REPÚBLICA DE COLOMBIA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

I S S N 0 1 2 3 - 9 0 6 6

AÑO XXXV - Nº 1460 | Bogotá, D. C., viernes, 2 de octubre de 2026 | EDICIÓN DE 26 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

PROYECTO DE LEY

PROYECTO DE LEY NÚMERO 364 DE 2026 CÁMARA

por medio de la cual se regula el uso de inteligencia artificial en el sector defensa y se dictan otras disposiciones.

Bogotá, D. C., septiembre de 2026

Secretario General

MIGUEL ÁNGEL SÁNCHEZ VÁSQUEZ

Cámara de Representantes Ciudad

Referencia: Radicación de Proyecto de Ley número 364 de 2026 Cámara.

En mi condición de miembro del Congreso de la República me permito poner a consideración de la Honorable Cámara de Representantes el Proyecto de Ley, *por medio de la cual se regula el uso de inteligencia artificial en el sector defensa y se dictan otras disposiciones*, el cual tiene por objeto establecer un marco jurídico para el uso de inteligencia artificial en defensa, Fuerza Pública y seguridad, prohibir de manera absoluta los sistemas de armas autónomas y regular estrictamente los sistemas de alto riesgo.

Cordialmente,



PROYECTO DE LEY NÚMERO 364 DE 2026 CÁMARA

por medio de la cual se regula el uso de inteligencia artificial en el sector defensa y se dictan otras disposiciones.

El Congreso de Colombia

DECRETA

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1°. *Objeto*. La presente ley tiene por objeto establecer el marco jurídico para el diseño, desarrollo, adquisición, importación, exportación, comercialización, prueba, despliegue, supervisión y uso de sistemas de inteligencia artificial en el sector defensa, las Fuerzas Militares, la Policía Nacional y las actividades estatales de seguridad, con el fin de garantizar el control humano significativo, la protección de los derechos humanos, el cumplimiento del Derecho Internacional Humanitario, la responsabilidad de la cadena de mando, la transparencia compatible con la seguridad nacional y la prohibición absoluta de los sistemas de armas autónomas.

Artículo 2°. *Ámbito de aplicación*. La presente ley se aplicará a:

1. El Ministerio de Defensa Nacional.
2. Las Fuerzas Militares.
3. La Policía Nacional.
4. Las entidades adscritas y vinculadas al sector defensa.
5. Las personas naturales o jurídicas, públicas, privadas o mixtas, nacionales o extranjeras, que diseñen, desarrollen, fabriquen, comercialicen, importen, exporten, transfieran, integren,

mantengan, operen o suministren sistemas de inteligencia artificial, componentes, modelos, software, hardware, sensores, plataformas o servicios destinados al sector defensa, la Fuerza Pública o actividades estatales de seguridad.

Parágrafo. La presente ley se aplicará sin perjuicio de los regímenes constitucionales y legales sobre defensa nacional, orden público, inteligencia y contrainteligencia, protección de datos personales, contratación estatal, comercio exterior, armas, municiones y explosivos, responsabilidad disciplinaria, responsabilidad penal y control fiscal.

Artículo 3°. ***Definiciones***. Para efectos de la presente ley, se entenderá por:

1. **Sistema de inteligencia artificial en defensa y seguridad:** sistema computacional, modelo, software, plataforma, dispositivo o infraestructura tecnológica que, mediante técnicas de aprendizaje automático, modelos algorítmicos, análisis automatizado de datos, visión por computador, procesamiento de lenguaje, autonomía robótica, sistemas expertos u otras técnicas similares, apoye, recomiende, automatice o ejecute funciones asociadas a defensa, seguridad, inteligencia, contrainteligencia, vigilancia, operaciones militares, operaciones policiales, ciberdefensa, logística, entrenamiento, simulación, análisis operacional o uso de la fuerza.

2. **Sistema de armas autónomas:** sistema integrado por una o más armas y componentes tecnológicos que, al operar conjuntamente y una vez activado, puede identificar, seleccionar y atacar objetivos mediante el empleo de fuerza letal o no letal contra personas u objetos, sin una decisión humana previa, específica e informada que determine el objetivo concreto o grupo específico de objetivos y el empleo de fuerza contra ellos, incluido el momento del ataque, bajo las condiciones de control humano significativo previstas en esta ley.

3. **Sistema semiautónomo asociado al uso de la fuerza:** sistema que incorpora funciones automatizadas o autónomas de apoyo, detección, navegación, identificación, seguimiento, recomendación, priorización o asistencia, pero cuyo empleo de fuerza requiere autorización humana previa, expresa, informada, trazable y jurídicamente responsable.

4. **Sistema de alto riesgo:** sistema de inteligencia artificial que, por su finalidad, contexto de uso, nivel de autonomía, datos utilizados o efectos previsibles, pueda incidir directa o indirectamente en la vida, la integridad personal, la libertad, la privacidad, la igualdad, la identificación de personas, la selección de objetivos, el uso de la fuerza, la conducción de operaciones militares o policiales, o la afectación de población civil.

5. **Control humano significativo:** intervención humana real, informada, oportuna, trazable y jurídicamente responsable sobre las decisiones críticas asociadas al uso de sistemas de inteligencia artificial en defensa y seguridad, especialmente cuando puedan afectar la vida, la integridad personal, la libertad, la población civil, bienes civiles, objetivos militares o el uso de la fuerza.

6. **Decisión crítica no automatizable:** decisión que, por comprometer derechos fundamentales, uso de fuerza, distinción entre civiles y combatientes, proporcionalidad, necesidad, precaución, responsabilidad de mando o legalidad operacional, no puede ser adoptada exclusivamente por un sistema automatizado.

7. **Proveedor privado de inteligencia artificial en defensa y seguridad:** persona natural o jurídica que diseñe, entrene, fabrique, comercialice, importe, exporte, integre, mantenga, actualice, suministre u opere sistemas de inteligencia artificial, datos, modelos, software, hardware, sensores, plataformas o servicios asociados para uso en defensa, Fuerza Pública o actividades estatales de seguridad.

8. **Trazabilidad:** capacidad técnica, documental y operacional de reconstruir el funcionamiento de un sistema de inteligencia artificial, sus entradas, salidas, versiones, parámetros, operadores, autorizaciones, eventos relevantes y cadena de responsabilidad.

9. **Sesgo de automatización:** tendencia de operadores, supervisores o autoridades a aceptar, privilegiar o ejecutar recomendaciones generadas por sistemas automatizados sin evaluación crítica suficiente.

10. **Incidente relevante:** evento en el que el diseño, funcionamiento, despliegue, uso, falla, vulneración, manipulación, sesgo, recomendación o resultado de un sistema de inteligencia artificial cause o pueda causar afectación grave a derechos fundamentales, población civil, bienes civiles, operaciones de la Fuerza Pública, seguridad nacional, Derecho Internacional Humanitario o responsabilidad institucional.

Artículo 4°. ***Principios.*** El diseño, desarrollo, adquisición, prueba, despliegue, supervisión y uso de sistemas de inteligencia artificial en defensa, Fuerza Pública y seguridad se regirá por los siguientes principios:

1. **Dignidad humana:** Ningún sistema de inteligencia artificial podrá ser diseñado, adquirido, desplegado o utilizado de manera que desconozca la condición de la persona humana como sujeto de derechos y no como simple dato, patrón, perfil, objetivo o variable operacional.

2. **Legalidad:** Todo uso de inteligencia artificial en defensa y seguridad deberá tener fundamento constitucional, legal, reglamentario u operacional válido, y deberá ejecutarse dentro de las competencias de la autoridad responsable.

3. **Necesidad:** Solo podrán utilizarse sistemas de inteligencia artificial cuando su empleo responda a una finalidad legítima de defensa, seguridad, protección de derechos, prevención de riesgos, apoyo

operacional o cumplimiento de funciones públicas, y cuando no exista una alternativa menos riesgosa o menos lesiva que permita alcanzar razonablemente la misma finalidad.

4. **Proporcionalidad:** El uso de sistemas de inteligencia artificial deberá guardar relación razonable entre la finalidad perseguida, el nivel de riesgo, el contexto de uso, los derechos comprometidos, el tipo de datos tratados y los efectos previsibles sobre personas, comunidades, población civil, bienes civiles o personal de la Fuerza Pública.

5. **Distinción:** En contextos de conflicto armado, los sistemas de inteligencia artificial asociados directa o indirectamente al uso de la fuerza deberán preservar la obligación de distinguir entre combatientes y población civil, así como entre objetivos militares y bienes civiles.

6. **Precaución:** Las autoridades responsables deberán adoptar medidas previas, concomitantes y posteriores para prevenir, mitigar, corregir o suspender riesgos previsibles derivados del uso de sistemas de inteligencia artificial.

7. **Humanidad:** Ningún sistema de inteligencia artificial podrá ser utilizado de manera que produzca sufrimientos innecesarios, tratos crueles, inhumanos o degradantes, afectaciones indiscriminadas o daños incompatibles con los principios humanitarios aplicables.

8. **Control humano significativo:** Las decisiones críticas asociadas al uso de fuerza, afectación de derechos fundamentales, identificación de personas, selección de objetivos o valoración de proporcionalidad deberán estar sujetas a intervención humana real, informada, oportuna, trazable y jurídicamente responsable.

9. **Responsabilidad de mando:** La intervención de sistemas de inteligencia artificial no exime ni reduce la responsabilidad de los comandantes, directores, superiores jerárquicos, operadores, supervisores, servidores públicos o proveedores que participen en su diseño, autorización, despliegue, operación o supervisión.

10. **Trazabilidad:** Los sistemas de inteligencia artificial de alto riesgo deberán permitir la reconstrucción suficiente de su funcionamiento, datos, versiones, recomendaciones, autorizaciones, operadores, cadena de mando e incidentes relevantes.

