

Bogotá D.C., septiembre de 2026

Doctor
SECRETARIO GENERAL
MIGUEL ÁNGEL SÁNCHEZ VÁSQUEZ
Cámara de Representantes
Ciudad

Asunto: Radicación del Proyecto de Ley Línea Segura

Respetado señor Secretario:

En ejercicio de la facultad prevista en los artículos 150 y 154 de la Constitución Política y de conformidad con los artículos 139 y siguientes de la Ley 5ª de 1992, presentó a consideración del Congreso de la República el proyecto de ley “Por medio de la cual se establecen medidas para prevenir y atender el uso fraudulento o delictivo de líneas y servicios móviles y se dictan otras disposiciones - Ley Línea Segura”.

En consecuencia, solicitó impartir el trámite constitucional y legal correspondiente, ordenar su publicación en la Gaceta del Congreso y remitir a la comisión constitucional permanente competente.

Cordialmente,

HEINER DE JESÚS GAITÁN PARRA
Representante a la Cámara
Movimiento Pacto Histórico

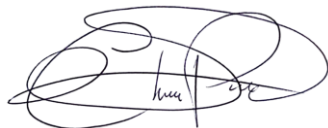
Coautores



SANTIAGO OSORIO MARÍN
Representante a la Cámara por Caldas



JAIRO LEÓN VARGAS
Representante a la Cámara por Bogotá

Alianza Verde - Coalición Pacto Histórico	Movimiento Pacto Histórico
 MARIA DEL MAR PIZARRO GARCÍA Representante Cámara por Bogotá Pacto Histórico	 CHRISTIAN HOSEP PALACIOS LEDEZMA Representante a la Cámara Pacto Histórico

Proyecto de Ley número _____ de 2026 Cámara

Por medio de la cual se establecen medidas para prevenir y atender el uso fraudulento o delictivo de líneas y servicios móviles y se dictan otras disposiciones

El Congreso de Colombia

DECRETA

Capítulo I Disposiciones generales

Artículo 1. Objeto. La presente ley busca impedir que las líneas móviles sean vendidas, activadas, respuestas o portadas sin controles y trazabilidad, y prevenir su uso fraudulento o delictivo; facilitar una reacción rápida cuando una persona pierda el control de su número; y conservar información útil para las autoridades, con respeto por la intimidad, el debido proceso y la protección de datos.

Artículo 2. Ámbito de aplicación. La ley se aplica a los proveedores de servicios móviles, incluidos los operadores móviles virtuales; a sus distribuidores, vendedores y agentes autorizados; y a las autoridades expresamente mencionadas. Comprende las tarjetas SIM físicas, las eSIM y las tecnologías que cumplan la misma función.

Artículo 3. Definiciones. Para esta ley se entenderá por: 1. Línea móvil: el número asociado a un servicio móvil. 2. SIM o eSIM: el medio físico o digital que permite identificar y habilitar al usuario en una red móvil. 3. Evento de alto riesgo: la activación, reposición, portabilidad, cambio de titular, transferencia de una eSIM, recuperación de cuenta o modificación de los medios de autenticación. 4. Traza: el registro que permite establecer cuándo, dónde, por qué canal, con qué verificación y por intervención de quién se realizó una actuación. 5. Comunicación móvil maliciosa: la llamada o mensaje

utilizado para amenazar, suplantar, engañar, enviar enlaces o códigos peligrosos o inducir la entrega de información o dinero.

Artículo 4. Garantías. Las medidas previstas en esta ley serán necesarias, proporcionales, accesibles y revisables. La ley no autoriza interceptaciones, vigilancia masiva, consulta general del contenido de las comunicaciones ni biometría obligatoria para todos los usuarios. La sola aparición de una persona como titular de una línea no prueba que haya cometido un delito o una infracción.

