



GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XXXV - N° 1504

Bogotá, D. C., jueves, 8 de octubre de 2026

EDICIÓN DE 18 PÁGINAS

DIRECTORES:

DIEGO ALEJANDRO GONZÁLEZ GONZÁLEZ
SECRETARIO GENERAL DEL SENADO
www.secretariasenado.gov.co

MIGUEL ÁNGEL SÁNCHEZ VÁSQUEZ
SECRETARIO GENERAL DE LA CÁMARA
www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

CÁMARA DE REPRESENTANTES

PROYECTOS DE LEY

PROYECTO DE LEY NÚMERO 416 DE 2026 CÁMARA

por medio de la cual se establecen medidas para garantizar la identificación de los titulares de las líneas móviles, la autenticidad y trazabilidad de las comunicaciones cursadas a través de redes públicas de telecomunicaciones móviles, se adoptan mecanismos para prevenir el fraude y otros usos ilícitos de estos servicios, y se dictan otras disposiciones. - Ley No Más Extorsión y Suplantación Telefónica.

Bogotá, D. C., 30 de septiembre de 2026

Señor,

MIGUEL ÁNGEL SÁNCHEZ

Secretario General

Cámara de Representantes

E. S. D.

Asunto: Radicación Proyecto de Ley número 416 de 2026 Cámara, *por medio de la cual se establecen medidas para garantizar la identificación de los titulares de las líneas móviles, la autenticidad y trazabilidad de las comunicaciones cursadas a través de redes públicas de telecomunicaciones móviles, se adoptan mecanismos para prevenir el fraude y otros usos ilícitos de estos servicios, y se dictan otras disposiciones. - Ley No Más Extorsión y Suplantación Telefónica.*

Respetado Secretario, cordial saludo.

En nuestra calidad de Congresistas de la República, y en uso del derecho consagrado en el artículo 150 Constitucional y de los artículos 139 y 140 de la Ley 5ª de 1992, por su digno conducto nos permitimos poner a consideración de la Honorable Cámara de Representantes el siguiente Proyecto de Ley número

416 de 2026 Cámara, *por medio de la cual se establecen medidas para garantizar la identificación de los titulares de las líneas móviles, la autenticidad y trazabilidad de las comunicaciones cursadas a través de redes públicas de telecomunicaciones móviles, se adoptan mecanismos para prevenir el fraude y otros usos ilícitos de estos servicios, y se dictan otras disposiciones. - Ley No Más Extorsión y Suplantación Telefónica.*

De los Honorables Congresistas,

DARWIN CASTELLANOS ROMERO
Representante a la Cámara por el Departamento del Meta
Partido Centro Democrático

MATED HIBALGO MONTÓYA
Representante a la Cámara por Caldas
Partido Centro Democrático

ANA LIGIA MORA MARTÍNEZ
Representante a la Cámara por Antioquia
Partido Centro Democrático

PROYECTO DE LEY NÚMERO 416 DE 2026
CÁMARA

por medio de la cual se establecen medidas para garantizar la identificación de los titulares de las líneas móviles, la autenticidad y trazabilidad de las comunicaciones cursadas a través de redes públicas de telecomunicaciones móviles, se adoptan mecanismos para prevenir el fraude y otros usos ilícitos de estos servicios, y se dictan otras disposiciones. - Ley No Más Extorsión y Suplantación Telefónica.

El Congreso de Colombia

DECRETA:

CAPÍTULO I

Disposiciones generales

Artículo 1º. Objeto. La presente ley tiene por objeto regular la adquisición, activación, registro, administración, portabilidad y uso de las líneas móviles asociadas a tarjetas SIM, eSIM y demás tecnologías equivalentes; garantizar la plena identificación de sus titulares; establecer mecanismos que aseguren la autenticidad, trazabilidad y confiabilidad de las comunicaciones realizadas a través de redes públicas de telecomunicaciones móviles; fortalecer la protección de los usuarios; y adoptar medidas para prevenir la extorsión, la suplantación de identidad, el fraude y demás conductas ilícitas cometidas mediante la utilización de estos servicios.

Artículo 2º. Ámbito de aplicación. Las disposiciones de la presente ley serán aplicables a los proveedores de redes y servicios de telecomunicaciones móviles, incluidos los operadores móviles virtuales; a los distribuidores y comercializadores autorizados de tarjetas SIM, eSIM y demás tecnologías equivalentes; a las personas naturales y jurídicas titulares de líneas móviles; a quienes utilicen recursos de identificación para originar llamadas, mensajes de texto u otras comunicaciones a través de redes públicas de telecomunicaciones móviles; y a las entidades públicas que ejerzan funciones de regulación, inspección, vigilancia, control, investigación o protección de datos personales en esta materia.

CAPÍTULO II

Titularidad, registro y activación de líneas móviles

Artículo 3º. Identificación obligatoria del titular. Toda línea móvil deberá encontrarse registrada a nombre de una persona natural o jurídica plenamente identificada. Ninguna tarjeta SIM, eSIM o tecnología equivalente podrá ser activada para la prestación de servicios de telecomunicaciones móviles sin que previamente se haya verificado la identidad de quien figurará como titular del servicio.

Artículo 4º. Verificación de identidad. La verificación de la identidad del titular se realizará mediante la validación del documento

de identificación correspondiente, la consulta de las bases de datos oficiales habilitadas para tal fin y, cuando las condiciones técnicas lo permitan, mediante mecanismos de autenticación biométrica u otros sistemas que ofrezcan un nivel equivalente de seguridad y confiabilidad. El Gobierno nacional reglamentará los estándares técnicos y operativos necesarios para la implementación de estos mecanismos en un periodo no superior a los seis (6) meses desde la entrada en vigencia de la presente ley.

Artículo 5º. Comercialización y activación de líneas móviles. Las tarjetas SIM, eSIM y demás tecnologías equivalentes únicamente podrán comercializarse en estado inactivo. Su activación corresponderá exclusivamente al proveedor de redes y servicios de telecomunicaciones móviles o al operador móvil virtual, una vez se haya surtido el procedimiento de identificación, verificación y vinculación a una persona natural o jurídica previsto en la presente ley.

Artículo 6º. Registro de personas jurídicas. Cuando el titular de una línea móvil sea una persona jurídica, esta deberá registrar la identificación de la entidad y de la persona natural responsable del uso de cada línea asignada, sin perjuicio de la responsabilidad que le corresponda por el uso de las líneas registradas a su nombre.

Artículo 7º. Cambio de titularidad. Todo cambio de titular de una línea móvil requerirá el cumplimiento del mismo procedimiento de identificación y verificación exigido para su activación inicial. Ningún proveedor podrá modificar la titularidad de una línea sin la autorización expresa del titular registrado y del nuevo titular, salvo disposición legal o judicial en contrario.

Artículo 8º. Reposición, duplicados y portabilidad. La reposición o expedición de duplicados de tarjetas SIM o eSIM y los procesos de portabilidad numérica solo podrán realizarse previa verificación de la identidad del titular, de conformidad con los procedimientos establecidos por el Gobierno nacional y la regulación expedida por la Comisión de Regulación de Comunicaciones.

Artículo 9º. Límite de líneas móviles. Ninguna persona natural podrá mantener registradas más de dos (2) líneas móviles en cualquier modalidad con un mismo proveedor de redes y servicios de telecomunicaciones móviles. La activación de una nueva línea requerirá la cancelación o transferencia previa de una de las líneas existentes.

Artículo 10. Líneas destinadas a comunicaciones máquina a máquina. El Gobierno nacional podrá establecer un procedimiento especial para el registro y administración de las líneas destinadas exclusivamente a servicios de comunicación máquina a máquina (M2M), Internet de las Cosas (IoT) u otras tecnologías equivalentes, siempre que ello no comprometa la identificación del responsable del servicio contratado.

CAPÍTULO III

Registro Único de Usuarios de Telefonía Móvil

Artículo 11. Creación del Registro Único de Usuarios de Telefonía Móvil. Créase el Registro Único de Usuarios de Telefonía Móvil (RUUTM), administrado por el Ministerio de Tecnologías de la Información y las Comunicaciones, como un sistema nacional destinado a consolidar la información de identificación de los titulares de las líneas móviles activas en el territorio nacional, garantizar la trazabilidad de su activación, modificación, portabilidad, suspensión y cancelación, y facilitar las actuaciones de las autoridades competentes en los términos previstos por la Constitución y la ley.

Artículo 12. Información del Registro Único de Usuarios de Telefonía Móvil. Los proveedores de redes y servicios de telecomunicaciones móviles y los operadores móviles virtuales deberán reportar y mantener permanentemente actualizada la información correspondiente a cada línea activa. El registro contendrá, como mínimo, la identificación del titular, el número de la línea, el operador responsable, el identificador de la tarjeta SIM o eSIM, el IMEI registrado al momento de la activación cuando resulte técnicamente procedente, las fechas de activación, suspensión, reposición, portabilidad, cambio de titularidad y cancelación, así como el historial de las modificaciones realizadas sobre cada línea. El Gobierno nacional podrá definir información adicional cuando resulte necesaria para el cumplimiento de los fines de la presente ley.

Artículo 13. Acceso al Registro Único de Usuarios de Telefonía Móvil. La información contenida en el Registro Único de Usuarios de Telefonía Móvil tendrá carácter reservado y solo podrá ser consultada por las autoridades judiciales y por las demás autoridades competentes, en los casos y bajo los procedimientos previstos en la Constitución Política y la ley.

Artículo 14. Protección de la información. El tratamiento de la información incorporada al Registro Único de Usuarios de Telefonía Móvil se sujetará a las disposiciones sobre protección de datos personales y *habeas data*. El Ministerio de Tecnologías de la Información y las Comunicaciones, los proveedores de redes y servicios de telecomunicaciones móviles y los operadores móviles virtuales deberán adoptar las medidas técnicas, administrativas y de seguridad necesarias para garantizar su confidencialidad, integridad, disponibilidad y trazabilidad, quedando prohibido su uso para fines distintos de los expresamente autorizados por la ley.

CAPÍTULO IV

Autenticidad de las comunicaciones móviles

Artículo 15. Identificación de las comunicaciones empresariales e institucionales. Toda llamada o mensaje de texto originado por una entidad pública, una entidad financiera, un proveedor de servicios públicos domiciliarios, una institución prestadora de servicios de salud, una empresa de mensajería

o transporte, un proveedor de redes y servicios de telecomunicaciones, una aseguradora o cualquier otra persona jurídica que realice comunicaciones masivas con fines comerciales, informativos, transaccionales o de atención al usuario deberá identificar de manera clara, visible y verificable la identidad de su remitente, en los términos establecidos por la presente ley y la regulación que expida la Comisión de Regulación de Comunicaciones.

Artículo 16. Identificadores autorizados para comunicaciones empresariales. Las personas jurídicas únicamente podrán originar comunicaciones masivas mediante los recursos de identificación asignados, autorizados o habilitados conforme a la regulación expedida por la Comisión de Regulación de Comunicaciones. En ningún caso podrán utilizar números móviles destinados al uso personal para el envío masivo de mensajes de texto o para la realización de llamadas automatizadas o masivas.