11. **Explicabilidad suficiente:** Los sistemas de inteligencia artificial deberán ofrecer, según su nivel de riesgo y contexto de uso, información comprensible para que los operadores y autoridades responsables conozcan sus capacidades, limitaciones, márgenes de error, condiciones de uso y criterios generales de funcionamiento.

12. **Previsibilidad:** No podrán autorizarse sistemas cuyo comportamiento, efectos o riesgos no puedan ser razonablemente anticipados, acotados, supervisados o corregidos por la autoridad responsable.

13. **Seguridad y ciberresiliencia:** Los sistemas deberán contar con medidas técnicas y organizativas para prevenir accesos no autorizados, manipulación adversarial, sabotaje, pérdida de integridad, filtración de datos, fallas críticas o uso por actores no autorizados.

14. **No discriminación:** Los sistemas no podrán diseñarse, entrenarse, adquirirse o utilizarse de manera que generen, reproduzcan o profundicen discriminaciones por razones políticas, étnicas, raciales, territoriales, religiosas, de género, orientación sexual, discapacidad, condición socioeconómica, actividad sindical, periodística, comunitaria, de defensa de derechos humanos o participación en protesta social.

15. **Minimización y protección de datos:** El tratamiento de datos personales, sensibles, biométricos, operacionales o reservados deberá limitarse a lo estrictamente necesario para la finalidad autorizada y deberá sujetarse a los regímenes legales aplicables.

16. **Supervisión institucional:** Los sistemas de inteligencia artificial de alto riesgo estarán sometidos a evaluación, autorización, seguimiento, auditoría y eventual suspensión por parte de las autoridades competentes.

17. **Reserva proporcional:** La reserva por razones de defensa, seguridad nacional, inteligencia, contrainteligencia u orden público deberá aplicarse de manera estricta, necesaria y proporcional, sin impedir los controles judiciales, disciplinarios, fiscales, penales o políticos que correspondan conforme a la Constitución y la ley.

18. **Rendición de cuentas:** Las entidades responsables deberán documentar, evaluar y reportar el uso de sistemas de inteligencia artificial, sus riesgos, incidentes relevantes, medidas correctivas y mecanismos de control, en los términos previstos por esta ley.

19. **Interoperabilidad segura:** La integración de sistemas de inteligencia artificial con armas, sensores, bases de datos, plataformas, sistemas de comunicación o infraestructuras críticas deberá cumplir estándares de seguridad, compatibilidad, control humano y prevención de fallas sistémicas.

20. **Prevención del sesgo de automatización:** Las entidades responsables deberán capacitar a operadores, supervisores y autoridades para evitar la aceptación acrítica de resultados, alertas, perfiles, clasificaciones o recomendaciones generadas por sistemas automatizados.

TÍTULO II.

DECISIONES NO AUTOMATIZABLES Y USOS PROHIBIDOS

Artículo 5°. ***Decisiones no automatizables***. En ningún caso podrán ser adoptadas exclusivamente por sistemas de inteligencia artificial las siguientes decisiones:

1. Autorizar el uso de fuerza letal o potencialmente letal.

2. Determinar que una persona es objetivo militar.

3. Determinar que una persona debe ser capturada, retenida, neutralizada, atacada o sometida al uso de la fuerza.

4. Seleccionar personas como objetivos militares, policiales o de inteligencia.

5. Autorizar bombardeos, ataques aéreos, ataques con drones, ataques con armas explosivas o empleo de armamento letal.

6. Evaluar de manera definitiva la distinción, proporcionalidad, necesidad, precaución o ventaja militar concreta y directa en una operación.

7. Ordenar allanamientos, registros, interceptaciones, capturas o medidas restrictivas de derechos fundamentales.

8. Determinar la participación de una persona en actividades delictivas, hostilidades, protesta social, asociación política, sindical, comunitaria o étnica.

9. Adoptar decisiones sobre personas privadas de la libertad.

10. Imponer sanciones disciplinarias, administrativas o penales.

11. Modificar por sí mismo los parámetros esenciales de misión, selección de objetivos, reglas de enfrentamiento o condiciones de uso de fuerza.

Parágrafo. Los sistemas de inteligencia artificial podrán apoyar la recolección, organización, análisis, visualización o recomendación de información, siempre que la decisión final sea adoptada por una autoridad humana competente, informada y jurídicamente responsable.

Artículo 6°. ***Prohibición absoluta de sistemas de armas autónomas***. Se prohíbe en todo el territorio nacional diseñar, desarrollar, fabricar, producir, entrenar, adquirir, poseer, almacenar, probar operacionalmente, desplegar, transferir, comercializar, importar, exportar, suministrar, financiar, facilitar o usar sistemas de armas autónomas.

Esta prohibición se aplica a actores públicos, privados, mixtos, nacionales, extranjeros, estatales y no estatales.

Parágrafo 1°. Ninguna entidad pública podrá contratar, directa o indirectamente, el diseño, desarrollo, fabricación, entrenamiento, integración, prueba, adquisición, importación, exportación, transferencia, comercialización o uso de sistemas de armas autónomas.

Parágrafo 2°. La prohibición establecida en este artículo no impide la investigación, adquisición o desarrollo de capacidades estrictamente defensivas destinadas a detectar, inhibir, interceptar, bloquear, neutralizar o destruir sistemas de armas autónomas empleados por terceros, siempre que dichas capacidades no permitan la identificación, selección y ataque autónomo de personas u objetivos sin intervención humana.

Artículo 7°. ***Prohibiciones especiales sobre inteligencia artificial y uso de la*** **fuerza.** Queda prohibido:

1. Usar inteligencia artificial para ejecutar autónomamente fuerza letal.

2. Usar inteligencia artificial para identificar, seleccionar o priorizar personas como blancos militares o policiales sin decisión humana competente.

3. Usar inteligencia artificial como única base para ordenar operaciones militares, policiales, de inteligencia o contrainteligencia que afecten derechos fundamentales.

4. Usar inteligencia artificial para vigilancia masiva, indiscriminada o no individualizada de población civil.

5. Usar inteligencia artificial para perfilar personas o grupos por razones políticas, sindicales, étnicas, raciales, religiosas, territoriales, de género, orientación sexual, actividad periodística, defensa de derechos humanos o participación en protesta social.

6. Usar sistemas biométricos o de reconocimiento facial para identificar, rastrear o perfilar participantes en protestas, movilizaciones sociales o reuniones públicas, salvo orden judicial o habilitación legal expresa, individualizada y proporcional.

7. Usar sistemas que no permitan trazabilidad, auditoría, intervención humana o atribución de responsabilidad.

8. Usar sistemas entrenados con datos obtenidos ilegalmente o con bases de datos cuya procedencia no pueda ser verificada.

9. Usar sistemas cuyo comportamiento no pueda ser razonablemente anticipado, limitado, desactivado o supervisado por operadores humanos.

10. Usar inteligencia artificial para ejecutar, activar, detonar o facilitar el uso de armas nucleares, químicas, biológicas o demás armas prohibidas por el derecho internacional.

TÍTULO III.

USOS PERMITIDOS Y SISTEMAS DE ALTO RIESGO

Artículo 8°. ***Usos permitidos de bajo o mediano riesgo***. Se permitirá el uso de sistemas de inteligencia artificial en defensa, Fuerza Pública y seguridad, siempre que no impliquen decisiones críticas no automatizables ni usos prohibidos, para las siguientes finalidades:

1. Logística, inventarios, abastecimiento y mantenimiento predictivo.

2. Gestión documental, traducción, archivo, clasificación administrativa y apoyo jurídico no decisorio.

3. Simulación, entrenamiento, doctrina, planeación académica y juegos de guerra sin efectos operacionales automáticos.

4. Medicina operacional, evacuación, búsqueda y rescate.

5. Desminado humanitario, detección de artefactos explosivos, neutralización de riesgos y protección de personal.

6. Monitoreo meteorológico, geográfico, ambiental, marítimo, fluvial, aéreo o terrestre para fines preventivos.

7. Protección de infraestructura crítica.

8. Ciberdefensa defensiva, detección de anomalías, protección de redes e infraestructura digital.

9. Análisis de fuentes abiertas, siempre que respete derechos fundamentales y no derive en perfilamiento prohibido.

10. Sistemas de apoyo a la decisión que no produzcan efectos automáticos sobre derechos fundamentales, selección de objetivos o uso de fuerza.

Artículo 9°. ***sistemas de alto riesgo.*** se consideran sistemas de alto riesgo, entre otros:

1. Sistemas de identificación, clasificación, seguimiento o priorización de personas, vehículos, instalaciones, objetos o patrones en contextos operacionales.

2. Sistemas de vigilancia aérea, terrestre, marítima, fluvial, satelital, biométrica o cibernética para operaciones militares o policiales.

3. Sistemas predictivos para planeación operacional, anticipación de amenazas o priorización territorial de acciones de seguridad.

4. Sistemas de reconocimiento facial, biométrico, comportamental o de voz.

5. Drones, robots, plataformas no tripuladas, sensores, enjambres o sistemas con autonomía de navegación, seguimiento o selección de rutas.

6. Sistemas semiautónomos asociados directa o indirectamente al uso de fuerza.

7. Sistemas de inteligencia artificial aplicados a inteligencia, contrainteligencia o ciberoperaciones cuando puedan afectar derechos fundamentales.

8. Sistemas que procesen datos sensibles, datos biométricos o datos de población civil.

9. Sistemas que puedan generar recomendaciones sobre selección de objetivos, asignación de riesgo, clasificación de personas o priorización de operaciones.

Artículo 10. ***Autorización estricta de sistemas de alto riesgo.*** El diseño, adquisición, importación, desarrollo, prueba, despliegue, modificación sustancial o uso operacional de sistemas de alto riesgo requerirá autorización previa del Ministerio de Defensa Nacional, conforme a la reglamentación que expida el Gobierno nacional.