Capítulo II Venta activación y control de las líneas

Artículo 5. Venta autorizada. Las SIM y eSIM solo podrán ser distribuidas o entregadas por el proveedor o por agentes autorizados e identificables. El proveedor deberá mantener actualizada la relación de sus puntos de venta físicos y digitales, capacitar a quienes atienden al público, controlar el acceso a los datos del usuario y retirar la autorización cuando se incumplan las reglas de seguridad.

Artículo 6. Prohibición de líneas preactivadas. Se prohíbe vender, entregar o poner en funcionamiento una SIM o eSIM activada antes de verificar la identidad y la voluntad del usuario. El proveedor deberá poder establecer qué agente recibió, custodió y entregó cada SIM física y quién generó o asignó cada perfil eSIM.

Artículo 7. Verificación de identidad. La identidad se verificará mediante mecanismos seguros y adecuados al riesgo. Cuando se usen datos biométricos deberán respetarse las reglas aplicables a los datos sensibles y existir una alternativa razonable, salvo que una ley especial disponga otra cosa. Habrá procedimientos para personas sin teléfono inteligente, sin conectividad o con barreras de acceso.

Artículo 8. Consulta de líneas. Toda persona tendrá derecho a consultar gratuitamente las líneas activas asociadas a su identificación, desconocer una línea que no haya solicitado y pedir su revisión. El proveedor entregará una constancia y adoptará medidas para evitar que la persona continúe afectada mientras verifica el caso. Desconocer una línea no trasladará al usuario la carga de demostrar el fraude.

Artículo 9. Alertas y verificación reforzada. El proveedor avisará al usuario cuando se solicite una activación, reposición, portabilidad, cambio de titular, transferencia de eSIM o modificación de sus medios de autenticación. Siempre que sea posible, el aviso se enviará antes de completar el trámite y por un canal distinto de la línea que puede estar comprometida. La autorización no podrá depender únicamente de un código o llamada recibida en esa misma línea.

Artículo 10. Bloqueo voluntario de seguridad. El usuario podrá pedir gratuitamente que su cuenta quede protegida contra reposiciones, portabilidades, cambios de titular

o transferencias de eSIM. El bloqueo deberá ser fácil de activar y solo podrá levantarse mediante una verificación reforzada. La Comisión de Regulación de Comunicaciones definirá sus condiciones sin impedir la portabilidad legítima, el acceso a emergencias o la continuidad del servicio.

Artículo 11. Trazabilidad y control de riesgos. El proveedor conservará registros suficientes para reconstruir la venta, entrega, activación, reposición, portabilidad, cambio de titular, transferencia de eSIM, restricción y recuperación de una línea. También deberá detectar patrones anormales, puntos de venta con operaciones irregulares y múltiples activaciones o reposiciones injustificadas. Una alerta automática deberá ser revisada por una persona antes de cancelar definitivamente un servicio o atribuir responsabilidad al usuario.

Capítulo III Protección de las víctimas

Artículo 12. Canal Línea Segura. Los proveedores dispondrán de un canal gratuito y permanente denominado Línea Segura. Allí podrán reportarse líneas desconocidas, pérdida de control del número, reposición o portabilidad no autorizada, transferencia fraudulenta de eSIM, suplantación, llamadas extorsivas y mensajes o enlaces maliciosos. El canal entregará número de caso, fecha y hora, permitirá seguimiento e informará las medidas adoptadas.

Artículo 13. Respuesta inmediata. Una vez verificada por un medio razonable, la persona afectada podrá solicitar que se detenga el trámite, se restrinja temporalmente la línea o se le devuelva su control. El proveedor deberá impedir que el procedimiento de recuperación facilite el acceso a otras cuentas. A solicitud del usuario, entregará una constancia del incidente y de las actuaciones realizadas, sin revelar datos de terceros o información reservada.

Artículo 14. Restricción y restablecimiento. Ante indicios objetivos de fraude, el proveedor podrá restringir temporalmente una línea o un trámite. La decisión será informada, tendrá una duración limitada y podrá ser controvertida. El usuario tendrá derecho a revisión humana. Si la medida fue equivocada, el servicio y los registros serán corregidos sin dilaciones, sin perjuicio de los demás derechos de la persona afectada.