Artículo 17. Identificación de mensajes de texto. Los mensajes de texto enviados por personas jurídicas deberán originarse desde códigos cortos, identificadores alfanuméricos, nombres comerciales verificados o cualquier otro mecanismo de identificación autorizado por la Comisión de Regulación de Comunicaciones, de manera que el destinatario pueda conocer claramente la identidad del remitente antes de acceder al contenido del mensaje.

Artículo 18. Identificación de llamadas empresariales. Toda llamada originada por una persona jurídica deberá mostrar al usuario receptor el nombre comercial, la marca o el identificador autorizado del remitente, conforme a las condiciones técnicas y operativas que establezca la Comisión de Regulación de Comunicaciones. Los proveedores de redes y servicios de telecomunicaciones móviles deberán implementar las medidas necesarias para garantizar la visualización de dicha información cuando ello sea técnicamente posible.

Artículo 19. Prohibición de la suplantación del identificador de origen. Se prohíbe la alteración, manipulación, falsificación, ocultamiento o utilización no autorizada de números telefónicos, códigos cortos, identificadores alfanuméricos, nombres comerciales o cualquier otro recurso destinado a identificar el origen de una comunicación. Los proveedores de redes y servicios de telecomunicaciones móviles deberán adoptar mecanismos para prevenir, detectar y bloquear este tipo de prácticas, de conformidad con la reglamentación vigente.

Artículo 20. Registro de identificadores. La Comisión de Regulación de Comunicaciones establecerá y administrará el registro de los recursos de identificación utilizados para llamadas y mensajes empresariales, así como las condiciones para su asignación, modificación, suspensión, cancelación y recuperación, garantizando su trazabilidad y uso exclusivo por parte de sus titulares autorizados.

Artículo 21. Conservación de registros. Los proveedores de redes y servicios de telecomunicaciones móviles conservarán los registros relacionados con la asignación, activación, utilización, modificación y cancelación de los recursos de identificación utilizados para llamadas y mensajes empresariales durante el término que establezca la ley o la regulación aplicable, con el fin de facilitar las actuaciones de las autoridades competentes.

CAPÍTULO V

Regularización de líneas móviles y actualización del registro

Artículo 22. Regularización de líneas activas. Los proveedores de redes y servicios de telecomunicaciones móviles y los operadores móviles virtuales dispondrán de un plazo máximo de doce (12) meses, contados a partir de la entrada en vigencia de la presente ley, para verificar y actualizar la información correspondiente a las líneas móviles activas que no cumplan las condiciones de identificación previstas en esta ley. El Gobierno nacional podrá prorrogar dicho plazo, por una sola vez, hasta por seis (6) meses cuando existan razones técnicas u operativas debidamente justificadas.

Artículo 23. Depuración periódica del registro de líneas móviles. Los proveedores de redes y servicios de telecomunicaciones móviles y los operadores móviles virtuales deberán realizar, como mínimo cada seis (6) meses, procesos de depuración y verificación de la información correspondiente a las líneas móviles activas, con el fin de garantizar que la información registrada en el Registro Único de Usuarios de Telefonía Móvil se encuentre completa, actualizada y corresponda al titular real de cada línea.

Cuando durante dichos procesos se identifiquen líneas cuya información no pueda ser validada o se encuentre incompleta, inconsistente o desactualizada, el operador deberá requerir al titular para que regularice su situación dentro del término máximo de un (1) mes contado a partir de la comunicación correspondiente.

La Comisión de Regulación de Comunicaciones (CRC) establecerá las condiciones técnicas, los medios de comunicación, el contenido de los requerimientos y los procedimientos que deberán seguir los operadores para informar a los usuarios sobre la obligación de actualizar su información y las consecuencias derivadas de su incumplimiento.

Artículo 24. Suspensión y cancelación de líneas no regularizadas. Vencido el término previsto en el artículo anterior sin que el titular hubiere regularizado su situación, el proveedor suspenderá la prestación del servicio.

Si transcurridos dos (2) meses contados a partir de la suspensión el titular no hubiere actualizado la información correspondiente, el operador cancelará la línea y procederá a su reasignación de conformidad con el Plan Nacional de Numeración y la regulación

expedida por la Comisión de Regulación de Comunicaciones.

Artículo 25. Actualización permanente de la información. Los titulares de líneas móviles deberán informar oportunamente cualquier modificación de los datos suministrados para el registro de la línea. Los proveedores de redes y servicios de telecomunicaciones móviles establecerán mecanismos que permitan mantener actualizada la información registrada y verificar periódicamente su consistencia.

Artículo 26. Portabilidad numérica. Todo proceso de portabilidad numérica requerirá la verificación de la identidad del titular conforme a las disposiciones previstas en la presente ley, sin perjuicio del cumplimiento de los demás requisitos establecidos en la regulación vigente.

Artículo 27. Cancelación voluntaria de líneas móviles. Los proveedores de redes y servicios de telecomunicaciones móviles deberán garantizar procedimientos ágiles, seguros y gratuitos para la cancelación voluntaria de líneas móviles por parte de sus titulares, verificando previamente su identidad y actualizando inmediatamente la información correspondiente en el Registro Único de Usuarios de Telefonía Móvil.

CAPÍTULO VI

Prevención de la extorsión, la suplantación y el fraude en las comunicaciones móviles

Artículo 28. Deber de prevención. Los proveedores de redes y servicios de telecomunicaciones móviles y los operadores móviles virtuales deberán implementar medidas técnicas, operativas y administrativas destinadas a prevenir la utilización de sus redes y servicios para la comisión de delitos, en especial la extorsión, la suplantación de identidad, el fraude informático y las demás conductas ilícitas que puedan ejecutarse mediante llamadas, mensajes de texto u otros servicios de telecomunicaciones móviles.

Artículo 29. Detección de patrones de riesgo. Los proveedores de redes y servicios de telecomunicaciones móviles deberán implementar mecanismos tecnológicos para identificar patrones de tráfico que razonablemente puedan asociarse con actividades fraudulentas o delictivas, sin que ello implique la interceptación, monitoreo o acceso al contenido de las comunicaciones, salvo en los casos autorizados por la Constitución Política y la ley.

Artículo 30. Deber de reporte. Cuando los proveedores de redes y servicios de telecomunicaciones móviles detecten patrones de tráfico que razonablemente puedan estar asociados con la comisión de delitos, deberán informar oportunamente a las autoridades competentes mediante los canales que establezca el Gobierno nacional, preservando la cadena de custodia y la reserva de la información.

Artículo 31. Prevención de comunicaciones originadas desde establecimientos de reclusión.

El Gobierno nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Justicia y del Derecho y el Instituto Nacional Penitenciario y Carcelario (Inpec), adoptará e implementará mecanismos tecnológicos dirigidos a prevenir la utilización de servicios de telecomunicaciones móviles para la comisión de delitos desde los establecimientos de reclusión, incluyendo sistemas de bloqueo, inhibición, identificación, monitoreo técnico y demás herramientas compatibles con el ordenamiento jurídico.

Artículo 32. Cooperación institucional. El Ministerio de Tecnologías de la Información y las Comunicaciones, la Comisión de Regulación de Comunicaciones, la Superintendencia de Industria y Comercio, la Fiscalía General de la Nación, la Policía Nacional, el Instituto Nacional Penitenciario y Carcelario (Inpec) y las demás autoridades competentes coordinarán las acciones necesarias para la implementación y cumplimiento de la presente ley, de conformidad con las competencias asignadas por el ordenamiento jurídico.

CAPÍTULO VII

Disposiciones finales

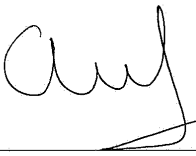
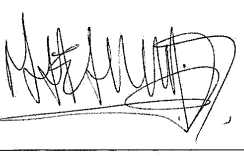
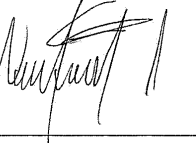
Artículo 33. Reglamentación. El Gobierno nacional reglamentará la presente ley dentro de los seis (6) meses siguientes a su promulgación. La Comisión de Regulación de Comunicaciones expedirá o ajustará la regulación necesaria para garantizar su implementación dentro del ámbito de sus competencias.

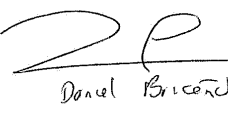
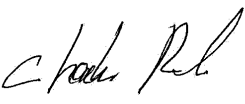
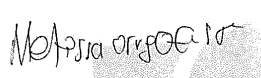
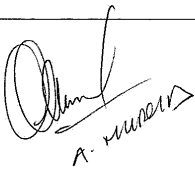
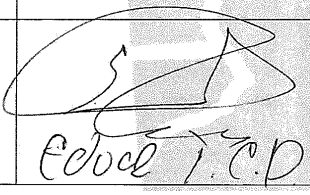
Artículo 34. Régimen de transición. Los proveedores de redes y servicios de telecomunicaciones móviles, los operadores móviles virtuales y los demás sujetos obligados dispondrán de un plazo máximo de doce (12) meses, contados a partir de la expedición de la reglamentación prevista en el artículo anterior, para adecuar sus procesos, plataformas tecnológicas y procedimientos internos a las obligaciones establecidas en la presente ley, sin perjuicio de los plazos especiales previstos para la regularización de líneas móviles activas.

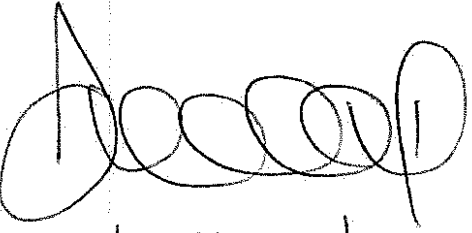
Artículo 35. Vigencia y derogatorias. La presente ley rige a partir de la fecha de su promulgación y deroga todas las disposiciones que le sean contrarias.

De los Honorables Congresistas,


DARWIN CASTELLANOS ROMERO
Representante a la Cámara por el Departamento del Meta
Partido Centro Democrático

	
	 Hilda Suárez

 Pinto	 Daniel Briceño
 C. Rodríguez	 Marta Ortega
 A. Muñoz	 Eduardo J.C.P.


Arledy Alvarado CD

EXPOSICIÓN DE MOTIVOS

1. OBJETO DEL PROYECTO DE LEY

El presente proyecto de ley tiene por objeto fortalecer el marco jurídico aplicable a las comunicaciones móviles en Colombia mediante la regulación de la adquisición, activación, registro, administración, portabilidad y uso de las líneas móviles asociadas a tarjetas SIM, eSIM y demás tecnologías equivalentes, garantizando la plena identificación de sus titulares, la autenticidad de las llamadas y mensajes de texto, así como la trazabilidad de las comunicaciones que se originan a través de las redes públicas de telecomunicaciones móviles.