Para otorgar la autorización, el Ministerio de Defensa Nacional deberá verificar que el sistema cuente con evaluación jurídica, evaluación técnica y evaluación integral de impacto, en los términos previstos en la presente ley. También deberá constatar que se hayan realizado pruebas realistas en entornos controlados y que exista una definición clara del operador humano responsable, de la cadena de mando y de los parámetros de misión.

La autorización deberá precisar la delimitación temporal, geográfica y funcional del sistema, así como los protocolos de activación, suspensión, desactivación y contingencia. De igual manera, deberá establecer los mecanismos de trazabilidad, auditoría, monitoreo posterior al despliegue y reporte de incidentes que permitan verificar el cumplimiento de esta ley durante todo el ciclo de vida del sistema.

Parágrafo 1°. La autorización de sistemas de alto riesgo no podrá comprender sistemas de armas autónomas ni usos prohibidos por la presente ley.

Parágrafo 2°. La autorización podrá constar en acto administrativo reservado cuando existan razones de defensa o seguridad nacional, sin perjuicio del control judicial, disciplinario, fiscal, penal o político que corresponda conforme a la Constitución y la ley.

Artículo 11. ***Modificación sustancial.*** Se entenderá por modificación sustancial todo cambio en algoritmos, modelos, datos de entrenamiento, fuentes de datos, funciones autónomas, parámetros de misión, entorno operacional, tipo de objetivo, capacidad de identificación, nivel de intervención humana, sistema de armas asociado, proveedor, interoperabilidad o contramedidas previsibles que pueda alterar el nivel de riesgo del sistema.

Toda modificación sustancial requerirá nueva evaluación y autorización previa.

Artículo 12. ***Parámetros mínimos de autorización.*** Toda autorización de sistemas de alto riesgo deberá definir, como mínimo:

1. Finalidad legítima.
2. Entidad responsable.
3. Sistema o tecnología autorizada.
4. Proveedor o desarrollador.
5. Nivel de riesgo.
6. Operador humano responsable.
7. Cadena de mando.
8. Tiempo de autorización.
9. Área geográfica de uso.
10. Ambiente operacional previsto.
11. Población o bienes potencialmente afectados.
12. Funciones automatizadas y funciones reservadas a humanos.
13. Protocolos de intervención humana.
14. Protocolos de desactivación.
15. Condiciones de suspensión inmediata.
16. Reglas de auditoría.
17. Medidas de mitigación de sesgos.

18. Medidas de protección de datos.

19. Pruebas realizadas.

20. Mecanismos de monitoreo posterior al despliegue.

Artículo 13. ***Suspensión preventiva***. El Ministerio de Defensa Nacional deberá suspender preventivamente el uso de un sistema de alto riesgo cuando:

1. Existan indicios de funcionamiento imprevisible.

2. Se presenten incidentes relevantes.

3. Se detecten sesgos discriminatorios no mitigados.

4. El sistema opere por fuera de los parámetros autorizados.

5. No sea posible garantizar control humano significativo.

6. Existan riesgos graves para población civil, derechos fundamentales, Derecho Internacional Humanitario o seguridad nacional.

7. El proveedor o entidad responsable oculte información relevante sobre el sistema.

TÍTULO IV.

GOBERNANZA INSTITUCIONAL

Artículo 14. ***Sistema de gobernanza de inteligencia artificial en defensa y seguridad.*** Créase el Sistema de Gobernanza de Inteligencia Artificial en Defensa y Seguridad como instancia sectorial de coordinación encargada de formular, articular, implementar y hacer seguimiento a las políticas, procedimientos, estándares, registros, evaluaciones, autorizaciones, auditorías y mecanismos de control aplicables al uso de inteligencia artificial en el sector defensa, la Fuerza Pública y las actividades estatales de seguridad.

El Sistema será coordinado por el Ministerio de Defensa Nacional, en el marco de sus competencias constitucionales y legales.

Artículo 15. ***Comité técnico de revisión de inteligencia artificial en defensa y seguridad***. El Ministerio de Defensa Nacional conformará un Comité Técnico de Revisión de Inteligencia Artificial en Defensa y Seguridad, encargado de emitir conceptos técnicos, jurídicos y operacionales para la autorización, seguimiento, suspensión o retiro de sistemas de alto riesgo.

El Comité estará integrado por delegados del Ministerio de Defensa Nacional, las Fuerzas Militares, la Policía Nacional y las entidades del sector defensa que determine la reglamentación.

Podrán ser invitados, con voz, pero sin voto, delegados del Ministerio de Relaciones Exteriores, Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Justicia y del Derecho, Departamento Nacional de Planeación, organismos de control, academia, expertos técnicos, expertos en Derecho Internacional Humanitario, organizaciones humanitarias o entidades públicas especializadas, cuando la naturaleza del sistema lo requiera.

Parágrafo. La participación de invitados estará sujeta a las reglas de reserva, seguridad de la información, confidencialidad y protección de información clasificada.

Artículo 16. ***Funciones del comité técnico.*** El Comité Técnico tendrá las siguientes funciones:

1. Recomendar la clasificación de sistemas de inteligencia artificial según nivel de riesgo.

2. Emitir concepto previo sobre sistemas de alto riesgo.

3. Revisar evaluaciones de impacto.

4. Recomendar autorizaciones, restricciones, suspensiones o retiros.

5. Proponer estándares técnicos mínimos.

6. Recomendar protocolos de prueba, auditoría y monitoreo.

7. Identificar riesgos de sesgo, automatización indebida, ciberseguridad o afectación de derechos.

8. Recomendar medidas de mitigación.

9. Apoyar la elaboración del informe semestral previsto en esta ley.

10. Las demás que defina la reglamentación.

Artículo 17. ***Registro nacional reservado de sistemas de inteligencia artificial en defensa y seguridad.*** Créase el Registro Nacional Reservado de Sistemas de Inteligencia Artificial en Defensa y Seguridad, administrado por el Ministerio de Defensa Nacional.

El Registro deberá contener información suficiente para identificar el sistema, la entidad responsable, el proveedor o desarrollador, la finalidad autorizada, el nivel de riesgo y las funciones automatizadas o semiautomatizadas que incorpore.

También deberá incorporar la información relativa a los datos utilizados, la interoperabilidad con otros sistemas, las autorizaciones otorgadas, el operador humano responsable, la cadena de mando, las pruebas realizadas, las auditorías practicadas, los incidentes relevantes reportados y las decisiones de suspensión, modificación o retiro que se adopten.

Parágrafo 1°. El Registro tendrá carácter reservado, sin perjuicio del acceso de autoridades judiciales, organismos de control y demás autoridades competentes conforme a la Constitución y la ley.

Parágrafo 2°. La información agregada y no sensible del Registro servirá como base para el informe semestral al Congreso del que trata el artículo 24 de la presente Ley.

Artículo 18. ***Evaluación integral de impacto***. La evaluación integral de impacto tendrá por finalidad identificar, valorar y mitigar los riesgos jurídicos, técnicos, operacionales, humanitarios, éticos, cibernéticos y de derechos fundamentales asociados al diseño, adquisición, desarrollo,

prueba, despliegue, modificación sustancial o uso operacional de sistemas de inteligencia artificial de alto riesgo en defensa y seguridad.

La evaluación deberá justificar la finalidad del sistema, su necesidad operacional, su proporcionalidad frente al objetivo perseguido y la existencia de alternativas menos lesivas o menos riesgosas que permitan alcanzar razonablemente la misma finalidad. También deberá valorar los riesgos para los derechos humanos, el Derecho Internacional Humanitario, la población civil, los bienes civiles, la igualdad, la privacidad, la seguridad nacional, la responsabilidad de mando y la atribución de responsabilidad humana.

La entidad responsable deberá examinar la calidad, origen, legalidad, pertinencia y suficiencia de los datos utilizados para el diseño, entrenamiento, validación, prueba o funcionamiento del sistema. Así mismo, deberá valorar el nivel de explicabilidad, previsibilidad, trazabilidad, ciberseguridad, interoperabilidad segura y control humano significativo disponible, así como los riesgos de falla técnica, manipulación adversarial, uso indebido, sesgos discriminatorios, sesgo de automatización o funcionamiento por fuera de los parámetros autorizados.

Cuando el sistema pueda incidir directa o indirectamente en decisiones críticas, la evaluación deberá precisar la forma en que se preservará la intervención humana real, informada, oportuna, trazable y jurídicamente responsable. Para tal efecto, deberá identificar el operador humano responsable, la cadena de mando aplicable, las funciones que permanecerán reservadas a decisión humana y las condiciones bajo las cuales el sistema deberá ser suspendido, desactivado o retirado.

Toda evaluación integral de impacto deberá contener medidas concretas de mitigación, monitoreo posterior al despliegue, revisión periódica y reporte de incidentes relevantes. La autorización del sistema no podrá otorgarse cuando la evaluación evidencie riesgos graves que no puedan ser razonablemente prevenidos, mitigados, supervisados o corregidos por la autoridad responsable.

Artículo 19. ***Revisión jurídica de sistemas asociados al uso de fuerza***. Todo sistema de inteligencia artificial asociado directa o indirectamente al uso de fuerza deberá contar con revisión jurídica previa a su desarrollo, adquisición, importación, prueba, despliegue o modificación sustancial.

La revisión deberá determinar si el sistema puede ser utilizado conforme a la Constitución, la ley, los derechos humanos, el Derecho Internacional Humanitario y las reglas operacionales aplicables.

TÍTULO V.