Capítulo IV Llamadas mensajes y enlaces maliciosos

Artículo 15. Reporte de comunicaciones maliciosas. Línea Segura permitirá reportar números, remitentes, enlaces, dominios y códigos QR utilizados en llamadas o mensajes presuntamente fraudulentos o extorsivos. Con base en información objetiva y actualizada, los proveedores podrán advertir al usuario o adoptar medidas en sus propias redes. Toda afectación a un remitente legítimo deberá poder corregirse. Este

artículo no autoriza bloquear sitios de internet ni revisar de manera general el contenido de las comunicaciones.

Artículo 16. Identificación del origen. La Comisión de Regulación de Comunicaciones establecerá, de manera gradual y cuando sea viable, reglas para identificar llamadas y mensajes con números o nombres de remitentes falsos. Podrá crear mecanismos para validar los nombres utilizados por empresas y entidades públicas y para impedir que números oficiales sean imitados desde redes no autorizadas. La regulación deberá evitar bloqueos equivocados y ofrecer un procedimiento de corrección.

Artículo 17. Preservación de información. Los proveedores deberán estar en capacidad de conservar y entregar datos existentes, concretos e debidamente identificados cuando lo ordene una autoridad competente. La preservación no autoriza por sí sola el acceso al contenido de las comunicaciones ni amplía las facultades de investigación previstas en la Constitución y la ley.

Capítulo V Coordinación institucional

Artículo 18. Prevención del fraude financiero. Cuando la pérdida de una línea pueda comprometer una cuenta bancaria, billetera digital u otro producto financiero, el proveedor informará al usuario las rutas existentes y facilitará su activación. Dentro de las autorizaciones legales, los sectores de telecomunicaciones y financiero podrán confirmar si una línea tuvo recientemente una reposición, portabilidad o cambio de control, utilizando únicamente la información necesaria y sin acceder al contenido de las comunicaciones.

Artículo 19. Comunicaciones desde establecimientos de reclusión. Las autoridades y los proveedores continuarán aplicando las reglas vigentes para identificar y bloquear comunicaciones no autorizadas originadas en establecimientos de reclusión. Sin crear un procedimiento paralelo, conservarán registro de la solicitud y de su cumplimiento. Los Ministerios de Justicia y del Derecho y de Tecnologías de la Información y las Comunicaciones publicarán anualmente un balance agregado sobre dispositivos identificados, solicitudes de bloqueo, tiempos de respuesta y correcciones, protegiendo la reserva de las investigaciones y la seguridad penitenciaria.

Artículo 20. Información pública. El Ministerio de Tecnologías de la Información y las Comunicaciones y la Comisión de Regulación de Comunicaciones acordarán categorías comunes para medir líneas preactivadas, activaciones irregulares, reposiciones o portabilidades fraudulentas, transferencias no autorizadas de eSIM, suplantación de números, reportes recibidos, bloqueos equivocados, restablecimientos y tiempos de respuesta. La información será agregada, no identificará a las víctimas y distinguirá entre reportes, casos confirmados y decisiones de autoridad.

Capítulo VI Aplicación y vigencia

Artículo 21. Protección de datos y acceso al servicio. Los datos tratados en aplicación de esta ley solo podrán utilizarse para las finalidades autorizadas y estarán sujetos a las reglas de protección de datos personales. Las medidas deberán contemplar alternativas para zonas rurales, personas con discapacidad, adultos mayores, migrantes, comunidades étnicas y usuarios sin conectividad. Nadie podrá ser excluido injustificadamente del servicio.

Artículo 22. Vigilancia y control. El Ministerio de Tecnologías de la Información y las Comunicaciones ejercerá sus funciones frente a los proveedores. La Superintendencia de Industria y Comercio actuará en protección del consumidor y de datos personales. Las demás autoridades intervendrán únicamente dentro de sus competencias. Los incumplimientos se investigarán y sancionarán conforme a los regímenes vigentes y con respeto del debido proceso.