Para alcanzar este propósito, la iniciativa establece mecanismos orientados a asegurar que toda línea móvil activa se encuentre asociada a un titular plenamente identificado, regular la identificación verificable de las comunicaciones originadas por entidades públicas y privadas, crear el Registro Único de Usuarios de Telefonía Móvil (RUUTM) y fortalecer las herramientas de prevención, investigación y judicialización de delitos como la extorsión, la suplantación de identidad, el fraude y demás conductas ilícitas cometidas mediante servicios de telecomunicaciones. Con ello se busca cerrar los vacíos normativos existentes, fortalecer la confianza de los ciudadanos en las comunicaciones móviles y garantizar que las medidas adoptadas se implementen con pleno respeto por los derechos fundamentales, el *habeas data* y la protección de los datos personales.

2. JUSTIFICACIÓN DEL PROYECTO DE LEY

La telefonía móvil se ha consolidado como uno de los principales medios de comunicación

entre los ciudadanos, las empresas y el Estado. Actualmente, millones de colombianos utilizan diariamente llamadas telefónicas, mensajes de texto y demás servicios móviles para realizar operaciones bancarias, acceder a servicios públicos y privados, recibir información oficial, efectuar transacciones comerciales y mantener comunicaciones personales y laborales. Como consecuencia de esta transformación tecnológica, las redes públicas de telecomunicaciones móviles se han convertido en una infraestructura esencial para el desarrollo económico, social e institucional del país.

Sin embargo, el crecimiento exponencial de estos servicios también ha sido aprovechado por organizaciones criminales y delinquentes para desarrollar nuevas modalidades de extorsión, fraude, suplantación de identidad, estafa y otros delitos que tienen como principal instrumento las comunicaciones móviles. En la actualidad, un número importante de estas conductas se ejecutan mediante llamadas telefónicas y mensajes de texto enviados desde líneas cuya titularidad no puede establecerse con certeza o cuya identidad de origen es manipulada para generar confianza en las víctimas.

El problema no radica exclusivamente en la utilización de líneas móviles registradas con información falsa o desactualizada. También obedece a la ausencia de mecanismos que permitan al ciudadano identificar con certeza quién origina una llamada o un mensaje de texto, situación que facilita la suplantación de entidades financieras, empresas de mensajería, operadores de telecomunicaciones, entidades públicas y demás organizaciones cuyos nombres son utilizados indebidamente para engañar a los usuarios.

En este contexto, el ordenamiento jurídico colombiano ha desarrollado diferentes instrumentos dirigidos a regular la prestación de los servicios de telecomunicaciones y fortalecer la seguridad de las redes. No obstante, la regulación vigente continúa concentrándose principalmente en aspectos relacionados con la prestación del servicio, la administración del espectro radioeléctrico, la protección de los usuarios y la asignación de recursos de numeración, sin establecer un sistema integral que garantice simultáneamente la identificación plena de los titulares de las líneas móviles y la autenticidad verificable de las comunicaciones que circulan por dichas redes.

La presente iniciativa legislativa busca llenar ese vacío normativo mediante un conjunto articulado de medidas que fortalecen la identificación de los usuarios, crean herramientas para mejorar la trazabilidad de las líneas móviles, regulan la autenticidad de las comunicaciones empresariales e institucionales y dotan a las autoridades de mayores capacidades para prevenir, investigar y judicializar los delitos cometidos mediante estos servicios, garantizando al mismo tiempo la protección de los datos personales y el respeto por los derechos fundamentales.

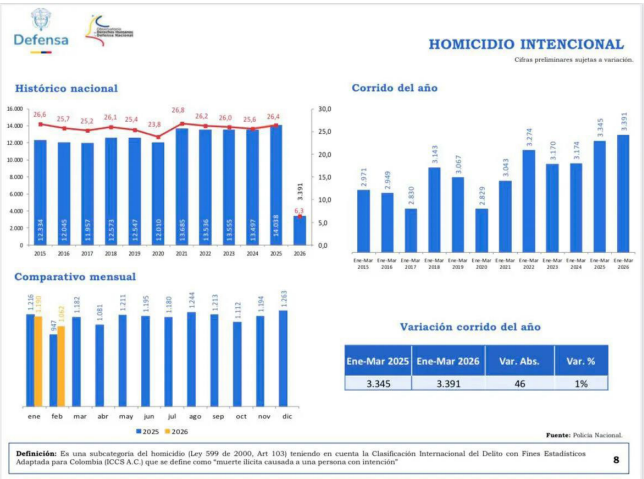
Con fundamento en estas consideraciones, el presente capítulo desarrolla las principales razones que justifican la adopción de la iniciativa, analizando la evolución de la extorsión telefónica, la suplantación de identidad y el fraude digital en Colombia; la necesidad de fortalecer la autenticidad de las comunicaciones móviles; las experiencias regulatorias implementadas en otras jurisdicciones; y el marco constitucional y legal que sustenta la competencia del legislador para adoptar las medidas previstas en el proyecto de ley.

2.1. La problemática de la extorsión telefónica, la suplantación de identidad y el fraude digital en Colombia.

Durante los últimos años, Colombia ha experimentado un incremento sostenido de los delitos que utilizan las redes públicas de telecomunicaciones móviles como principal medio para su comisión. La masificación del acceso a la telefonía móvil, el crecimiento de los canales digitales y la facilidad con la que actualmente pueden adquirirse y utilizarse líneas telefónicas sin mecanismos robustos de identificación de sus titulares han sido aprovechados por organizaciones criminales para desarrollar nuevas modalidades de extorsión, fraude, estafa y suplantación de identidad que afectan diariamente a miles de ciudadanos.

La extorsión constituye hoy una de las principales amenazas contra la seguridad ciudadana. De acuerdo con cifras oficiales del Ministerio de Defensa Nacional, durante el primer trimestre de 2026 se registraron 2.914 casos de extorsión, la cifra más alta para ese período desde 2015, lo que confirma una tendencia creciente de este delito y evidencia la necesidad de fortalecer las herramientas normativas dirigidas a combatirlo¹.

Figura 1. Evolución de los delitos de homicidio intencional y extorsión en Colombia (primer trimestre 2025-2026).



Fuente: Ministerio de Defensa Nacional – Policía Nacional. Informe de Orden Público. Primer trimestre de 2026.

¹ Ministerio de Defensa Nacional. Informe de Orden Público. Primer trimestre de 2026. Cifras oficiales sobre la evolución del delito de extorsión en Colombia.

La preocupación institucional frente a este fenómeno también ha sido advertida por la Defensoría del Pueblo. En enero de 2024, esa entidad informó que las denuncias por extorsión pasaron de 8.188 casos en 2020 a 9.871 casos en 2023, lo que representa un incremento del 20,5 % en apenas cuatro años². Asimismo, señaló que este delito afecta de manera considerable la seguridad ciudadana y requiere una actuación articulada entre las diferentes entidades del Estado para implementar medidas efectivas que permitan prevenir su ocurrencia.

Uno de los principales focos de preocupación corresponde a la denominada extorsión carcelaria, modalidad mediante la cual personas privadas de la libertad realizan llamadas telefónicas y envían mensajes de texto utilizando teléfonos celulares y tarjetas SIM ingresadas ilegalmente a los establecimientos penitenciarios. Según la Defensoría del Pueblo, de los 125 establecimientos de reclusión del orden nacional administrados por el Inpec, únicamente 16 contaban con sistemas de inhibición de señal, de los cuales solamente seis se encontraban operando, además con tecnología 2.5G, claramente insuficiente frente a las tecnologías actuales de comunicación móvil.

La misma entidad advirtió la necesidad de fortalecer la coordinación entre el Ministerio de Justicia y del Derecho, el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Inpec y los operadores de telefonía móvil, con el propósito de modernizar los sistemas de inhibición de señal e implementar mecanismos que permitan identificar las llamadas realizadas desde establecimientos penitenciarios y carcelarios.

Las autoridades han evidenciado igualmente el alto grado de organización que han alcanzado estas estructuras criminales. En distintos operativos adelantados por la Policía Nacional y el Instituto Nacional Penitenciario y Carcelario se han incautado teléfonos celulares, tarjetas SIM, bases de datos de potenciales víctimas y registros sistemáticos de llamadas, demostrando que muchas de estas organizaciones operan bajo esquemas similares a centros de contacto (*call centers*) clandestinos. De acuerdo con información oficial divulgada por la Policía Nacional, desde un solo teléfono celular pueden llegar a realizarse hasta 250 llamadas extorsivas en un día, mientras que estas redes criminales movilizan aproximadamente \$2.000 millones de pesos anuales producto de esta actividad ilícita³.

² Defensoría del Pueblo. Extorsión en Colombia preocupa a la Defensoría del Pueblo, pues creció el 20,5% en los últimos cuatro años. Comunicado 483, 16 de enero de 2024.

³ Policía Nacional – Dirección Antisecuestro y Antiextorsión (GAULA), información oficial divulgada sobre operativos contra redes de extorsión carcelaria, reproducida por *Infobae Colombia*, “Redes de extorsión desde cárceles mueven \$2.000 millones al año en Colombia”, 27 de junio de 2025.

No obstante, la problemática trasciende la extorsión tradicional. Actualmente los delincuentes recurren cada vez con mayor frecuencia a mecanismos de suplantación de identidad, mediante los cuales hacen creer a las víctimas que las llamadas o mensajes provienen de entidades financieras, operadores de telecomunicaciones, empresas de mensajería, entidades públicas, autoridades judiciales o incluso familiares, incrementando la credibilidad del engaño y aumentando significativamente la probabilidad de éxito de la conducta criminal.

A esta situación se suma el crecimiento sostenido del fraude digital. De acuerdo con cifras de Asobancaria, durante 2023 fueron reportados cerca de 407.000 casos de fraude a través de canales digitales, con pérdidas superiores a \$500.000 millones de pesos, lo que evidencia que las comunicaciones electrónicas se han convertido en uno de los principales vectores utilizados por las organizaciones criminales para afectar el patrimonio de los ciudadanos y del sistema financiero⁴.

Las circunstancias descritas demuestran que el principal desafío ya no consiste únicamente en controlar la comercialización de tarjetas SIM, sino en garantizar la autenticidad de las comunicaciones móviles y la identificación cierta de quienes las originan. La posibilidad de adquirir líneas telefónicas utilizando información falsa o desactualizada, la utilización de mecanismos de ocultamiento o manipulación de la identidad del remitente y la ausencia de sistemas que permitan al ciudadano reconocer fácilmente cuándo una llamada o un mensaje proviene realmente de una entidad legítima han generado un escenario que facilita la comisión de múltiples conductas delictivas.

En consecuencia, resulta necesario adoptar un marco normativo integral que fortalezca la identificación de los titulares de las líneas móviles, garantice la autenticidad de las llamadas y mensajes de texto, incremente la trazabilidad de las comunicaciones y proporcione a las autoridades herramientas más eficaces para prevenir, investigar y judicializar la extorsión, la suplantación de identidad, el fraude y demás delitos que utilizan las redes públicas de telecomunicaciones móviles como instrumento para su comisión.