CONTROL HUMANO, OPERACIÓN Y TRAZABILIDAD

Artículo 20. ***Requisitos del control humano significativo***. Para que exista control humano significativo deberán concurrir, como mínimo, los siguientes elementos:

1. Comprensión suficiente del contexto operacional.
2. Conocimiento de las capacidades y limitaciones del sistema.
3. Información suficiente para adoptar una decisión autónoma frente a la recomendación del sistema.
4. Tiempo razonable para intervenir.
5. Capacidad técnica real de modificar, suspender, cancelar o desactivar la acción del sistema.
6. Identificación clara del operador humano.
7. Identificación de la cadena de mando.
8. Registro verificable de la decisión humana.
9. Responsabilidad jurídica atribuible.

Artículo 21. ***Bitácora obligatoria.*** Todo sistema de alto riesgo deberá contar con una bitácora técnica y operacional que permita reconstruir de manera suficiente su uso, funcionamiento, supervisión y cadena de responsabilidad durante todo su ciclo de vida.

La bitácora deberá registrar, como mínimo, la fecha, hora y lugar de uso del sistema, la entidad responsable, el operador humano, la cadena de mando aplicable, la versión del sistema, los parámetros de misión, los datos o fuentes relevantes utilizados, las recomendaciones generadas, las decisiones humanas adoptadas y las activaciones, suspensiones, modificaciones o desactivaciones realizadas.

Cuando el sistema produzca alertas, fallas, incidentes relevantes, resultados inesperados o recomendaciones que incidan en decisiones críticas, la bitácora deberá conservar la información necesaria para verificar el cumplimiento de los principios, obligaciones y prohibiciones previstos en la presente ley. Esta información deberá permitir identificar si existió control humano significativo, si el sistema operó dentro de los parámetros autorizados y si se adoptaron medidas de mitigación o corrección.

La bitácora tendrá carácter reservado cuando contenga información relacionada con seguridad nacional, defensa, orden público, inteligencia, contrainteligencia, fuentes, métodos, capacidades, vulnerabilidades, planes operacionales o datos personales protegidos. Lo anterior no impedirá su acceso por parte de autoridades judiciales, disciplinarias, fiscales, penales, administrativas, de control fiscal o del Ministerio Público, conforme a sus competencias constitucionales y legales.

El Ministerio de Defensa Nacional definirá los estándares mínimos de conservación, integridad, seguridad, interoperabilidad, acceso, custodia y tiempo de almacenamiento de las bitácoras obligatorias.

Artículo 22. ***Capacitación obligatoria.*** Los operadores, supervisores, comandantes, directores y funcionarios que intervengan en el diseño, autorización, despliegue, supervisión u operación de sistemas de alto riesgo deberán recibir capacitación periódica, suficiente y verificable antes de participar en cualquiera de dichas actividades.

La capacitación deberá abordar el funcionamiento general del sistema, sus capacidades, limitaciones, márgenes de error, condiciones de uso, riesgos previsibles y protocolos de operación. También deberá incluir formación en derechos humanos, Derecho Internacional Humanitario, responsabilidad de mando, protección de datos, reserva de información, ciberseguridad, reporte de incidentes y prevención del sesgo de automatización.

Cuando el sistema pueda incidir directa o indirectamente en decisiones críticas, la capacitación deberá incluir entrenamiento específico sobre control humano significativo, criterios para apartarse de recomendaciones automatizadas, condiciones de suspensión o desactivación del sistema, identificación de fallas, manejo de alertas y obligaciones de registro en la bitácora correspondiente.

La participación en la capacitación y la aprobación de los criterios mínimos definidos por la reglamentación serán condiciones necesarias para operar, supervisar o autorizar sistemas de alto riesgo. El Ministerio de Defensa Nacional establecerá la periodicidad mínima, los contenidos básicos, los mecanismos de evaluación y los soportes documentales que acrediten el cumplimiento de esta obligación.

Artículo 23. ***Interfaz humano-máquina.*** Los sistemas de alto riesgo deberán contar, cuando sea técnicamente posible, con interfaces humano-máquina comprensibles, verificables y adecuadas para que el operador pueda identificar alertas, limitaciones, niveles de confianza, fuentes relevantes, incertidumbre, riesgos y opciones de intervención.

TÍTULO VI.

TRANSPARENCIA, RESERVA Y CONTROL POLÍTICO

Artículo 24. ***Informe semestral al congreso***. El Ministerio de Defensa Nacional presentará semestralmente a las Comisiones Segundas Constitucionales Permanentes de Senado y Cámara de Representantes un informe sobre la implementación de la presente ley.

El informe deberá contener información agregada sobre los sistemas registrados, su clasificación por niveles de riesgo, las autorizaciones otorgadas y negadas, los sistemas suspendidos o retirados, las evaluaciones de impacto realizadas y los incidentes relevantes reportados.

También deberá incluir información agregada sobre las medidas correctivas adoptadas, los avances en capacitación, los desarrollos de investigación, innovación e industria nacional, la contratación pública relacionada con inteligencia artificial en defensa y seguridad, y la cooperación internacional o participación del Estado colombiano en escenarios multilaterales sobre la materia.

Parágrafo 1°. El informe no incluirá información publicada reservada de acuerdo con lo dispuesto en la Ley 1712 de 2014.

Artículo 25. ***Conservación de información y acceso por autoridades competentes***. Las entidades responsables del uso de sistemas de inteligencia artificial de alto riesgo deberán conservar la información técnica, documental y operacional necesaria para verificar el cumplimiento de la presente ley, incluyendo bitácoras, autorizaciones, evaluaciones, auditorías, incidentes relevantes y registros de intervención humana.

Dicha información deberá ser puesta a disposición de las autoridades judiciales, disciplinarias, fiscales, penales, administrativas, de control fiscal o del Ministerio Público que la requieran en ejercicio de sus competencias constitucionales y legales, conforme a los regímenes de reserva, seguridad nacional, defensa, inteligencia, contrainteligencia, protección de datos personales y demás normas aplicables.

Las solicitudes formuladas por particulares se tramitarán conforme al régimen vigente de derecho de petición, acceso a la información pública, protección de datos personales*, habeas data* y demás normas aplicables, sin que la presente ley cree un procedimiento especial de acceso a información reservada o clasificada.

TÍTULO VII

PROVEEDORES PRIVADOS, CONTRATACIÓN E INDUSTRIA MILITAR

Artículo 26. ***Obligaciones de proveedores.*** Los proveedores privados de sistemas de inteligencia artificial en defensa y seguridad deberán:

1. Informar capacidades y limitaciones del sistema.
2. Revelar riesgos conocidos.
3. Garantizar trazabilidad técnica.
4. Permitir auditorías conforme al contrato y la ley.
5. Acreditar la legalidad de los datos utilizados.
6. Adoptar medidas de ciberseguridad.
7. Abstenerse de reutilizar datos estatales para fines no autorizados.
8. Informar fallas, vulnerabilidades o incidentes.
9. Cumplir protocolos de confidencialidad y reserva.
10. Responder por defectos, ocultamientos, incumplimientos o usos no autorizados atribuibles a su conducta.

Artículo 27. ***Cláusulas obligatorias en contratación***. Los contratos estatales para

adquisición, desarrollo, integración, mantenimiento, prueba o despliegue de sistemas de inteligencia artificial en defensa y seguridad deberán incluir cláusulas que garanticen auditoría, trazabilidad, seguridad de la información, protección de datos, confidencialidad y control estatal sobre los datos utilizados o generados en la ejecución contractual.

Dichos contratos deberán establecer de manera expresa la prohibición de usos no autorizados, la obligación de reporte de incidentes, las reglas aplicables a actualizaciones y modificaciones sustanciales, y la responsabilidad del proveedor por defectos, ocultamientos, incumplimientos, vulnerabilidades o usos indebidos atribuibles a su conducta.

Los contratos deberán prever mecanismos de terminación, suspensión o ajuste cuando el sistema genere un riesgo grave para derechos fundamentales, población civil, Derecho Internacional Humanitario, seguridad nacional, reserva de la información, ciberseguridad o cumplimiento de la presente ley.

En todos los contratos deberá incorporarse una prohibición expresa de desarrollar, suministrar, integrar, entrenar, adaptar, comercializar o facilitar sistemas de armas autónomas.

Artículo 28. ***Prohibición de sistemas no auditables***. No podrán contratarse, adquirirse, importarse, desplegarse o usarse sistemas de alto riesgo que, por su diseño, condiciones contractuales, restricciones técnicas o secreto comercial, impidan la auditoría suficiente por parte del Estado colombiano.

La protección de secretos industriales o información propietaria no podrá impedir la verificación estatal del cumplimiento de la Constitución, la ley, los derechos humanos, el Derecho Internacional Humanitario y las condiciones de autorización.

Artículo 29. ***Rol de la industria militar***. La industria militar estatal podrá desarrollar, adaptar, integrar, probar y transferir sistemas de inteligencia artificial para fines lícitos, defensivos, humanitarios, logísticos, preventivos, de ciberdefensa, protección de infraestructura crítica, desminado, búsqueda y rescate, entrenamiento, simulación, protección de la Fuerza Pública y reducción de riesgos para la población civil.

En ningún caso la industria militar estatal podrá desarrollar, fabricar, adquirir, transferir, comercializar, exportar, importar o desplegar sistemas de armas autónomas.

Parágrafo. El Gobierno nacional promoverá el desarrollo de capacidades nacionales de inteligencia artificial responsable en defensa y seguridad, con el fin de reducir dependencia tecnológica, fortalecer la soberanía digital y garantizar control estatal sobre tecnologías críticas.

TÍTULO VIII.

IMPORTACIÓN, EXPORTACIÓN, TRANSFERENCIA Y TECNOLOGÍAS DE USO DUAL

Artículo 30. ***Tecnologías prohibidas***. Se prohíbe la importación, exportación, transferencia, comercialización, intermediación o suministro de:

1. Sistemas de armas autónomas.

2. Componentes diseñados principalmente para permitir identificación, selección y ataque autónomo sin intervención humana.