Artículo 23. Reglamentación y evaluación. El Gobierno nacional y la Comisión de Regulación de Comunicaciones reglamentarán la ley, dentro de sus competencias, en los doce meses siguientes a su promulgación. Escucharán a usuarios, víctimas, operadores, vendedores, autoridades, academia y organizaciones de derechos digitales. Dos años después de iniciada la implementación, el Ministerio de Tecnologías de la Información y las Comunicaciones presentará a las Comisiones Sextas del Congreso una evaluación pública sobre resultados, costos, tiempos de respuesta, bloqueos equivocados, afectaciones territoriales y ajustes necesarios.

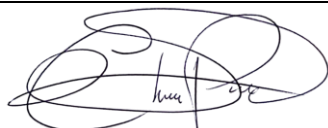
Artículo 24. Implementación y vigencia. La presente ley rige a partir de su promulgación. Las obligaciones técnicas se aplicarán gradualmente, de acuerdo con el riesgo, la capacidad de los sujetos obligados, la continuidad del servicio y los plazos que fije la reglamentación. La transición no suspende las obligaciones vigentes ni permite la venta de SIM preactivadas.

HEINER DE JESÚS GAITÁN PARRA

Representante a la Cámara
Movimiento Pacto Histórico

Coautores:

	
---	--

SANTIAGO OSORIO MARÍN Representante a la Cámara por Caldas Alianza Verde - Coalición Pacto Histórico	
 MARIA DEL MAR PIZARRO GARCÍA Representante Cámara por Bogotá Pacto Histórico	 CHRISTIAN HOSEP PALACIOS LEDEZMA Representante a la Cámara Pacto Histórico

Exposición de motivos

Proyecto de Ley Línea Segura

1 Propuesta

Hoy una línea móvil no solo sirve para llamar. También permite recuperar contraseñas, recibir códigos bancarios, abrir cuentas, mover dinero y demostrar una identidad digital. Cuando un delincuente toma el control del número de otra persona, puede hacerse pasar por ella, entrar a sus cuentas y utilizar su nombre para amenazar o defraudar.

Línea Segura propone una regla sencilla: toda línea debe dejar una huella verificable desde su venta hasta su activación y cada vez que alguien pretenda cambiarla, reponerla o recuperarla. Si ocurre una irregularidad, la víctima debe poder detener el daño y recuperar el control sin recorrer una cadena interminable de trámites.

El proyecto no promete acabar por sí solo con la extorsión. Cierra vacíos concretos que hoy facilitan el anonimato operativo, la venta de líneas preactivadas, la suplantación, el cambio fraudulento de SIM o eSIM y la pérdida de información útil para investigar.

2 Un problema reconocido por las autoridades colombianas

Las respuestas oficiales recibidas durante la preparación de la iniciativa coinciden en que el problema no se limita a identificar al titular de una línea. También es necesario conocer quién la vendió, cómo fue activada, qué verificación se realizó, quién autorizó una reposición o portabilidad y qué hizo el proveedor cuando la víctima reportó el fraude.

MinTIC informó que, en el primer trimestre de 2026, Colombia tenía 94.563.660 líneas móviles en servicio y que 71.051.101 correspondían a prepago, cerca del 75,1 %. Durante el mismo trimestre se registraron 9.748.992 activaciones y 9.018.985 retiros. La magnitud y rotación del mercado muestran por qué un tope fijo de líneas sería insuficiente y por qué conviene controlar los momentos en que una línea nace, cambia de manos o es recuperada.

La Superintendencia Financiera reportó 2.408 quejas relacionadas con duplicación o reposición fraudulenta de SIM, portabilidad irregular, SIM preactivadas e identidades falsas entre julio de 2025 y el 2 de septiembre de 2026. También informó reclamaciones asociadas a smishing y vishing por \$30.622 millones en 2022, \$62.836 millones en 2023 y \$92.235 millones en 2024. Son registros administrativos y no condenas penales, pero muestran la conexión entre una comunicación engañosa, la apropiación de una línea y la pérdida de dinero.