2.2. La necesidad de fortalecer la autenticidad de las comunicaciones móviles.

El incremento de la extorsión telefónica, la suplantación de identidad y las distintas modalidades de fraude digital ha puesto de manifiesto que los mecanismos tradicionales de regulación de los servicios de telecomunicaciones resultan insuficientes para responder a los desafíos actuales en materia de seguridad digital y protección de los usuarios. Aunque el ordenamiento jurídico colombiano establece obligaciones relacionadas con la prestación del servicio, la asignación de recursos de numeración y la protección de los datos

⁴ Asobancaria. *Informe sobre fraude bancario y cibernético en Colombia 2023*.

personales, no existe una regulación integral que garantice la autenticidad de las comunicaciones móviles ni que permita a los ciudadanos conocer con certeza quién es el verdadero originador de una llamada o un mensaje de texto.

En la actualidad, los usuarios reciben diariamente comunicaciones que aparentan provenir de entidades bancarias, operadores de telefonía móvil, empresas de mensajería, plataformas de comercio electrónico, entidades públicas o incluso de miembros de la Fuerza Pública. En muchos casos, estas comunicaciones son utilizadas para inducir a las víctimas a suministrar información confidencial, realizar consignaciones, compartir códigos de autenticación o efectuar otras actuaciones bajo la falsa creencia de estar interactuando con una entidad legítima. Esta circunstancia ha deteriorado progresivamente la confianza de los ciudadanos en los servicios de telecomunicaciones y ha convertido las llamadas y mensajes de texto en uno de los principales instrumentos utilizados para la comisión de actividades delictivas.

A esta problemática se suma la facilidad con la que actualmente pueden adquirirse, activarse y utilizarse líneas móviles sin que exista un sistema uniforme que garantice la identificación plena de sus titulares y la permanente actualización de dicha información. Aunque los operadores cuentan con mecanismos de registro de usuarios, la inexistencia de un modelo unificado de verificación, trazabilidad y depuración de la información dificulta la individualización de los responsables cuando las líneas son utilizadas para la comisión de delitos y facilita que estas permanezcan activas aun cuando sus datos sean incompletos, inconsistentes o no correspondan al verdadero usuario.

De igual manera, el desarrollo de nuevas tecnologías de comunicación ha incrementado la necesidad de fortalecer la autenticidad del origen de las comunicaciones. Hoy en día no basta con identificar al titular de una línea móvil; también resulta indispensable que los ciudadanos puedan reconocer de manera clara y verificable cuándo una llamada o un mensaje de texto proviene efectivamente de una entidad pública, una entidad financiera, un operador de telecomunicaciones, una empresa de mensajería o cualquier otra organización legítima. Ello constituye una herramienta fundamental para reducir las posibilidades de engaño, fortalecer la confianza de los usuarios y facilitar la identificación temprana de comunicaciones fraudulentas.

En este contexto, el presente proyecto de ley propone un modelo integral orientado a fortalecer la autenticidad y la trazabilidad de las comunicaciones móviles en Colombia. Para ello establece mecanismos dirigidos a garantizar la identificación plena de los titulares de las líneas móviles, regular los procedimientos para la adquisición, activación, portabilidad y actualización de tarjetas SIM y eSIM, crear el Registro Único de Usuarios de Telefonía Móvil (RUUTM), fortalecer la identificación de las comunicaciones empresariales e institucionales

y promover la utilización de mecanismos que permitan a los usuarios reconocer de forma clara y verificable el origen de las llamadas y mensajes de texto que reciben.

Estas medidas no tienen como finalidad restringir el acceso de los ciudadanos a los servicios de telecomunicaciones ni imponer cargas desproporcionadas a los operadores del sector. Por el contrario, buscan incrementar la seguridad jurídica y tecnológica del ecosistema de comunicaciones móviles, fortalecer la confianza de los usuarios, reducir los espacios de anonimato que hoy son aprovechados por las organizaciones criminales y dotar al Estado de herramientas más eficaces para prevenir, investigar y judicializar la extorsión, la suplantación de identidad, el fraude y demás conductas ilícitas cometidas mediante redes públicas de telecomunicaciones móviles, garantizando en todo momento el respeto por los derechos fundamentales, el *habeas data* y la protección de los datos personales.

2.3. Experiencias desde el derecho comparado

La problemática que aborda la presente iniciativa no es exclusiva de Colombia. En los últimos años, el crecimiento de la extorsión telefónica, la suplantación de identidad y las distintas modalidades de fraude digital ha llevado a que numerosos países revisen y fortalezcan sus marcos regulatorios en materia de telecomunicaciones, con el propósito de incrementar la seguridad de las comunicaciones, garantizar la identificación de los usuarios y devolver a los ciudadanos la confianza en las llamadas y mensajes de texto que reciben diariamente.

Aunque cada país ha diseñado soluciones acordes con su realidad institucional, tecnológica y normativa, existe un elemento común en todas estas experiencias: la seguridad de las comunicaciones ya no depende únicamente de identificar al titular de una línea telefónica, sino también de garantizar que quien realiza una llamada o envía un mensaje sea realmente quien dice ser. En otras palabras, la tendencia internacional ha evolucionado desde sistemas centrados exclusivamente en el registro de usuarios hacia modelos que fortalecen la autenticidad, la trazabilidad y la verificación del origen de las comunicaciones móviles.

Bajo ese contexto, diferentes países han desarrollado mecanismos regulatorios y tecnológicos encaminados a combatir el uso fraudulento de las redes de telecomunicaciones, fortalecer la confianza de los usuarios y facilitar la investigación de delitos cometidos mediante llamadas telefónicas y mensajes de texto. A continuación, se presentan algunas de las experiencias internacionales más relevantes sobre la materia.

2.3.1. Estados Unidos

Uno de los referentes más importantes es el caso de los Estados Unidos. Durante los últimos años, ese país enfrentó un crecimiento significativo de las llamadas fraudulentas realizadas mediante la técnica conocida como *caller ID spoofing*, consistente en

alterar el número telefónico que aparece en la pantalla del usuario para hacer creer que la llamada proviene de una entidad financiera, una autoridad pública, una empresa reconocida o incluso de un familiar. Esta modalidad fue ampliamente utilizada para cometer estafas, obtener información confidencial y realizar diferentes formas de fraude.

Como respuesta a esta problemática, la Federal Communications Commission (FCC) impulsó la implementación obligatoria del marco STIR/SHAKEN, un conjunto de estándares tecnológicos que permite autenticar el origen de las llamadas telefónicas y verificar que el número mostrado al usuario corresponde efectivamente al operador que origina la comunicación. Paralelamente, la FCC estableció obligaciones para que los operadores implementaran mecanismos permanentes de mitigación y bloqueo de llamadas ilegales, fortaleciendo la confianza de los usuarios y reduciendo el impacto de las comunicaciones fraudulentas⁵.

2.3.2. Singapur

Una problemática similar se presentó en Singapur, donde el incremento de campañas de fraude mediante mensajes de texto llevó a que delincuentes utilizaran el nombre de entidades bancarias, organismos públicos y empresas privadas para engañar a los ciudadanos mediante técnicas de *smishing*. Como consecuencia, muchas personas recibían mensajes aparentemente legítimos que realmente provenían de organizaciones criminales.

Con el fin de enfrentar esta situación, las autoridades implementaron el SMS Sender ID Registry (SSIR), un registro obligatorio administrado por la Singapore Network Information Centre (SGNIC), mediante el cual únicamente las entidades previamente verificadas pueden enviar mensajes utilizando nombres comerciales o identificadores alfanuméricos. Esta medida ha fortalecido la autenticidad de los mensajes de texto y ha reducido significativamente las posibilidades de suplantación de identidad a través de este medio⁶.

2.3.3. India

En India, el fortalecimiento de la seguridad de las comunicaciones móviles se desarrolló en dos frentes. Por una parte, se consolidaron mecanismos cada vez más robustos para verificar la identidad de los usuarios durante la activación de líneas telefónicas. Posteriormente, las autoridades identificaron la necesidad de controlar también las comunicaciones comerciales que diariamente reciben millones de usuarios.

⁵ Federal Communications Commission (FCC). *STIR/SHAKEN Call Authentication Framework*. Disponible en: <https://www.fcc.gov/call-authentication>

⁶ Infocomm Media Development Authority (IMDA) y Singapore Network Information Centre (SGNIC). *SMS Sender ID Registry (SSIR)*. Disponible en: <https://www.imda.gov.sg>

Como respuesta, la Telecom Regulatory Authority of India (TRAI) implementó la plataforma Distributed Ledger Technology (DLT), mediante la cual las empresas deben registrar previamente su identidad, los encabezados utilizados para el envío de mensajes y las campañas autorizadas. Este sistema ha permitido fortalecer la autenticidad de las comunicaciones empresariales y reducir considerablemente el envío de mensajes fraudulentos y comunicaciones masivas no autorizadas⁷.

2.3.4. Brasil

Brasil también ha desarrollado mecanismos orientados a recuperar la confianza de los ciudadanos frente a las llamadas telefónicas. La creciente utilización del nombre de entidades públicas y privadas para cometer fraudes motivó a la Agência Nacional de Telecomunicações (ANATEL) a promover el programa Origem Verificada.

Mediante este sistema, determinadas empresas previamente verificadas pueden aparecer identificadas con su nombre comercial durante la llamada, permitiendo que el usuario conozca quién realiza la comunicación antes de contestarla. Con ello se busca disminuir la suplantación de identidad, fortalecer la confianza de los consumidores y facilitar la diferenciación entre llamadas legítimas y comunicaciones fraudulentas⁸.

2.3.5. Reino Unido

En el Reino Unido, la preocupación por el incremento de las llamadas fraudulentas llevó a la Office of Communications (Ofcom) a fortalecer las obligaciones impuestas a los operadores de telecomunicaciones para detectar, bloquear y reducir las comunicaciones que utilizan números telefónicos falsificados o manipulados. Paralelamente, la autoridad regulatoria ha promovido la adopción de soluciones tecnológicas dirigidas a autenticar el origen de las llamadas y proteger a los consumidores frente a nuevas modalidades de fraude telefónico⁹.

2.3.6. Emiratos Árabes Unidos

Los Emiratos Árabes Unidos han orientado sus esfuerzos hacia el fortalecimiento de la identificación de los titulares de las líneas móviles desde el momento mismo de su adquisición. La normativa vigente exige la verificación de la identidad mediante documentos oficiales y autenticación biométrica para la activación de tarjetas SIM, además de establecer límites al número de líneas que pueden registrarse a nombre de una misma persona.

⁷ Telecom Regulatory Authority of India (TRAI). *Distributed Ledger Technology (DLT) Framework for Commercial Communications*. Disponible en: <https://www.trai.gov.in>

⁸ Agência Nacional de Telecomunicações (ANATEL). *Origem Verificada*. Disponible en: <https://www.gov.br/anatel>

⁹ Office of Communications (Ofcom). *Protecting customers from scam calls*. Disponible en: <https://www.ofcom.org.uk>

Estas medidas buscan reducir el uso de líneas telefónicas registradas con identidades falsas, fortalecer la trazabilidad de las comunicaciones y facilitar las labores de investigación de las autoridades frente a delitos como el fraude, la extorsión y otras formas de delincuencia organizada¹⁰.