3. Sistemas que permitan modificación autónoma de parámetros de ataque sin intervención humana.

4. Sistemas asociados a uso de fuerza que no cuenten con mecanismo de desactivación humana.

5. Sistemas destinados a actores armados no estatales, estructuras criminales o personas no autorizadas para el uso de armas o tecnologías de defensa.

Artículo 31. ***Tecnologías controladas***. Estarán sujetas a autorización previa del Gobierno nacional, conforme a la reglamentación, las operaciones de importación, exportación, transferencia o comercialización de:

1. Sistemas semiautónomos asociados al uso de fuerza.

2. Drones, robots, sensores, enjambres o plataformas autónomas de uso operacional.

3. Sistemas biométricos destinados a defensa, seguridad o policía.

4. Sistemas predictivos para inteligencia, contrainteligencia, seguridad o operaciones.

5. Software de selección, seguimiento o priorización de objetivos.

6. Sistemas de ciberoperaciones con funciones autónomas.

7. Componentes de uso dual que puedan integrarse a sistemas de armas autónomas o semiautónomas.

Artículo 32. ***Certificado de usuario final***. Toda operación de importación, exportación, transferencia o comercialización de tecnologías controladas deberá contar, cuando corresponda, con certificado de usuario final y evaluación de riesgo sobre derechos humanos, Derecho Internacional Humanitario, seguridad nacional, proliferación y desvío a actores no autorizados.

TÍTULO IX

RESPONSABILIDAD, INCIDENTES Y SANCIONES

Artículo 33. ***Responsabilidad humana.*** La responsabilidad por el diseño, autorización, despliegue, operación, supervisión y uso de sistemas de inteligencia artificial en defensa y seguridad corresponderá siempre a personas naturales o jurídicas determinadas, conforme a la Constitución y la ley.

La responsabilidad no podrá trasladarse, diluirse o extinguirse por la intervención de sistemas automatizados, modelos algorítmicos o inteligencia artificial.

Artículo 34. ***Responsabilidad de mando***. Los comandantes, directores, superiores jerárquicos y autoridades que autoricen, desplieguen, supervisen u ordenen el uso de sistemas de inteligencia artificial

en defensa y seguridad responderán conforme a la Constitución, la ley, el Derecho Internacional Humanitario, el régimen disciplinario, el régimen penal y los demás regímenes aplicables.

Artículo 35. ***Reporte de incidentes relevantes.*** Toda entidad que use sistemas de alto riesgo deberá reportar al Ministerio de Defensa Nacional los incidentes relevantes dentro del término que establezca la reglamentación.

Cuando el incidente pueda constituir falta disciplinaria, delito, violación de derechos humanos, infracción al Derecho Internacional Humanitario, daño antijurídico, detrimento patrimonial o riesgo grave para la población civil, deberá darse traslado a la autoridad competente.

Artículo 36. ***Sanciones contractuales y administrativas***.

El incumplimiento de las obligaciones establecidas en esta ley por parte de proveedores podrá dar lugar, según corresponda, a:

1. Suspensión del contrato.
2. Terminación del contrato.
3. Declaratoria de incumplimiento.
4. Multas y cláusula penal.
5. Reporte a autoridades competentes.
6. Inhabilidad para contratar en los términos de la ley.
7. Retiro del registro de proveedores, si este fuere creado por la reglamentación.
8. Las demás consecuencias previstas en el contrato y en la normativa aplicable.

Artículo 37. Modifíquese el Artículo 367 de la Ley 599 de 2000, el cual quedará así:

Artículo 367. ***Fabricación, importación, tráfico, posesión y uso de armas químicas, biológicas, nucleares y armas autónomas.*** El que importe, trafique, fabrique, almacene, conserve, adquiera, suministre, use o porte armas químicas, biológicas, nucleares o sistemas de armas autónomas, incurrirá en prisión de noventa y seis (96) a ciento ochenta (180) meses y multa de ciento treinta y tres punto treinta y tres (133.33) a treinta mil (30.000) salarios mínimos legales mensuales vigentes.

La pena se aumentará hasta la mitad si se utiliza la ingeniería genética para producir armas biológicas o exterminadoras de la especie humana.

TÍTULO X

DISPOSICIONES FINALES

Artículo 38. ***Reglamentación.*** El Gobierno nacional, a través del Ministerio de Defensa Nacional y en coordinación con las entidades competentes, reglamentará la presente ley dentro de los doce (12) meses siguientes a su promulgación.

La reglamentación deberá desarrollar los criterios para clasificar los sistemas de inteligencia artificial por nivel de riesgo, el procedimiento de autorización de sistemas de alto riesgo, el funcionamiento del Comité Técnico de Revisión y las reglas de operación del Registro Nacional Reservado.

También deberá regular las evaluaciones de impacto, los protocolos de auditoría, los mecanismos de reporte de incidentes, el contenido mínimo del informe semestral al Congreso y las condiciones para la contratación estatal de sistemas de inteligencia artificial en defensa y seguridad.

La reglamentación deberá establecer los controles aplicables a tecnologías de uso dual, los procedimientos de transición para sistemas en operación o contratación y las demás disposiciones necesarias para garantizar la implementación gradual, segura y verificable de las obligaciones previstas en esta ley.

Parágrafo. Las prohibiciones establecidas en esta ley serán exigibles desde su promulgación y su cumplimiento no estará condicionado a la expedición de la reglamentación. El plazo para reglamentar y los procedimientos de transición no podrán interpretarse como autorización para iniciar, continuar o reanudar actividades o usos prohibidos, ni podrán emplearse para establecer excepciones a dichas prohibiciones.

Artículo 39. ***Inventario inicial.*** Dentro de los seis (6) meses siguientes a la expedición de la reglamentación, las entidades sujetas a la presente ley deberán remitir al Ministerio de Defensa Nacional un inventario reservado de los sistemas de inteligencia artificial en defensa, Fuerza Pública y seguridad que se encuentren en diseño, adquisición, prueba, operación o contratación.

El inventario deberá identificar los sistemas y usos comprendidos en las prohibiciones de esta ley y registrar las medidas adoptadas para hacerlas efectivas, incluyendo el cese de actividades, la desactivación, el retiro del servicio y las actuaciones contractuales correspondientes, según resulte aplicable.

Artículo 40. ***Transición.*** Los sistemas de alto riesgo que se encuentren en operación al momento de entrada en vigencia de la reglamentación deberán ser evaluados dentro de los doce (12) meses siguientes, con el fin de determinar su conformidad con esta ley y adoptar las decisiones de autorización, adecuación, suspensión o retiro que correspondan.

Desde la promulgación de la presente ley deberán cesar las actividades y usos prohibidos. Las entidades y personas responsables deberán impedir su continuidad y adoptar las medidas de desactivación y retiro del servicio que correspondan, de manera segura y sin perjuicio de la preservación de la información y de los elementos de prueba requeridos por las autoridades competentes.

Cuando un sistema de alto riesgo no permita garantizar las condiciones mínimas de control humano significativo, trazabilidad, seguridad o legalidad exigidas por esta ley, su uso deberá suspenderse de inmediato, sin esperar a la expedición de la reglamentación ni al vencimiento del plazo de evaluación.

Su operación solo podrá reanudarse cuando se acredite el cumplimiento de dichas condiciones y se obtengan las autorizaciones legalmente exigibles, siempre que no corresponda a un sistema o uso prohibido.

Parágrafo. La existencia de contratos, convenios, autorizaciones, pruebas o proyectos iniciados antes de la promulgación de esta ley no habilitará la continuación de actividades o usos prohibidos. Las entidades competentes adoptarán las medidas contractuales y administrativas necesarias para hacer efectivas las prohibiciones, con observancia del debido proceso y de los regímenes aplicables.

Artículo 41. ***Impacto fiscal***. La implementación de la presente ley se atenderá con cargo a las apropiaciones presupuestales existentes de las entidades competentes, de conformidad con el Marco Fiscal de Mediano Plazo, el Marco de Gasto de Mediano Plazo y las normas orgánicas de presupuesto.

Artículo 42. ***Vigencia y derogatorias.*** La presente ley rige a partir de su promulgación y deroga las disposiciones que le sean contrarias.

DAVID ALEJANDRO TORO RAMÍREZ
Representante a la Cámara
Pacto Histórico

EXPOSICIÓN DE MOTIVOS

PROYECTO DE LEY NÚMERO 366 DE 2026 CÁMARA

por medio de la cual se regula el uso de inteligencia artificial en el sector defensa y se dictan otras disposiciones.

Con el fin de realizar la exposición de motivos del presente Proyecto de Ley, este acápite se divide en las siguientes partes: (1) objeto del proyecto de Ley, (2) antecedentes, (3) marco constitucional, legal y de competencia legislativa, (4) justificación del proyecto, (5) estándares internacionales y derecho comparado, (6) descripción del articulado, (7) impacto fiscal, (8) conflicto de interés, y (9) consideraciones finales.

I. Objeto del proyecto de ley

El presente proyecto de ley tiene por objeto establecer un marco jurídico para el uso de inteligencia artificial en el sector defensa, la Fuerza Pública y las actividades estatales de seguridad, bajo criterios de control humano significativo, respeto por los derechos humanos, cumplimiento del Derecho Internacional Humanitario, responsabilidad de mando, trazabilidad, supervisión institucional y reserva compatible con la seguridad nacional.

La iniciativa retoma como antecedente el Proyecto de Ley número 368 de 2025 Cámara, cuyo objeto era prohibir el uso de sistemas de armas autónomas letales en el territorio nacional y establecer un marco estricto para sistemas semiautónomos letales en el sector defensa. La presente propuesta amplía ese alcance: la prohibición comprende los sistemas de armas autónomas definidos en el artículo 3, con independencia de que empleen fuerza letal o no letal, y se integra en una regulación sectorial más amplia sobre inteligencia artificial en defensa y seguridad.