La Fiscalía General de la Nación explicó que sus sistemas no clasifican de manera uniforme variables como SIM o eSIM, reposición, portabilidad, enlaces, códigos QR, suplantación de línea u origen penitenciario. La ausencia de esas categorías impide medir el fenómeno de forma comparable y justifica que el proyecto ordene una taxonomía común, sin imponer a la Fiscalía la creación retroactiva de información ni desconocer su autonomía.

La Comisión de Regulación de Comunicaciones señaló límites en su capacidad para intervenir directamente frente a distribuidores y otros actores que no son proveedores. Por ello, la ley obliga al operador a organizar, identificar y controlar su cadena autorizada. MinTIC destacó, a su vez, la importancia de la trazabilidad, la autenticación proporcional y la coordinación entre sistemas, y confirmó sus funciones de inspección, vigilancia y control.

La Procuraduría General de la Nación advirtió en 2023 y 2024 sobre fallas en inhibidores de señal, uso de eSIM y plataformas financieras desde establecimientos de reclusión y falta de articulación institucional. El Decreto 851 de 2024 reconoció que las comunicaciones no autorizadas desde las cárceles persistían pese a las normas existentes. Línea Segura no duplica ese régimen: exige dejar registro de su ejecución y publicar resultados agregados para saber si las órdenes se cumplen.

3 ¿Qué cambia para la ciudadanía?

Primero, nadie deberá recibir una SIM ya activada. Segundo, cualquier persona podrá saber qué líneas aparecen a su nombre y desconocer las que no solicitó. Tercero, antes de una reposición, portabilidad, cambio de titular o transferencia de eSIM deberá existir una verificación reforzada y, cuando sea posible, una alerta por un canal distinto de la línea comprometida.

Cuarto, el usuario podrá activar un bloqueo voluntario para impedir cambios sobre su línea. Quinto, existirá el canal gratuito Línea Segura para detener un trámite, restringir temporalmente el número, recuperar su control y obtener una constancia del incidente. Sexto, las decisiones equivocadas deberán revisarse por una persona y corregirse sin demora.

4 ¿Qué cambia para los proveedores?

Los operadores deberán conocer y supervisar a quienes venden sus SIM, impedir la venta de líneas preactivadas, registrar los eventos importantes y detectar comportamientos anormales. También deberán ofrecer una ruta sencilla de atención y estar en capacidad de preservar información concreta cuando exista una orden legítima.

La ley fija resultados mínimos, pero no obliga a utilizar una marca, programa o tecnología determinada. Esta decisión permite que los controles mejoren con el tiempo y evita que la ley revele a los delincuentes un único procedimiento que puedan aprender a burlar.

5 Llamadas mensajes y enlaces maliciosos

Dirección: Bogotá. Edificio nuevo del Congreso.
Cra 7 #8-68

La iniciativa recoge el trabajo previo conocido como “Ley Anti-Enlaces”, pero lo limita a las comunicaciones móviles. Un enlace, dominio o código QR podrá reportarse cuando llegue mediante una llamada o mensaje utilizado para suplantar, amenazar o engañar. El proyecto no regula todo internet, no autoriza revisar conversaciones y no permite bloquear sitios web por decisión general de un operador.

Página web: <https://heinergaitan.com/>

También se habilita a la CRC para desarrollar reglas que ayuden a identificar números o nombres de remitentes falsificados, especialmente cuando imitan bancos, empresas o entidades públicas. Cualquier medida deberá permitir corregir los bloqueos equivocados.

6 Lecciones internacionales utilizadas como referencia

La experiencia extranjera se utilizó como fuente de orientación y no como texto para copiar. Estados Unidos exige verificar de forma segura las reposiciones y portabilidades, avisar al usuario, ofrecer bloqueo voluntario y documentar el incidente. Australia combina verificación reforzada, auditoría y sanción, y ha reportado reducciones importantes en el fraude de portabilidad. ENISA (En España, Empresa Nacional de

Innovación S.A) recomienda coordinar operadores, bancos y autoridades y capacitar al personal que atiende estos trámites.