Las experiencias anteriormente descritas evidencian que la comunidad internacional ha venido evolucionando hacia modelos regulatorios cada vez más robustos para fortalecer la autenticidad de las comunicaciones móviles. Más allá de exigir la identificación de los titulares de las líneas telefónicas, la tendencia actual consiste en implementar mecanismos que permitan verificar el origen de las llamadas y mensajes de texto, brindar mayor transparencia a las comunicaciones empresariales e institucionales y reducir las posibilidades de que las redes de telecomunicaciones sean utilizadas como instrumento para la comisión de delitos.

En ese contexto, el presente proyecto de ley recoge varias de estas buenas prácticas internacionales y las adapta al ordenamiento jurídico colombiano, procurando un equilibrio entre la protección de los usuarios, la prevención del delito y el respeto por los derechos fundamentales.

2.4. Marco Constitucional y legal

El presente proyecto de ley encuentra fundamento en diversos mandatos de la Constitución Política que atribuyen al Estado la responsabilidad de garantizar la seguridad de las personas, proteger sus derechos fundamentales y regular la prestación de los servicios públicos. En particular, los artículos 2º, 15, 75 y 365 establecen, respectivamente, los fines esenciales del Estado de proteger la vida, honra y bienes de los habitantes; garantizan el derecho fundamental a la intimidad y al *habeas data*; reconocen que el espectro electromagnético es un bien público sujeto a la gestión y control del Estado; y disponen que los servicios públicos son inherentes a la finalidad social del Estado, correspondiéndole asegurar su prestación eficiente en beneficio de todos los habitantes.

En desarrollo de estos mandatos constitucionales, el legislador ha venido consolidando un marco normativo orientado a regular progresivamente el sector de las telecomunicaciones. Uno de sus primeros antecedentes corresponde a la Ley 37 de 1993, mediante la cual se reguló la prestación del servicio de telefonía móvil celular en Colombia y se establecieron las bases jurídicas para el desarrollo de este servicio en el país. Posteriormente, el Decreto número 741 de 1993 desarrolló varios aspectos técnicos y operativos relacionados con su implementación.

Con la expedición de la Ley 1341 de 2009 se produjo una transformación integral del régimen de las Tecnologías de la Información y las

Comunicaciones, al establecer los principios que orientan el sector, definir las competencias de las autoridades encargadas de su regulación y fortalecer el marco aplicable a los proveedores de redes y servicios de telecomunicaciones. Posteriormente, la Ley 1978 de 2019 modernizó la institucionalidad del sector TIC, fortaleció el modelo regulatorio vigente y consolidó el esquema de supervisión y regulación de los servicios de telecomunicaciones, procurando una mayor eficiencia en su prestación y una mejor protección para los usuarios.

Paralelamente, el ordenamiento jurídico ha incorporado instrumentos dirigidos a fortalecer la seguridad de las comunicaciones y prevenir su utilización con fines ilícitos. En ese sentido, el Decreto 1630 de 2011 adoptó medidas para restringir la operación de equipos terminales móviles hurtados, mientras que la Ley 1908 de 2018 fortaleció la lucha contra las organizaciones criminales e incorporó disposiciones dirigidas a controlar las comunicaciones realizadas desde los establecimientos penitenciarios y carcelarios, ordenando la implementación de mecanismos que permitan identificar las llamadas originadas desde dichos centros de reclusión.

La regulación administrativa también ha evolucionado en esa misma dirección. La Comisión de Regulación de Comunicaciones (CRC), mediante la Resolución CRC 5050 de 2016, compiló el régimen regulatorio aplicable al sector e incorporó disposiciones relacionadas con la protección de los usuarios, la identificación de llamadas y otras obligaciones dirigidas a fortalecer la seguridad y transparencia en la prestación de los servicios de telecomunicaciones.

De otra parte, el tratamiento de la información personal derivado de las medidas previstas en esta iniciativa encuentra respaldo en las Leyes Estatutarias 1266 de 2008 y 1581 de 2012, las cuales desarrollan el derecho fundamental al *habeas data* y establecen los principios, derechos, deberes y garantías aplicables al tratamiento de datos personales. En consecuencia, cualquier mecanismo de identificación, autenticación o registro que se implemente en desarrollo de la presente ley deberá sujetarse estrictamente a los principios de legalidad, finalidad, necesidad, proporcionalidad, seguridad y confidencialidad previstos en dichas normas.

No obstante los importantes avances alcanzados por este marco normativo, la legislación colombiana aún carece de un sistema integral que articule la identificación plena de los titulares de las líneas móviles con mecanismos que permitan autenticar el origen de las llamadas y mensajes de texto, fortalecer la trazabilidad de las comunicaciones y reducir el uso de los servicios de telecomunicaciones para la comisión de delitos como la extorsión, la suplantación de identidad y el fraude digital.

En ese contexto, el presente proyecto de ley no sustituye el marco jurídico existente, sino que lo complementa y desarrolla. La iniciativa armoniza las

¹⁰ Telecommunications and Digital Government Regulatory Authority (TDRA). Normativa sobre registro de usuarios de telefonía móvil e identificación biométrica de titulares de líneas. Disponible en: <https://tdra.gov.ae>

normas vigentes en materia de telecomunicaciones, seguridad ciudadana y protección de datos personales, incorporando herramientas que responden a los desafíos actuales derivados de la evolución tecnológica y de las nuevas modalidades delictivas que utilizan las redes públicas de telecomunicaciones móviles como instrumento para su comisión. De esta manera, se busca fortalecer la confianza de los ciudadanos en las comunicaciones móviles y dotar al Estado de mecanismos más eficaces para prevenir, investigar y judicializar estas conductas, garantizando siempre el respeto por los derechos fundamentales y el tratamiento adecuado de la información personal.

3. CONFLICTO DE INTERÉS

El artículo 293 de la Ley 5ª de 1992, modificado por el artículo 3º de la Ley 2003 de 2019, establece la obligación de los autores y ponentes de presentar en el cuerpo de la exposición de motivos las posibles circunstancias o eventos que puedan configurar un conflicto de interés a la luz del artículo 286 de la Ley 5ª de 1992.

En el caso particular, es necesario mencionar el inciso segundo del artículo 286 del Reglamento del Congreso, el cual establece lo siguiente:

“...Para todos los efectos se entiende que no hay conflicto de interés en las siguientes circunstancias:

a) Cuando el congresista participe, discuta o vote un proyecto de ley o de acto legislativo que otorgue beneficios o cargos de carácter general, es decir, cuando el interés del congresista coincide o se fusione con los intereses de los electores.

b) Cuando el beneficio podría o no configurarse para el congresista en el futuro”.

De la norma citada se evidencia que el presente proyecto de ley establece medidas dirigidas a fortalecer la identificación de los titulares de las líneas móviles, la autenticidad y trazabilidad de las comunicaciones realizadas a través de redes públicas de telecomunicaciones móviles y la prevención de la extorsión, la suplantación de identidad, el fraude y demás conductas ilícitas asociadas al uso de estos servicios. Se trata de una regulación de carácter general, abstracto e impersonal, cuyos efectos están dirigidos a fortalecer la seguridad de las comunicaciones móviles, proteger a los usuarios y dotar al Estado de herramientas para prevenir e investigar la comisión de delitos, sin conferir beneficios particulares, directos o inmediatos a los congresistas.

Ahora bien, el Consejo de Estado, en sentencia proferida el 10 de noviembre de 2009, hizo las siguientes precisiones al referirse a los elementos que deben concurrir para que se configure la violación al régimen de conflicto de intereses como causal de pérdida de investidura:

“No cualquier interés configura la causal de desinvestidura en comento, pues se sabe que sólo lo será aquél del que se pueda predicar que es directo, esto es, que per se el alegado beneficio, provecho

o utilidad encuentre su fuente en el asunto que fue conocido por el legislador; particular, que el mismo sea específico o personal, bien para el congresista o quienes se encuentren relacionados con él; y actual o inmediato, que concurra para el momento en que ocurrió la participación o votación del congresista, lo que excluye sucesos contingentes, futuros o imprevisibles. También se tiene noticia que el interés puede ser de cualquier naturaleza, esto es, económico o moral, sin distinción alguna”.

En consecuencia, sin perjuicio del deber individual que asiste a cada congresista de evaluar y declarar los conflictos de interés que puedan configurarse durante el trámite de la presente iniciativa, podrían presentarse situaciones de conflicto respecto de quienes, por sí mismos o por interpuesta persona, tengan un interés particular, directo y actual derivado de su participación en sociedades operadoras de telecomunicaciones, operadores móviles virtuales, empresas proveedoras de redes y servicios de telecomunicaciones, sociedades dedicadas a la comercialización o distribución de tarjetas SIM, eSIM o tecnologías equivalentes, empresas que administren o utilicen masivamente recursos de identificación de llamadas o mensajes de texto regulados por la presente ley, o cualquier otra actividad directamente relacionada con las materias objeto de esta iniciativa, así como en los demás eventos previstos en la Constitución Política, la Ley 5ª de 1992 y la Ley 2003 de 2019.

4. IMPACTO FISCAL

En cumplimiento de lo dispuesto en el artículo 7º de la Ley 819 de 2003, se deja constancia de que el presente proyecto de ley puede generar impactos fiscales derivados de la implementación de algunas de las medidas previstas en su articulado, en particular aquellas relacionadas con la creación, administración e interoperabilidad del Registro Único de Usuarios de Telefonía Móvil (RUUTM), así como con el fortalecimiento de los mecanismos tecnológicos, operativos y de supervisión requeridos para garantizar la autenticidad de las comunicaciones móviles y el cumplimiento de las obligaciones establecidas en la presente ley.

No obstante, la iniciativa no ordena apropiaciones presupuestales específicas, no crea rentas de destinación específica ni modifica las competencias constitucionales y legales del Gobierno nacional en materia de programación presupuestal. La implementación de las medidas previstas deberá sujetarse al Marco Fiscal de Mediano Plazo, al Marco de Gasto de Mediano Plazo, a la disponibilidad presupuestal, a las apropiaciones que anualmente apruebe el Congreso de la República mediante la Ley de Presupuesto General de la Nación y a las demás normas fiscales y presupuestales vigentes.

Por su parte, las obligaciones de carácter técnico, operativo y tecnológico que recaen sobre los proveedores de redes y servicios de telecomunicaciones móviles, los operadores móviles virtuales y los demás sujetos regulados

deberán ser asumidas por estos en el marco de sus obligaciones legales y regulatorias, sin perjuicio de los mecanismos de coordinación o cofinanciación que el Gobierno nacional pueda establecer durante la reglamentación de la presente ley.