La autonomía en el empleo de armas plantea un problema que no depende exclusivamente de la posibilidad de causar la muerte. También compromete la integridad y la libertad de las personas, la protección de bienes y la atribución de responsabilidad por el uso de la fuerza. A su vez, los riesgos de la inteligencia artificial en defensa y seguridad se extienden a la vigilancia, la inteligencia, la ciberdefensa, el análisis predictivo y los sistemas de apoyo a decisiones operacionales, aunque esas aplicaciones no constituyan sistemas de armas.

Por esa razón, el proyecto establece una prohibición absoluta de los sistemas de armas autónomas, comprendidos los que empleen fuerza letal o no letal contra personas u objetos. Para los sistemas de inteligencia artificial de alto riesgo que no se encuentren prohibidos, dispone un régimen de autorización estricta, evaluación, registro, auditoría, seguimiento, trazabilidad y responsabilidad. La definición del artículo 3° delimita la categoría prohibida a partir de sus funciones y de la ausencia de una decisión humana previa, específica e informada sobre el objetivo concreto o grupo específico de objetivos, el empleo de la fuerza y el momento del ataque.

La finalidad no es impedir que el Estado colombiano desarrolle capacidades tecnológicas para su defensa legítima. Por el contrario, la finalidad es asegurar que la modernización tecnológica de la Fuerza Pública ocurra dentro de límites constitucionales, humanitarios y democráticos. La inteligencia artificial puede fortalecer capacidades logísticas, preventivas, defensivas, humanitarias, de ciberseguridad, búsqueda y rescate, desminado, protección de infraestructura crítica y reducción de riesgos para la población civil. Lo que no puede permitirse es que decisiones de vida, muerte, captura, vigilancia masiva, perfilamiento o uso de fuerza queden entregadas a sistemas automatizados sin control humano real.

II. Antecedentes

El Proyecto de Ley número 368 de 2025 Cámara fue radicado el 24 de septiembre de 2025 por los representantes David Alejandro Toro Ramírez, Carmen Felisa Boscán Ramírez, David Ricardo Racero Mayorca, Erick Adrián Velasco Burbano, Gabriel Becerra Yáñez, Gabriel Ernesto Parrado Durán, Ingrid Johana Aguirre Juvinao, John Jairo González Agudelo y Norman David Bañol Álvarez, y fue publicado en la ***Gaceta del Congreso*** número 1846 de 2025. Posteriormente, el 22 de octubre de 2025, la Secretaría de la Comisión Segunda de la

Cámara designó como ponentes a los representantes David Alejandro Toro Ramírez, en calidad de coordinador, y Elizabeth Jay-Pang Díaz.

Dicho proyecto retomó una iniciativa radicada en la legislatura 2024-2025, identificada como Proyecto de Ley número 436 de 2024 Cámara, que fue archivada conforme a lo dispuesto en el artículo 190 de la Ley 5ª de 1992. En el marco de la construcción del PL 368 de 2025 se realizó una mesa técnica el 20 de marzo de 2025 con participación del Ministerio de Defensa Nacional, el Ministerio de Relaciones Exteriores, académicos y otros actores, con el propósito de fortalecer la iniciativa y revisar su alcance normativo.

La mencionada iniciativa legislativa identificó como ejes sustantivos la prohibición de sistemas de armas autónomas letales, el registro y control de sistemas semiautónomos letales, la responsabilidad de operadores, supervisores, desarrolladores y comandantes, y la necesidad de reglamentación por parte del Gobierno nacional.

La audiencia pública realizada el 28 de abril de 2026 en la Comisión Segunda de la Cámara permitió ampliar el alcance del debate. Allí se planteó que la discusión no podía limitarse a una categoría específica de armas, sino que debía abordarse como una transformación profunda en la forma como se ejerce la fuerza, se integran sistemas de información, se utilizan tecnologías emergentes y se delegan funciones críticas en entornos operacionales.

En dicha audiencia, el Ministerio de Defensa Nacional sostuvo que Colombia necesita regular la prohibición de sistemas de armas autónomas letales y el uso de sistemas semiautónomos en defensa y seguridad nacional, subrayando que estos sistemas no son ciencia ficción, sino una realidad operacional documentada en conflictos recientes. También se advirtió que el Derecho Internacional Humanitario impone obligaciones como distinción, proporcionalidad y precaución, las cuales exigen juicio humano contextual, ético y dinámico.

El debate permitió identificar tres necesidades adicionales que justifican esta nueva propuesta: (i) precisar el concepto de control humano significativo; (ii) regular los sistemas de alto riesgo que no son armas autónomas, pero pueden afectar derechos fundamentales, población civil o decisiones operacionales; y (iii) incorporar reglas sobre proveedores privados, tecnologías de uso dual, industria militar, auditoría, trazabilidad e informes al Congreso.

III. Marco Constitucional, Legal y de Competencia Legislativa

La Constitución Política ofrece el fundamento para una regulación sectorial del uso de inteligencia artificial en defensa y seguridad. El artículo 1° establece que Colombia es un Estado social de derecho fundado en el respeto de la dignidad humana. Este principio impide que una persona sea reducida a una variable estadística, a un perfil de riesgo o a un objetivo definido exclusivamente por un sistema automatizado.

El artículo 2° dispone que son fines esenciales del Estado servir a la comunidad, garantizar la efectividad de los derechos, defender la independencia nacional, mantener la integridad territorial, asegurar la convivencia pacífica y proteger a todas las personas residentes en Colombia en su vida, honra, bienes, creencias y demás derechos y libertades. La defensa y la seguridad son funciones constitucionales legítimas; sin embargo, deben ejercerse dentro de un orden jurídico que preserve la vida, la libertad, la igualdad, el debido proceso, la intimidad y la paz.

El artículo 6° establece que los particulares son responsables ante las autoridades por infringir la Constitución y las leyes, y que los servidores públicos lo son por la misma causa y por omisión o extralimitación en el ejercicio de sus funciones. Esta regla es esencial en materia de inteligencia artificial: la intervención de sistemas automatizados no puede diluir la responsabilidad de servidores públicos, comandantes, operadores, supervisores, desarrolladores, proveedores o entidades responsables.

El artículo 11 consagra la inviolabilidad del derecho a la vida y prohíbe la pena de muerte. El artículo 12 prohíbe la desaparición forzada, la tortura y los tratos o penas crueles, inhumanos o degradantes. El artículo 13 protege la igualdad y prohíbe la discriminación. El artículo 15 protege la intimidad, el buen nombre, el habeas data y las garantías aplicables al tratamiento de datos. El artículo 20 protege la libertad de expresión e información. El artículo 22 reconoce la paz como derecho y deber de obligatorio cumplimiento. El artículo 29 garantiza el debido proceso. Estas normas justifican que el Estado trace límites frente al uso de inteligencia artificial cuando pueda incidir en decisiones de fuerza, vigilancia, perfilamiento, captura, clasificación o afectación de derechos.

El artículo 93 incorpora el bloque de constitucionalidad en materia de derechos humanos y Derecho Internacional Humanitario. Esta disposición es central porque los sistemas de inteligencia artificial asociados al uso de la fuerza deben interpretarse conforme a las obligaciones internacionales de Colombia, en especial los principios de humanidad, distinción, proporcionalidad y precaución.

El artículo 114 atribuye al Congreso la función de reformar la Constitución, hacer las leyes y ejercer control político sobre el Gobierno y la administración. El artículo 150 le confiere al Congreso la competencia general para expedir códigos y leyes en todos los ramos de la legislación, así como para regular materias de orden público cuando corresponda dentro de sus competencias. En desarrollo de estas normas, la presente iniciativa establece un marco general de límites, prohibiciones, autorizaciones estrictas y responsabilidades frente al uso de inteligencia artificial en defensa y seguridad.

El artículo 189 reconoce al Presidente de la República como Jefe de Estado, Jefe de Gobierno, Suprema Autoridad Administrativa y Comandante Supremo de las Fuerzas Armadas. En particular, le corresponde dirigir la Fuerza Pública, conservar el orden público y dirigir las operaciones de guerra cuando lo estime conveniente. Por ello, el proyecto no confiere al Congreso facultades de autorización, certificación o conducción operacional. El Congreso ejerce su función legislativa y de control político, mientras que el Gobierno nacional, a través del Ministerio de Defensa Nacional y las autoridades competentes, conserva la dirección constitucional de la seguridad nacional y de la Fuerza Pública.

Los artículos 217 y 218 regulan las Fuerzas Militares y la Policía Nacional. Las Fuerzas Militares tienen como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional. La Policía Nacional tiene como fin primordial el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes convivan en paz. Ambos mandatos son compatibles con una regulación que permita innovación tecnológica, pero impida delegar en máquinas decisiones críticas que comprometan derechos, población civil o uso de fuerza.

En materia penal, el proyecto modifica el artículo 367 de la Ley 599 de 2000 para incorporar los sistemas de armas autónomas al régimen de armas prohibidas. La denominación empleada remite a la definición del artículo 3° de esta ley y comprende los sistemas que utilicen fuerza letal o no letal. La consecuencia penal se circunscribe a las conductas descritas en el tipo y se aplica conforme a los principios de legalidad, culpabilidad y debido proceso; la existencia de un sistema automatizado no sustituye la determinación de la responsabilidad individual.

IV. Justificación del Proyecto

La inteligencia artificial es una tecnología de propósito general con capacidad de transformar actividades civiles, económicas, institucionales, militares y de seguridad. En el ámbito de defensa, puede mejorar la logística, el mantenimiento predictivo, la protección de infraestructura crítica, la ciberdefensa, el análisis de información, la simulación, el entrenamiento, la búsqueda y rescate, el desminado y la protección de la Fuerza Pública. No obstante, también puede intensificar riesgos de automatización del uso de la fuerza, opacidad, sesgos, vigilancia masiva, escalamiento militar, errores de identificación, debilitamiento de la responsabilidad humana y afectación de población civil.