NIST (Por sus siglas en inglés *National Institute of Standards and Technology* o Instituto Nacional de Estándares y Tecnología) advierte que no es seguro depender únicamente de mensajes enviados a la misma línea cuyo control está en discusión. España ha avanzado en la validación de los nombres utilizados como remitentes de mensajes empresariales y públicos. India permite que cada ciudadano consulte las conexiones registradas a su nombre y reporte las desconocidas.

También se estudiaron experiencias que aconsejan prudencia. La Suprema Corte mexicana invalidó un padrón nacional con biometría obligatoria, y la GSMA (Por sus siglas en inglés *Global System For Mobile Communications Association*) ha advertido que registrar usuarios no basta si existen identidades prestadas, ventas informales, fallas de control o exclusión de personas vulnerables. Por eso el proyecto colombiano no crea un padrón biométrico central, no fija un número máximo de líneas y no presume culpable al titular.

7 Antecedentes legislativos y diferencia de Línea Segura

El Congreso ha conocido iniciativas orientadas al registro y venta de SIM. El Proyecto de Ley 077 de 2026 Cámara, presentado por el representante Daniel Felipe Briceño Montes, propone un registro nacional, desactivación por falta de registro y límites para líneas prepago. Línea Segura comparte la preocupación por el anonimato, pero propone una respuesta diferente: controlar la cadena de venta, proteger los cambios de SIM y eSIM, alertar al usuario, atender a la víctima y corregir los bloqueos equivocados.

La eventual acumulación deberá analizarse conforme a la Ley 5ª de 1992. En cualquier escenario, las garantías de atención, recuperación, trazabilidad y proporcionalidad de esta iniciativa pueden enriquecer la discusión legislativa.

8 Fundamento constitucional y legal

El Congreso es competente conforme a los artículos 150 y 154 de la Constitución. La iniciativa desarrolla el deber estatal de proteger la vida, honra y bienes; la intimidad y el habeas data; el debido proceso; la libertad de comunicación; y los principios de la función administrativa previstos en los artículos 2, 15, 20, 29 y 209.

Se propone una ley ordinaria porque su materia principal es la prestación segura de servicios móviles y las obligaciones de sus agentes. No regula integralmente un derecho fundamental, no crea interceptaciones ni modifica el procedimiento penal. Se articula con las Leyes 1341 de 2009, 1978 de 2019, 1266 de 2008, 1581 de 2012, 1908 de 2018 y 2573 de 2026; con el Decreto 851 de 2024; y con la regulación compilada por la CRC.

9 Unidad de materia competencias e impacto fiscal

Todos los artículos desarrollan un mismo propósito: prevenir y atender el uso fraudulento o delictivo de líneas y servicios móviles. La venta, activación, reposición, portabilidad, eSIM, atención de la víctima, mensajes maliciosos, preservación y medición forman parte de una misma cadena de prevención y respuesta.

La iniciativa utiliza autoridades y sistemas existentes. No crea una entidad, fondo o planta de personal. Puede generar costos de adaptación para proveedores y cargas de reglamentación y seguimiento que deberán precisarse mediante el análisis de impacto normativo y atenderse dentro de las competencias y disponibilidades existentes. Durante el trámite se solicitarán los conceptos fiscales y sectoriales correspondientes.

10 Construcción participación y revisión técnica

El texto fue construido a partir de derechos de petición y respuestas oficiales de MinTIC, CRC, Superintendencia Financiera, Ministerio de Justicia y del Derecho, Fiscalía General de la Nación y Policía Nacional; del análisis de la regulación vigente y de proyectos previamente radicados; y de documentos públicos de Procuraduría, INPEC y autoridades internacionales.