Sin perjuicio de lo anterior, y con el fin de dar cumplimiento a lo previsto en el artículo 7° de la Ley 819 de 2003, durante el trámite legislativo se solicitará al Ministerio de Hacienda y Crédito Público el concepto correspondiente sobre el impacto fiscal de la presente iniciativa y, de ser procedente, el respectivo aval fiscal, para que, en el marco de sus competencias, emita las observaciones que considere pertinentes.

Asimismo, resulta pertinente reiterar el criterio desarrollado por la Corte Constitucional en la Sentencia C-490 de 2011, según el cual la exigencia de analizar el impacto fiscal de los proyectos de ley no puede convertirse en una barrera para el ejercicio de la función legislativa ni otorgar al Gobierno nacional un poder de veto sobre la iniciativa parlamentaria. En el mismo sentido, la Corte Constitucional, mediante Sentencia C-502 de 2007, precisó que las exigencias previstas en el artículo 7° de la Ley 819 de 2003 deben interpretarse de manera armónica con el principio democrático y la autonomía del Congreso de la República para ejercer su función legislativa.



CAMARA DE REPRESENTANTES
SECRETARÍA GENERAL

El día 01 de OCTUBRE del año 2026

Ha sido presentado en este despacho el Proyecto de Ley X Acto Legislativo

No. 416 Con su correspondiente Exposición de Motivos, suscrito Por: H. DARWIN CASTELLANOS ROZAS, MATEO HIDALGO, ANA LIGIA FLORA Y OTROS


SECRETARIO GENERAL

PROYECTO DE LEY NÚMERO 418 DE 2026
CÁMARA

por medio de la cual se adiciona a la Ley 2626 de 2026 el artículo 3A para fortalecer el pensamiento crítico, la autonomía y el uso ético y responsable de la inteligencia artificial y las redes sociales en la educación básica y media.

Bogotá, D. C., 1° de octubre de 2026
Doctor
MIGUEL ÁNGEL SÁNCHEZ VÁSQUEZ
Secretario General
Secretaría General de la Cámara de Representantes

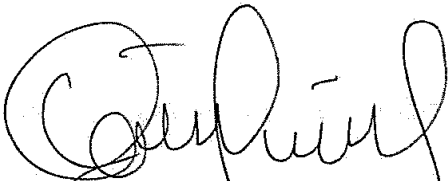
Referencia: Radicación del Proyecto de Ley número 418 de 2026 Cámara, por medio de la cual se adiciona a la Ley 2626 de 2026 el artículo 3A para

fortalecer el pensamiento crítico, la autonomía y el uso ético y responsable de la inteligencia artificial y las redes sociales en la educación básica y media.

Apreciado doctor Miguel Sánchez, cordial saludo,

En mi calidad de Representante a la Cámara por el departamento del Vaupés y en uso de las atribuciones que me han sido conferidas constitucional y legalmente, respetuosamente me permito radicar el Proyecto de Ley número 418 de 2026 Cámara, por medio de la cual se adiciona a la Ley 2626 de 2026 el artículo 3A para fortalecer el pensamiento crítico, la autonomía y el uso ético y responsable de la inteligencia artificial y las redes sociales en la educación básica y media en cumplimiento de los requisitos contenidos en la Ley 5ª de 1992, en especial lo señalado en los artículos 139 y 140, le solicito se sirva dar inicio al trámite legislativo respectivo.

Del honorable Representante a la Cámara:


OSCAR FABIAN ESPINOSA TORRES
Representante a la Cámara
Departamento del Vaupés

EXPOSICIÓN DE MOTIVOS

1. OBJETO Y ALCANCE DE LA INICIATIVA

Se somete a consideración del Congreso de la República una iniciativa orientada a fortalecer la capacidad de los estudiantes para comprender, evaluar y utilizar responsablemente la inteligencia artificial y las redes sociales. Para ello, se establece la incorporación de aprendizajes específicos dentro del área existente de tecnología e informática, aprovechando los procesos de actualización curricular previstos en la Ley 2626 de 2026.

La propuesta busca que los estudiantes puedan identificar las influencias que reciben en los entornos digitales, contrastar información, proteger sus datos y asumir responsabilidad por sus decisiones. Su alcance es educativo: precisa aprendizajes y condiciones para su desarrollo pedagógico, sin crear una asignatura independiente, ampliar la jornada escolar ni establecer un régimen general de regulación de la inteligencia artificial.

El resultado educativo esperado es que el estudiante pueda explicar por qué acepta, cuestiona o descarta una información y cómo protege sus derechos y los de los demás al usar herramientas digitales. La iniciativa propone aprendizajes que acompañen decisiones reales, con independencia de la marca o plataforma que se utilice. Esa independencia permite que el contenido conserve pertinencia frente a cambios tecnológicos.

El énfasis en la autonomía también comprende reconocer cuándo una tarea requiere acompañamiento. Solicitar orientación a un docente, a la familia o a las instancias de protección existentes puede ser una decisión responsable. Por tanto, la capacidad de decidir no se equipará con dejar a niños y adolescentes solos frente a los riesgos, ni reduce los deberes de cuidado de los adultos.

2. ANTECEDENTES Y RELACIÓN CON LA LEGISLACIÓN VIGENTE

NORMATIVIDAD	JUSTIFICACIÓN
Ley 115 de 1994 en su artículo 5°, numeral 9	Establece como fin educativo el fortalecimiento de las capacidades crítica, reflexiva y analítica, orientadas al desarrollo científico y tecnológico y al mejoramiento de la sociedad. Este propósito sustenta la formación para evaluar información y utilizar la inteligencia artificial con criterio propio.
Ley 1581 de 2012 en su artículo 7°	Asigna al Estado y a las entidades educativas responsabilidades de información y formación sobre los riesgos del tratamiento indebido de datos personales de niños, niñas y adolescentes. También contempla conocimientos sobre su uso seguro y responsable y la protección de la privacidad. Sustenta el componente de protección de información personal del proyecto.
Ley 2170 de 2021, artículos 2° a 4°	Establece responsabilidades del Ministerio de Educación Nacional, las instituciones educativas y las familias para promover el uso adecuado de herramientas tecnológicas. Contempla orientaciones técnicas y mecanismos dentro de los acuerdos de convivencia escolar. Permite articular los aprendizajes propuestos con estas responsabilidades y mecanismos existentes.
Ley 2489 de 2025, artículo 6°	Dispone la definición de lineamientos para incorporar estrategias curriculares sobre ciudadanía digital, privacidad, hábitos saludables y prevención de riesgos, atendiendo la edad, el nivel educativo y el contexto. El proyecto busca complementar este marco mediante aprendizajes expresos sobre verificación de información, evaluación de respuestas de inteligencia artificial, comprensión de sesgos e influencia de algoritmos y uso académico responsable.

El antecedente inmediato es la Ley 2626 de 2026, que incorpora competencias digitales y establece una actualización curricular periódica. Sus artículos 3° y 11 ya contemplan la ética digital y la apropiación crítica de las tecnologías.

En consecuencia, su aporte consiste en precisar resultados formativos sobre influencia algorítmica, verificación de información, criterio propio, privacidad, honestidad académica y autocuidado. La adición de un artículo 3A permite articular estos aprendizajes con el marco existente, conservando su ámbito de aplicación.

La opción de adicionar una disposición específica permite distinguir entre la finalidad general de la política de educación digital y los aprendizajes que el legislador considera relevantes para su desarrollo. La precisión propuesta deberá incorporarse en los instrumentos curriculares existentes. Su valor normativo consiste en fijar una orientación estable sobre capacidades de evaluación y responsabilidad, dejando a las autoridades educativas y a los establecimientos la concreción pedagógica.

La actualización técnica del área y la formación ética pueden desarrollarse de manera articulada. Reconocer el funcionamiento de una recomendación automatizada sirve para comprender sus efectos; aprender a utilizar una herramienta implica examinar también la información que se le entrega y la calidad de los resultados. El proyecto busca hacer explícita esa relación dentro de las actividades del área.

3. NECESIDAD Y JUSTIFICACIÓN DE LA PROPUESTA

La formación escolar debe ofrecer herramientas para examinar las decisiones que se toman al consultar una respuesta automatizada, compartir información o interactuar con otras personas en redes sociales. En estas situaciones, el aprendizaje exige comprender el contexto del mensaje, su procedencia, su finalidad y las consecuencias de utilizarlo.

Desde esa perspectiva, el proyecto propone que las instituciones educativas trabajen situaciones concretas: una respuesta que parece convincente, pero debe comprobarse; una imagen que puede haber sido alterada; una recomendación cuyo propósito comercial no resulta evidente; o un trabajo académico en el que debe explicarse cómo se empleó la inteligencia artificial. Estos son ejemplos pedagógicos y no afirmaciones sobre la frecuencia de tales situaciones en la población escolar.

La autonomía digital se entiende en esta iniciativa como una capacidad educativa para tomar decisiones informadas. Supone reconocer influencias, examinar alternativas y valorar consecuencias. El proyecto no atribuye a la tecnología la capacidad de determinar inevitablemente la conducta ni pretende imponer opiniones a los estudiantes.

La protección de la información personal se aborda desde la prevención. Se busca que el estudiante comprenda por qué debe actuar con cuidado al compartir imágenes, voces o datos y por

qué debe respetar los derechos de otras personas. La propuesta no modifica las reglas legales sobre tratamiento de datos ni convierte una actividad escolar en autorización para entregar información a plataformas.

En materia académica, el propósito es promover un uso transparente de las herramientas disponibles. La intervención humana debe permitir revisar la información utilizada, explicar el proceso de elaboración y asumir responsabilidad por el resultado presentado. Los establecimientos conservarán la posibilidad de concretar estas orientaciones en sus prácticas pedagógicas.

El autocuidado se plantea como aprendizaje sobre atención, emociones y convivencia en el uso de tecnologías. No crea servicios de atención clínica ni funciones de diagnóstico para los docentes. Su finalidad es favorecer hábitos de autorregulación y el reconocimiento de situaciones en las que resulte necesario buscar apoyo.

Según la Comisión de Regulación de Comunicaciones en un estudio llamado Infancia y Medios Audiovisuales. Consumo, Mediación Parental y Apropiación. 2024 donde indica lo siguiente:

“(…) El 40% de los NNyA tiene cuenta en redes sociales, principalmente adolescentes (77%), los preadolescentes (33%) y solo un 9% en la infancia temprana.

Mayoría usa cuentas personales: El 83% accede con cuentas propias, cifra que sube a 92% entre adolescentes. En el grupo de 6 a 9 años, fue común que compartieran cuentas con sus padres.

Preferencias por edad: TikTok domina entre los más jóvenes, el 67% la prefieren, mientras que Facebook lidera entre los adolescentes con 30%. (…)”.

Estos resultados muestran que la presencia en redes sociales aumenta con la edad y que, entre quienes acceden a ellas, predomina el uso de cuentas propias. Las diferencias entre grupos de edad y preferencias de plataformas respaldan la pertinencia de una formación digital progresiva, adaptada al desarrollo y al contexto de los estudiantes. En este sentido, el proyecto busca fortalecer capacidades para evaluar críticamente los contenidos, proteger la información personal, identificar riesgos y tomar decisiones autónomas y responsables. Se pretende que la participación en los entornos digitales esté acompañada de conocimientos y criterios para aprovechar sus oportunidades y prevenir riesgos, con el apoyo de las familias y la comunidad educativa.