La regulación propuesta permite el desarrollo de inteligencia artificial en defensa dentro de límites definidos por la protección de las personas y el control humano sobre el uso de la fuerza. La prohibición de sistemas de armas autónomas se fundamenta en la decisión de impedir que la identificación, selección y ataque de objetivos queden en manos de un sistema sin una decisión humana previa, específica e informada, en los términos del artículo 3°. El mismo criterio se aplica cuando la fuerza empleada se presenta como no letal: la ausencia de un resultado mortal no elimina la afectación posible de la integridad, la libertad o los bienes, ni resuelve el problema de quién decide ejercer esa fuerza.

La decisión humana exigida debe recaer sobre objetivos concretos y sobre el empleo de la fuerza, incluido el momento del ataque. El control humano significativo permite valorar el contexto y las condiciones jurídicas de la operación, y evita que una autorización general de misión sea tratada como una decisión suficiente sobre personas u objetos que el sistema seleccione posteriormente. La prohibición se acompaña de límites al uso de inteligencia artificial para vigilancia masiva, perfilamiento y decisiones críticas que afecten derechos fundamentales.

El documento A/79/88 presentado por el Secretario General de las Naciones Unidas sobre sistemas de armas autónomas letales señala que la tecnología para que un arma rastree, seleccione y ataque un objetivo de forma autónoma después de su activación, sin intervención humana adicional, ya existe. También advierte que las capacidades autónomas y habilitadas por inteligencia artificial ya están presentes en campos de batalla contemporáneos, generando preocupaciones jurídicas, éticas y de seguridad. Esa realidad exige que la regulación no espere a que el daño sea irreversible.

El mismo documento subraya que el control humano se ha consolidado como un componente necesario para la dimensión ética, de seguridad y de cumplimiento jurídico de los sistemas autónomos, especialmente en relación con el Derecho Internacional Humanitario. Sin embargo, también advierte que no existe claridad suficiente sobre qué significa control humano, cómo se materializa y qué nivel resulta suficiente. Este proyecto responde a esa brecha al definir el control humano significativo y establecer requisitos mínimos de comprensión del contexto, conocimiento de capacidades y limitaciones del sistema, información suficiente, tiempo razonable para intervenir, capacidad de modificar o desactivar el sistema, operador identificable, cadena de mando y responsabilidad jurídica atribuible.

El riesgo no consiste únicamente en que una máquina dispare. También puede aparecer cuando sistemas de inteligencia artificial producen perfiles, alertas, priorizaciones, predicciones o recomendaciones que las autoridades aceptan de manera acrítica. Ese fenómeno, conocido como sesgo de automatización, puede llevar a que una decisión formalmente humana sea materialmente determinada por el sistema. De ahí la necesidad de capacitar operadores, exigir trazabilidad, evaluar sesgos, conservar bitácoras y preservar responsabilidad humana.

La regulación también se justifica por la expansión de tecnologías de uso dual. Drones, sensores, sistemas de visión por computador, modelos de reconocimiento, software de navegación autónoma, capacidades de análisis predictivo y herramientas de ciberseguridad pueden tener usos civiles, humanitarios o defensivos; pero también pueden ser integrados a operaciones militares o policiales de alto riesgo. Por ello, el proyecto diferencia entre usos permitidos, sistemas de alto riesgo y tecnologías prohibidas.

El proyecto también reconoce la importancia de la industria militar estatal y de las capacidades nacionales. Colombia no debe quedar rezagada en el desarrollo de inteligencia artificial responsable para fines defensivos, humanitarios, logísticos, preventivos, de ciberdefensa, desminado, búsqueda y rescate o protección de infraestructura crítica. Sin embargo, esa agenda de soberanía tecnológica debe tener una frontera infranqueable: la industria militar estatal no podrá desarrollar, fabricar, adquirir, transferir, comercializar, exportar, importar o desplegar sistemas de armas autónomas.

La prohibición del reconocimiento biométrico o facial para identificar, rastrear o perfilar participantes en protestas, salvo orden judicial o habilitación legal expresa, individualizada y proporcional, responde a la necesidad de proteger el ejercicio democrático de la protesta social, la libertad de expresión y la participación política. El proyecto no crea un procedimiento especial de protección de derechos, sino que establece un límite sectorial al uso de tecnologías de vigilancia por razones de defensa y seguridad.

La propuesta diferencia la prohibición de sistemas de armas autónomas de la regulación de otras aplicaciones de inteligencia artificial. Las capacidades logísticas, humanitarias, de entrenamiento, búsqueda y rescate, protección de infraestructura y ciberdefensa podrán desarrollarse dentro de las condiciones previstas en el articulado. La finalidad defensiva de una tecnología no constituye, por sí sola, una excepción a la prohibición: las capacidades destinadas a enfrentar sistemas empleados por terceros deben respetar los límites del artículo 6 y el control humano significativo exigido por la ley.

La aplicación inmediata de las prohibiciones es necesaria para que los plazos de implementación no se conviertan en un período de tolerancia de las conductas que la ley excluye. Por ello, los artículos 38 a 40 separan la reglamentación, el inventario y la evaluación de sistemas de la obligación de cesar las actividades prohibidas desde la promulgación. La suspensión de sistemas que no garanticen las condiciones mínimas de control humano, trazabilidad, seguridad o legalidad tampoco queda aplazada por esos plazos.

V. Estándares Internacionales, Derecho Comparado y Líneas Rojas de IA

El documento CCW/GGE.1/2026/CRP.1/Rev.1, de 3 de septiembre de 2026, sirve como referente de la discusión del Grupo de Expertos Gubernamentales de la Convención sobre Ciertas Armas Convencionales. Su párrafo 25 caracteriza los sistemas a partir de la identificación, selección y ataque sin intervención humana. Aclara que programar posibles objetivos no los excluye y distingue esa programación de la determinación humana de objetivos específicos y del momento del ataque. También comprende empleos que causen lesiones o daños materiales sin muerte (GGE, 2026, párr. 25).

La revisión reafirma la aplicación del Derecho Internacional Humanitario y la responsabilidad humana. Combina prohibiciones de determinados sistemas y usos con medidas de control sobre los demás; contempla control directo o indirecto y medidas anteriores o simultáneas al empleo. No establece una prohibición general de toda la categoría ni constituye, por sí misma, un tratado vinculante (GGE, 2026, párrs. 26-46).

El proyecto colombiano adopta una decisión legislativa más estricta: prohíbe todos los sistemas comprendidos en su definición de armas autónomas, con independencia de la letalidad de la fuerza. Esta opción se sustenta en los fines constitucionales de protección de la vida, la integridad, la libertad y la dignidad humana y en la preservación de una decisión humana jurídicamente responsable sobre el empleo de la fuerza. El referente internacional orienta la caracterización y las salvaguardas, pero no se invoca como fuente de una obligación internacional de prohibición absoluta. La regulación de los sistemas de alto riesgo recae sobre tecnologías y usos que no estén comprendidos en las prohibiciones de la ley.

El AI Guardrails Act presentado por la Senadora Elissa Slotkin en el Senado de Estados Unidos en el presente año constituye un antecedente comparado relevante porque reconoce que la inteligencia artificial militar requiere límites específicos. Ese proyecto prohíbe al Departamento de Defensa usar IA para ejecutar el lanzamiento o detonación de armas nucleares; para monitorear, rastrear, perfilar o seleccionar individuos o grupos sin base legal individualizada y articulable; y para emplear fuerza letal mediante sistemas de armas autónomas sin niveles apropiados de juicio y supervisión humana.

Aunque su diseño institucional no se traslada mecánicamente a Colombia, confirma que la discusión regulatoria debe ir más allá de las armas autónomas y abarcar vigilancia, perfilamiento, fuerza letal y sistemas de alto riesgo.

La discusión internacional sobre líneas rojas de inteligencia artificial también respalda la necesidad del proyecto. The Future Society define las líneas rojas como límites claros y exigibles que los sistemas de IA no deben cruzar para proteger al público frente a daños graves e irreversibles. Según

esa organización, los principios vagos, las guías voluntarias y las buenas prácticas sugeridas no son suficientes cuando se trata de riesgos inaceptables; se requieren límites duros.

En la Athens Roundtable de 2025, expertos convocados por The Future Society identificaron clusters de riesgo asociados a manipulación a gran escala, amenazas químicas, biológicas, radiológicas y nucleares, capacidades ciberofensivas, control autónomo de infraestructura crítica, armas autónomas letales, escalamiento y riesgos para derechos humanos y justicia. Los participantes resaltaron la necesidad de traducir normas generales en umbrales técnicos verificables, mecanismos de cumplimiento y estándares multilaterales apoyados en el derecho internacional existente.

En 2026, el taller de The Future Society y CeSIA en la conferencia IASEAI señaló que las líneas rojas exigibles requieren tres condiciones: acuerdo sobre umbrales, infraestructura de verificación y construcción de coaliciones diplomáticas. El mismo reporte identificó consenso técnico y político sobre capacidades especialmente peligrosas, incluyendo amenazas CBRN, vigilancia masiva habilitada por IA y pérdida de control sobre sistemas avanzados.

La OCDE ha señalado que, sin líneas rojas claras y exigibles que prohíban usos o comportamientos inaceptables de sistemas de IA, los daños pueden volverse amplios, irreversibles y desestabilizadores. Su análisis define las líneas rojas como prohibiciones no negociables frente a usos o comportamientos considerados demasiado peligrosos, de alto riesgo o éticamente inadmisibles, e incluye como ejemplos los sistemas de armas autónomas letales, la vigilancia masiva en espacios públicos y la operación de infraestructura crítica sin supervisión humana.