La iniciativa no se presenta como un texto cerrado. Antes de la ponencia para primer debate deberán realizarse mesas públicas con SIC, INPEC, USPEC, operadores móviles y virtuales, distribuidores, organizaciones de víctimas y consumidores, universidades y expertos en privacidad y seguridad digital. Las observaciones deberán registrarse y explicar qué cambios fueron aceptados o descartados. Este procedimiento permitirá que la técnica esté al servicio de una decisión legislativa comprensible y verificable.

11 Consulta previa conflicto de intereses y Ley 5ª

El proyecto contiene medidas generales y no identifica una afectación directa, específica y diferenciada a comunidades étnicas que haga exigible consulta previa. Esta conclusión deberá revisarse si durante el trámite se incorporan medidas territoriales o culturalmente diferenciadas.

Por su carácter general, la discusión y votación no genera por sí misma un beneficio particular, actual y directo para los congresistas. Cada integrante deberá valorar y declarar las circunstancias personales previstas en el artículo 291 de la Ley 5ª de 1992 y la Ley 2003 de 2019.

El expediente contiene carta de radicación, título, encabezamiento, articulado, exposición de motivos y espacio de firmas, de conformidad con los artículos 139 y siguientes de la Ley 5ª de 1992. La materia dominante corresponde a comunicaciones y tecnologías, por lo que su comisión constitucional natural es la Comisión Sexta, conforme a la Ley 3ª de 1992.

12 Conclusión

Detrás de cada línea fantasma puede existir una víctima real: alguien a quien le usaron el nombre, le vaciaron una cuenta, lo amenazaron o lo obligaron a demostrar que nunca pidió ese número. Línea Segura no busca vigilar a los ciudadanos. Busca que quienes venden, activan y modifican una línea respondan por el procedimiento; que cada cambio deje una huella; y que la víctima tenga una puerta clara para detener el daño.

Fuentes principales

- Respuestas oficiales allegadas por MinTIC, CRC, Superintendencia Financiera, Ministerio de Justicia y del Derecho, Fiscalía General de la Nación y Policía Nacional al proceso de preparación de la iniciativa.
- Procuraduría General de la Nación, pronunciamientos del 17 de julio de 2023 y 10 de enero de 2024 sobre comunicaciones y extorsión desde establecimientos de reclusión.
- Ministerio de Tecnologías de la Información y las Comunicaciones, Decreto 851 de 2024.
- INPEC, Informe de las acciones y compromisos de respuesta a audiencia pública, 14 de noviembre de 2024.
- Federal Communications Commission, Protecting Consumers from SIM-Swap and Port-Out Fraud, 88 FR 85794, 2023.
- ENISA, Countering SIM-Swapping, 2021; NIST Special Publication 800-63B; Australian Communications and Media Authority, reglas e informes sobre portabilidad y SIM swap.
- Lee, Kaiser, Mayer y Narayanan, An Empirical Study of Wireless Carrier Authentication for SIM Swaps, SOUPS 2020.
- España, Orden TDF/149/2025 y Circular 1/2026 de la CNMC; India, Sanchar Saathi y TAF COP; Suprema Corte de Justicia de la Nación de México, Acción de inconstitucionalidad 82/2021 y acumulada 86/2021; GSMA, estudios sobre registro obligatorio de SIM prepago.

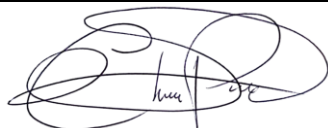
Cordialmente,

HEINER DE JESÚS GAITÁN PARRA

Representante a la Cámara
Movimiento Pacto Histórico

Coautores

Proyecto de Ley Línea Segura

 SANTIAGO OSORIO MARÍN Representante a la Cámara por Caldas Alianza Verde - Coalición Pacto Histórico	
	 CHRISTIAN HOSEP PALACIOS LEDEZMA Representante a la Cámara Pacto Histórico
 MARIA DEL MAR PIZARRO GARCÍA Representante Cámara por Bogotá Pacto Histórico	

Autores y coautores

Proyecto de Ley Línea Segura