3.1. CONTEXTO NACIONAL DE USO DE INTELIGENCIA ARTIFICIAL

La Encuesta de Tecnologías de la Información y las Comunicaciones en Hogares del DANE reportó que, en 2024, el 18,0% de las personas de cinco años y más que utilizaron internet empleó herramientas de inteligencia artificial. La proporción fue del 20,4% en cabeceras y del 8,1% en centros poblados y rural disperso.

La diferencia entre esos dos ámbitos fue de 12,3 puntos porcentuales, calculada a partir de los valores publicados.

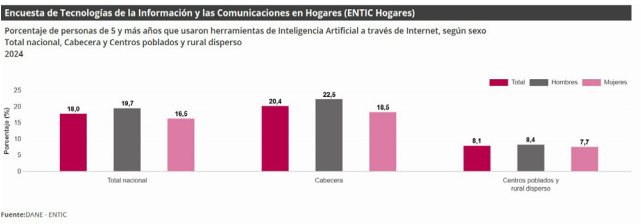


IMAGEN NÚMERO 1 DE ENCUESTA DEL DANE.

El proyecto reconoce que no todos los estudiantes tienen el mismo acceso a internet y a herramientas digitales. Por eso, las actividades no deben exigir una conexión permanente ni aplicaciones de pago, pues algunos podrían quedar excluidos. Estos temas pueden enseñarse mediante ejemplos, análisis de situaciones y materiales disponibles en las instituciones educativas, sin que cada estudiante tenga que acceder a una plataforma.

3.2. ALFABETIZACIÓN DIGITAL Y COMPRENSIÓN DE LA INFLUENCIA ALGORÍTMICA

La propuesta busca que los estudiantes, además de saber utilizar una aplicación o plataforma, comprendan cómo funciona y aprendan a evaluar la información que ofrece. Saber buscar información o crear un contenido no significa necesariamente saber si es confiable. Por eso, se propone enseñarles a hacer preguntas que les ayuden a verificar lo que encuentran.

Por ejemplo, el docente puede presentar dos listas de contenidos recomendados y preguntar por qué son diferentes. A partir de ese ejercicio, puede explicar que las recomendaciones pueden depender de los gustos de cada persona, de lo que ha visto anteriormente o de intereses publicitarios. Para realizar esta actividad no es necesario utilizar cuentas reales ni datos personales de los estudiantes.

El propósito es que comprendan que un contenido no es más importante, imparcial o verdadero por aparecer primero en una búsqueda o recomendación. También se busca que aprendan a consultar otras fuentes y a reconocer cuándo necesitan más información para tomar una decisión. Este es un ejemplo de cómo enseñar la influencia digital; cada institución educativa podrá escoger las actividades más adecuadas para sus estudiantes.

3.3. VERIFICACIÓN DE INFORMACIÓN Y RESPONSABILIDAD ACADÉMICA

La evaluación crítica puede desarrollarse mediante una secuencia de preguntas: quién produce el mensaje, qué evidencia ofrece, cuándo se publicó, si corresponde al contexto que se discute y qué fuentes independientes permiten contrastarlo. La enseñanza debe permitir que el estudiante explique sus razones y reconozca los límites de la información disponible, incluida la posibilidad de no contar aún con elementos suficientes para concluir.

En los trabajos académicos, la transparencia sobre el uso de inteligencia artificial puede concretarse mediante una explicación breve del apoyo recibido y de las verificaciones realizadas. Esa práctica ayuda al docente a observar el proceso de aprendizaje y al estudiante a diferenciar su contribución del contenido obtenido mediante herramientas. La propuesta no establece un formato nacional de declaración ni exige contratar sistemas de detección.

La valoración pedagógica deberá atender al objetivo de la actividad. Si se pretende observar la capacidad de argumentar, resulta pertinente que el estudiante sustente oralmente sus razones o describa cómo llegó a una conclusión. Estos ejemplos ilustran formas de preservar la responsabilidad académica con recursos habituales de aula, sin crear procedimientos de evaluación adicionales por mandato de esta iniciativa.

3.4. PRIVACIDAD Y CONVIVENCIA EN ENTORNOS DIGITALES

La Superintendencia de Industria y Comercio ha explicado que el tratamiento de datos de niños, niñas y adolescentes está sometido a condiciones reforzadas: respeto por su interés superior y sus derechos fundamentales, así como la autorización del representante legal en los términos aplicables y la consideración de la opinión del menor según su madurez. Estas condiciones muestran por qué una actividad educativa no debe convertir el registro en una plataforma en un trámite automático.

La protección de datos puede enseñarse con ejemplos ficticios. Un caso sobre publicación de una fotografía puede servir para discutir qué personas aparecen, si conocen la finalidad de la publicación y qué consecuencias podría tener su circulación. El uso de situaciones inventadas evita exponer información íntima del grupo mientras permite aprender a reconocer problemas reales.

La Ley 1620 de 2013 incorpora el *Ciberbullying* o ciberacoso escolar en el marco de la convivencia escolar y contempla acciones de prevención y atención. La formación propuesta complementa ese enfoque mediante aprendizajes preventivos, sin crear otra ruta de atención ni sustituir las responsabilidades ya existentes. Cuando un caso concreto desborde el ejercicio pedagógico, deberán operar los mecanismos aplicables.

4. DESARROLLO PEDAGÓGICO Y PERTINENCIA TERRITORIAL

Estos contenidos se incorporarán a la planeación del área de Tecnología e Informática, respetando la autonomía de cada institución educativa para organizar su enseñanza. Las actividades deberán adaptarse a la edad, al grado escolar y a las condiciones de los estudiantes, sin exigir conocimientos técnicos para los que todavía no estén preparados.

Los temas podrán enseñarse mediante ejemplos, comparación de textos y conversaciones sobre decisiones cotidianas, sin que los estudiantes deban crear cuentas en redes sociales o plataformas de inteligencia artificial. Por ejemplo, el docente puede

presentar dos respuestas y pedirles que expliquen cómo comprobarían la información y qué fuentes consultarían.

Esta forma de trabajo permite desarrollar las actividades en las instituciones educativas con acceso limitado a internet, especialmente en zonas rurales y dispersas. Tampoco exige que las familias compren dispositivos o paguen por aplicaciones. Sin embargo, estas alternativas no solucionan las diferencias de acceso a la tecnología ni sustituyen las obligaciones del Estado en materia de conectividad.

La enseñanza deberá respetar la diversidad de opiniones, la libertad de conciencia y el proyecto educativo de cada institución educativa. El propósito es que los estudiantes aprendan a analizar la información y a utilizar la tecnología con criterio propio, en armonía con la formación prevista en la Ley 2626 de 2026.

4.1. GRADUALIDAD Y AUTONOMÍA DE LOS ESTABLECIMIENTOS

En los primeros niveles, las actividades pueden centrarse en reconocer información privada, pedir ayuda y distinguir situaciones en las que compartir un contenido puede afectar a otra persona. En niveles posteriores, puede profundizarse en contraste de fuentes, finalidad de los mensajes, errores de las respuestas automatizadas y responsabilidad en la producción de trabajos. Esta progresión es ilustrativa y no sustituye la definición curricular de las autoridades competentes.

La autonomía institucional permite seleccionar materiales, organizar ejemplos y relacionarlos con las experiencias del entorno. El marco común establece qué capacidades se busca fortalecer; la adaptación pedagógica permite determinar cómo trabajarlas. Así se evita que una disposición nacional se convierta en un libreto único, desconectado del nivel de los estudiantes o del proyecto educativo de cada establecimiento.

4.2. APLICACIÓN EN TERRITORIOS RURALES Y CULTURALMENTE DIVERSOS

En departamentos apartados como el Vaupés, la formación sobre inteligencia artificial y uso responsable de la tecnología debe reconocer la riqueza cultural y lingüística de los pueblos indígenas. Los contenidos y las actividades deben dialogar con sus saberes, sus lenguas y sus formas propias de enseñar y aprender, para que resulten pertinentes para los estudiantes y sus comunidades.

Su aplicación debe contar con la participación de las comunidades, las autoridades indígenas y los docentes, respetando su autonomía y sus procesos educativos propios. Esto implica reconocer que el uso de imágenes, relatos y conocimientos de una comunidad requiere especial cuidado y respeto por sus decisiones sobre cómo se comparten. La tecnología puede contribuir a fortalecer y transmitir estos saberes, de acuerdo con las prioridades que los propios pueblos definan.

Asimismo, las limitaciones de conectividad no deben convertirse en una barrera para acceder a estos aprendizajes. Las actividades podrán desarrollarse con materiales disponibles y sin conexión permanente a internet, sin que ello reduzca la responsabilidad del Estado de avanzar en el acceso efectivo y de calidad a la tecnología. La propuesta busca que la formación digital sea pertinente para los territorios y contribuya a ampliar las oportunidades educativas, con respeto por la identidad de sus comunidades.

4.3. PAPEL DEL DOCENTE Y ACOMPAÑAMIENTO FAMILIAR

La mediación docente consiste en orientar preguntas, promover el contraste y ayudar a argumentar decisiones. La iniciativa no exige que cada docente desarrolle aplicaciones ni que domine técnicas avanzadas de programación para enseñar estos aprendizajes. Su concreción deberá guardar relación con las capacidades disponibles y con las competencias del área.

El acompañamiento de las familias puede abordarse en los espacios ordinarios de comunicación escolar. Compartir criterios sobre privacidad o explicar el propósito de una actividad puede favorecer su comprensión, sin que esta iniciativa ordene nuevas reuniones, escuelas de padres o campañas. Tampoco debe trasladarse a las familias la obligación de financiar licencias, dispositivos o servicios para aprobar las actividades.

5. FUNDAMENTO CONSTITUCIONAL Y LEGAL

Los artículos 15 y 16 protegen la intimidad, los datos personales y el libre desarrollo de la personalidad.

Los artículos 44 y 45 respaldan la protección y formación integral de niños y adolescentes, mientras el artículo 68 aporta garantías para la comunidad educativa y la elección de la educación por los padres.

El artículo 67 de la Constitución reconoce la educación como derecho y servicio público con función social.

La propuesta se desarrolla mediante una adición legal de contenido curricular. No define integralmente el núcleo de los derechos fundamentales mencionados ni sustituye sus regímenes de protección. La referencia a ellos sirve como fundamento de las capacidades educativas que se pretende fortalecer.

En el ámbito legal, la Ley 115 de 1994 constituye el marco general de la formación escolar y la Ley 2626 de 2026 es el instrumento que se adiciona. El proyecto conserva las competencias de las autoridades educativas y la autonomía institucional, sin crear entidades o instancias administrativas.

