricos. Esa identificación permitiría valorar las distintas alternativas técnicas y regulatorias, evitando que la incorporación de nuevas obligaciones se traduzca en mayores costos o cargas sin una mejora verificable de la seguridad y trazabilidad de los usuarios.

En este contexto, la CRC considera conveniente fortalecer el Proyecto a partir de tres criterios: **(i)** asignar las responsabilidades y los costos al actor con capacidad efectiva para gestionar cada riesgo; **(ii)** preservar la distribución legal de competencias, especialmente el carácter técnico y operativo de la intervención regulatoria; y **(iii)** evaluar las alternativas de arquitectura,

autenticación e implementación bajo criterios de proporcionalidad, seguridad y eficiencia económica. Estas precisiones permitirían avanzar hacia un esquema normativo más claro, verificable y sostenible.

En estos términos, la CRC reitera su disposición para brindar el acompañamiento técnico necesario durante el trámite legislativo del proyecto de ley de la referencia y contribuir a la construcción de un marco normativo que fortalezca la seguridad de los usuarios, proteja los datos personales y preserve la eficiencia regulatoria del sector de comunicaciones.

Cordial saludo,
DÍAZ SUAZA

FELIPE

AUGUSTO

FELIPE AUGUSTO DÍAZ SUAZA

Director Ejecutivo

Firmado digitalmente por
DÍAZ SUAZA FELIPE
AUGUSTO
Fecha: 2026.10.15 11:09:30
-05'00'

Proyectado por: Laura Vanessa Sánchez

Revisado por: Víctor Baldrich

Aprobado por: Zoila Vargas



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