5.1. ALCANCE DE LA INTERVENCIÓN LEGISLATIVA

El proyecto establece orientaciones sobre lo que deben aprender los estudiantes, manteniendo la estructura del área de Tecnología e Informática.

La definición de los contenidos y las actividades se realizará mediante los procesos educativos existentes. De esta manera, la ley podrá seguir siendo útil aunque cambien las aplicaciones y herramientas tecnológicas.

Las disposiciones sobre privacidad, autonomía y convivencia buscan enseñar a los estudiantes a actuar de manera responsable y respetar los derechos de los demás. Su aplicación deberá cumplir las normas vigentes sobre protección de datos personales, autoría y convivencia escolar. El proyecto no crea nuevas sanciones para los estudiantes ni para las plataformas digitales.

Para alcanzar estos objetivos, se propone incorporar los aprendizajes en el área existente, permitir que cada institución educativa elija las actividades más adecuadas y evitar que la participación dependa del pago de aplicaciones o servicios. Durante el trámite legislativo deberá revisarse que estas medidas sean claras y puedan desarrollarse con el personal y los recursos disponibles.

6. CONTENIDO DEL PROYECTO

Artículo 1º: Define el objeto de la iniciativa y su articulación con el área de Tecnología e Informática.

Artículo 2º: Adiciona el artículo 3A a la Ley 2626 de 2026. Precisa seis aprendizajes sobre influencia digital, evaluación de información, criterio propio, protección de datos, responsabilidad académica y autocuidado. Establece gradualidad y preserva la intensidad horaria existente.

Artículo 3º: Regula el desarrollo pedagógico a través de las actividades curriculares existentes y establece que la participación y evaluación no podrán depender de adquirir dispositivos o licencias, crear cuentas personales o suministrar datos a las plataformas.

Artículo 4º: Delimita la implementación a las capacidades existentes y excluye nuevos órdenes de creación de cargos, dependencias, fondos, capacitación adicional, contratación, adquisición de equipos o campañas.

Artículo 5º: Establece la vigencia a partir de la promulgación.

7. ANÁLISIS DEL IMPACTO FISCAL

El artículo 7º de la Ley 819 de 2003 exige identificar el impacto fiscal de los proyectos que ordenen gasto o concedan beneficios tributarios y verificar su compatibilidad con el Marco Fiscal de Mediano Plazo.

La iniciativa incorpora contenidos en los procesos de actualización curricular existentes, sin ordenar subsidios, nuevas estructuras administrativas, ampliación de la jornada o de la planta docente, adquisición de tecnología ni contratación de servicios.

La ausencia de gasto adicional depende de que estas actividades puedan realizarse con las capacidades disponibles. La cláusula de implementación con recursos existentes no demuestra, por sí sola, un

costo fiscal nulo, y todavía no se cuenta con una estimación que permita confirmarlo.

Por ello, deberá verificarse la viabilidad con el Ministerio de Educación Nacional y solicitarse concepto al Ministerio de Hacienda y Crédito Público. Si se identifican costos adicionales, será necesario ajustar la propuesta para evitar nuevas cargas fiscales.

Este análisis comprende únicamente los efectos adicionales del proyecto y no modifica ni limita las obligaciones de financiación establecidas en la Ley 2626 de 2026.

8. CONFLICTO DE INTERESES

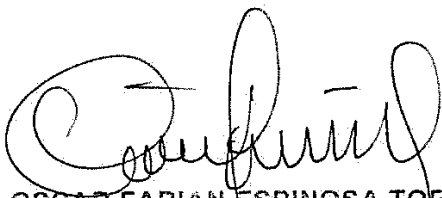
En cumplimiento del artículo 291 de la Ley 5ª de 1992, se presenta el análisis de las circunstancias que podrían generar conflictos de interés durante la discusión y votación de esta iniciativa.

El proyecto busca fortalecer el pensamiento crítico, la autonomía y el uso ético y responsable de la inteligencia artificial y las redes sociales en la educación básica y media. Sus disposiciones tienen alcance general y finalidad educativa.

No establecen beneficios individualizados, favorecen proveedores determinados ni ordenan la adquisición de productos o servicios tecnológicos. Por ello, de su contenido no se advierte, en principio, un beneficio particular, actual y directo para los congresistas.

Sin perjuicio de lo anterior, deberá examinarse cualquier situación en la que un congresista, o las personas comprendidas en el artículo 286 de la Ley 5ª de 1992, tenga intereses en instituciones educativas, empresas tecnológicas o proveedores de contenidos y servicios pedagógicos que puedan resultar específicamente beneficiados por alguna disposición. La existencia de estos vínculos no configura automáticamente un conflicto de interés; deberá valorarse si la decisión legislativa puede producir un beneficio particular, actual y directo en los términos legales.

Este análisis tiene carácter orientador y no sustituye la evaluación individual que corresponde realizar a cada congresista. Quienes identifiquen circunstancias constitutivas de conflicto de interés deberán manifestar oportunamente su impedimento, conforme al procedimiento aplicable, teniendo en cuenta también las modificaciones que se introduzcan durante el trámite legislativo.



OSCAR FABIAN ESPINOSA TORRES
Representante a la Cámara
Departamento del Vaupés

**PROYECTO DE LEY NÚMERO 418 DE 2026
CÁMARA**

por medio de la cual se adiciona a la Ley 2626 de 2026 el artículo 3A para fortalecer el pensamiento crítico, la autonomía y el uso ético y responsable de la inteligencia artificial y las redes sociales en la educación básica y media.

**El Congreso de Colombia
DECRETA:**

Artículo 1º. Objeto. La presente ley tiene por objeto fortalecer el pensamiento crítico, la autonomía en la toma de decisiones y el uso ético y responsable de la inteligencia artificial y las redes sociales, mediante la incorporación de aprendizajes específicos en el área de Tecnología e Informática, en el marco de la Ley 2626 de 2026.

Artículo 2º. Formación para la toma de decisiones en entornos digitales.

Adiciónese un artículo 3A a la Ley 2626 de 2026, así:

Artículo 3A. Pensamiento crítico y autonomía en entornos digitales. En los procesos de actualización curricular previstos en el artículo 3 de la presente ley se incorporarán, dentro de los componentes de inteligencia artificial y alfabetización digital, los siguientes aprendizajes:

1. Comprensión de la influencia digital. Reconocer cómo los algoritmos de recomendación, la publicidad y la selección automatizada de contenidos pueden influir en las opiniones, preferencias, hábitos y decisiones de las personas.

2. Evaluación crítica de la información. Contrastar fuentes, distinguir hechos de opiniones y reconocer los riesgos de la desinformación y de los contenidos generados o modificados mediante inteligencia artificial.

3. Autonomía y criterio propio. Comprender las capacidades y limitaciones de los sistemas de inteligencia artificial, incluidos sus posibles errores y sesgos, y la necesidad de evaluar sus respuestas antes de utilizarlas para tomar decisiones.

4. Protección de la información personal. Identificar los riesgos asociados a compartir datos personales y al uso de imágenes, voces y otros contenidos propios o de terceros, con énfasis en la privacidad, el consentimiento y la prevención de la suplantación de identidad.

5. Responsabilidad en el uso de la inteligencia artificial. Promover la honestidad académica, el respeto por la autoría y el reconocimiento del uso de herramientas de inteligencia artificial en las actividades escolares, conforme a las orientaciones pedagógicas de cada establecimiento educativo.

6. Autocuidado y convivencia digital. Reconocer la influencia de los entornos digitales

en la atención, las emociones y las relaciones interpersonales, y desarrollar prácticas de autorregulación, trato respetuoso y búsqueda de apoyo frente a situaciones de riesgo.

Parágrafo 1º. Estos aprendizajes se desarrollarán de manera gradual, de acuerdo con la edad y el nivel educativo de los estudiantes, respetando la autonomía escolar, el proyecto educativo institucional, la libertad de conciencia y las características del contexto educativo.

Parágrafo 2º. Su incorporación se realizará dentro de la intensidad horaria existente del área de Tecnología e Informática o quien haga de sus veces y no dará lugar a la creación de una asignatura o cátedra independiente ni a la ampliación de la jornada escolar.

Artículo 3º. Desarrollo pedagógico. Los establecimientos educativos comprendidos en el ámbito de aplicación de la Ley 2626 de 2026 integrarán los aprendizajes previstos en esta ley mediante las actividades de planeación y desarrollo curricular existentes.

Para ello podrán emplear análisis de casos, contraste de fuentes, debates y ejercicios de reflexión sobre situaciones cotidianas, utilizando los recursos pedagógicos disponibles.

La participación y evaluación de los estudiantes no podrán condicionarse a la adquisición de dispositivos o licencias, a la creación de cuentas personales en redes sociales o servicios de inteligencia artificial, ni al suministro de datos personales a dichas plataformas. Las actividades podrán desarrollarse sin conexión a internet.

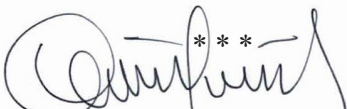
Artículo 4º. Implementación con capacidades existentes. Las disposiciones de la presente ley se incorporarán en los procesos de actualización

curricular y gestión educativa previstos en la Ley 2626 de 2026, con los recursos humanos, técnicos y presupuestales existentes, sin exigir una actualización extraordinaria.

La presente ley no ordena la creación de cargos, dependencias, fondos, programas adicionales de capacitación ni instancias administrativas, ni impone la contratación de servicios, la adquisición de equipos o licencias o la realización de campañas.

Lo dispuesto en este artículo se circunscribe a las medidas incorporadas por la presente ley y no modifica las obligaciones establecidas en la Ley 2626 de 2026.

5º. Vigencia. La presente ley rige a partir de su promulgación.



OSCAR FABIAN ESPINOSA TORRES
Representante a la Cámara
Departamento del Vaupés

DE REPRESENTANTES
SECRETARÍA GENERAL

El día 01 de OCTUBRE del año 2026

Ha sido presentado en este despacho el

Proyecto de Ley X Ato Legislativo

Nº. 418 Con su correspondiente

Exposición de Motivos, suscrito Por: HON. OSCAR FABIAN ESPINOSA TORRES


SECRETARÍO GENERAL

CONTENIDO

Gaceta número 1504 - Jueves, 8 de octubre de 2026

CÁMARA DE REPRESENTANTES

PROYECTOS DE LEY

Págs.

Proyecto de Ley número 416 de 2026 Cámara, por medio de la cual se establecen medidas para garantizar la identificación de los titulares de las líneas móviles, la autenticidad y trazabilidad de las comunicaciones cursadas a través de redes públicas de telecomunicaciones móviles, se adoptan mecanismos para prevenir el fraude y otros usos ilícitos de estos servicios, y se dictan otras disposiciones. - Ley No Más Extorsión y Suplantación Telefónica 1

Proyecto de Ley número 418 de 2026 Cámara, por medio de la cual se adiciona a la Ley 2626 de 2026 el artículo 3A para fortalecer el pensamiento crítico, la autonomía y el uso ético y responsable de la inteligencia artificial y las redes sociales en la educación básica y media 12