La OTAN, en su estrategia revisada de inteligencia artificial, reconoce principios de uso responsable en defensa como legalidad, responsabilidad y rendición de cuentas, explicabilidad y trazabilidad, confiabilidad, gobernabilidad y mitigación de sesgos. Estos estándares son compatibles con el articulado propuesto, que exige autorización previa de sistemas de alto riesgo, bitácoras, evaluaciones de impacto, revisión jurídica, capacitación, auditoría y mecanismos de suspensión.

El Departamento de Defensa de Estados Unidos también ha desarrollado una estrategia de inteligencia artificial responsable orientada a construir sistemas robustos, resilientes y confiables, e incorporar criterios éticos desde el diseño, desarrollo, adquisición, despliegue y uso. Aunque Colombia debe construir su propio marco conforme a su Constitución, estos antecedentes muestran que la regulación de IA en defensa se está convirtiendo en un estándar de gobernanza democrática y seguridad internacional.

VI. Descripción del Proyecto

El proyecto se compone de cuarenta y dos (42) artículos organizados en diez títulos.

El Título I contiene las disposiciones generales: objeto, ámbito de aplicación, definiciones y principios. La definición de sistemas de armas autónomas comprende fuerza letal y no letal contra personas u objetos, y exige una decisión humana previa, específica e informada sobre los objetivos concretos, el empleo de fuerza y el momento del ataque para delimitar la categoría prohibida.

El Título II establece las decisiones no automatizables y los usos prohibidos. Allí se prohíbe de manera absoluta diseñar, desarrollar, fabricar, producir, entrenar, adquirir, poseer, almacenar, probar operacionalmente, desplegar, transferir, comercializar, importar, exportar, suministrar, financiar, facilitar o usar sistemas de armas autónomas. También se prohíben usos especiales de IA asociados a fuerza letal autónoma, vigilancia masiva, perfilamiento discriminatorio, uso de datos ilegales, sistemas no trazables y automatización de armas prohibidas por el derecho internacional.

El Título III regula los usos permitidos y los sistemas de alto riesgo. Distingue entre usos lícitos de bajo o mediano riesgo, como logística, mantenimiento predictivo, entrenamiento, búsqueda y rescate, desminado, protección de infraestructura y ciberdefensa defensiva, y sistemas de alto riesgo que requieren autorización estricta del Ministerio de Defensa Nacional.

El Título IV crea el Sistema de Gobernanza de Inteligencia Artificial en Defensa y Seguridad como instancia sectorial de coordinación, establece el Comité Técnico de Revisión, define sus funciones, crea el Registro Nacional Reservado de Sistemas de IA en Defensa y Seguridad, regula la evaluación de impacto y exige revisión jurídica de sistemas asociados al uso de fuerza.

El Título V desarrolla reglas de control humano, operación y trazabilidad. Exige requisitos mínimos para el control humano significativo, bitácora obligatoria, capacitación de operadores y supervisores, e interfaces humano-máquina comprensibles cuando sea técnicamente posible.

El Título VI regula transparencia, reserva y control político. Prevé informes semestrales al Congreso y conservación de información para acceso por autoridades competentes, sin crear un procedimiento especial de acceso a información reservada o clasificada.

El Título VII regula proveedores privados, contratación e industria militar. Establece obligaciones de proveedores, cláusulas obligatorias en contratos, prohibición de sistemas no auditables y reglas sobre el rol de la industria militar estatal.

El Título VIII regula importación, exportación, transferencia y tecnologías de uso dual. Distingue entre tecnologías prohibidas y tecnologías controladas sujetas a autorización previa y certificado de usuario final.

El Título IX desarrolla responsabilidad, incidentes y sanciones. Contiene reglas de responsabilidad humana, responsabilidad de mando, reporte de incidentes, sanciones contractuales y administrativas, y una modificación al artículo 367

del Código Penal para incluir los sistemas de armas autónomas en el régimen de armas prohibidas.

El Título X contiene disposiciones finales sobre reglamentación, inventario inicial, transición, impacto fiscal, vigencia y derogatorias. Las prohibiciones son exigibles desde la promulgación y los plazos de reglamentación y evaluación no habilitan la continuidad de actividades o usos prohibidos. El inventario registrará los sistemas y usos comprendidos en las prohibiciones y las medidas adoptadas para hacerlas efectivas. Los contratos o autorizaciones anteriores tampoco permiten mantener esas actividades.

VII. Impacto Fiscal

De conformidad con el artículo 7° de la Ley 819 de 2003, el impacto fiscal de cualquier proyecto de ley que ordene gasto o que otorgue beneficios tributarios debe hacerse explícito y ser compatible con el Marco Fiscal de Mediano Plazo.

El presente proyecto de ley no crea entidades nuevas, no ordena la creación de cargos, no modifica plantas de personal, no establece beneficios tributarios, no crea subsidios, no impone transferencias presupuestales específicas y no ordena apropiaciones adicionales al Presupuesto General de la Nación. La arquitectura institucional se construye sobre entidades existentes, principalmente el Ministerio de Defensa Nacional, las Fuerzas Militares, la Policía Nacional y las entidades adscritas o vinculadas al sector defensa.

Sin perjuicio de lo anterior, se trae a colación los dicho sobre la materia por la Corte Constitucional. La Sentencia C-502 de 2007 expresó que los requisitos establecidos en el artículo se constituyen como instrumentos de racionalización de la actividad legislativa, pero que no pueden limitar el ejercicio de la función legislativa por parte del Congreso de la República ni pueden otorgar un poder de veto al Ministerio de Hacienda y Crédito Público en relación con el trámite y aprobación de los proyectos de ley, pues ello vulneraría la autonomía del legislador y el principio de separación de las ramas del poder público. Así mismo, señaló que es el Ministerio de Hacienda y Crédito Público el principal responsable de cumplir los requisitos establecidos en el artículo 7° de la Ley 819 de 2003:

"Por todo lo anterior, la Corte considera que los primeros tres incisos del artículo 7° de la Ley 819 de 2003 deben entenderse como parámetros de racionalidad de la actividad legislativa, y como una carga que le incumbe inicialmente al Ministerio de Hacienda, una vez que el Congreso ha valorado, con la información y las herramientas que tiene a su alcance, las incidencias fiscales de un determinado proyecto de ley. Esto significa que ellos constituyen instrumentos para mejorar la labor legislativa."

"Es decir, el mencionado artículo debe interpretarse en el sentido de que su fin es obtener que las leyes que se dicten tengan en cuenta las realidades macroeconómicas, pero sin crear barreras insalvables en el ejercicio de la función legislativa ni crear un poder de veto legislativo en cabeza del ministro de Hacienda. Y en ese proceso de racionalidad legislativa la carga principal reposa en el Ministerio de Hacienda, que es el que cuenta con los datos, los equipos de funcionarios y la experticia en materia económica. Por lo tanto, en el caso de que los congresistas tramiten un proyecto incorporando estimativos erróneos sobre el impacto fiscal, sobre la manera de atender esos nuevos gastos o sobre la compatibilidad del proyecto con el Marco Fiscal de Mediano Plazo, le corresponde al ministro de Hacienda intervenir en el proceso legislativo para ilustrar al Congreso acerca de las consecuencias económicas del proyecto. Y el Congreso habrá de recibir y valorar el concepto emitido por el Ministerio. No obstante, la carga de demostrar y convencer a los congresistas acerca de la incompatibilidad de cierto proyecto con el Marco Fiscal de Mediano Plazo recae sobre el ministro de Hacienda".

VIII. Conflicto de Interés

De acuerdo con lo ordenado por la Ley 2003 de 2019, en concordancia con los artículos 286 y siguientes de la Ley 5ª de 1992, y conforme con el objeto de la presente iniciativa, se puede concluir preliminarmente que la misma no representa un conflicto de interés general para los congresistas que participen en su trámite, dado que se trata de una regulación general, abstracta e impersonal sobre el uso de inteligencia artificial en defensa, Fuerza Pública y seguridad, así como sobre la prohibición de sistemas de armas autónomas.

Lo anterior se entiende sin perjuicio de la obligación que tiene cada congresista de examinar las circunstancias particulares que puedan configurarle un beneficio particular, actual y directo, a su favor, de su cónyuge o compañero permanente, o de sus parientes en los grados previstos por la ley, caso en el cual deberá declararse impedido en los términos del Reglamento del Congreso.

Sobre el conflicto de interés el Consejo de Estado se ha pronunciado en Sentencia del año 2022, estableciendo que:

"Siempre que se produzca un resultado provechoso por el simple ejercicio de una función oficial, que convenga al agente o a otra persona allegada, en el orden moral o material, surgirá un conflicto de intereses. Si la ley protege el interés, será lícito; pero si se persigue con fines personales, particulares, que sobrepasen el interés social, será ilícito".

También el Consejo de Estado el año 2010 sobre el conflicto de interés, conceptuó:

"La institución del conflicto de intereses apunta a trazar un límite entre el ejercicio legítimo de la función legislativa y el aprovechamiento de esta función por parte del congresista para obtener beneficios personales o en favor de aquellas personas allegadas que determina la ley. Así las cosas, no se presenta conflicto entre el interés personal del congresista y el interés general cuando

la ley tiene por destinataria a la generalidad de la sociedad, en abstracto, hipótesis en la cual quedan incluidos los amplios sectores sociales que son objeto de determinadas leyes, como por ejemplo las minorías étnicas o culturales, las profesiones, los contribuyentes o, como el caso que nos ocupa, las víctimas de la violencia en Colombia.

No sería razonable, por consiguiente, afirmar que por el hecho de ser abogado un congresista estaría impedido para participar en la aprobación de una ley que expida el estatuto de esa profesión; que por ser indígena estaría impedido para participar en el trámite de la ley orgánica que reglamente las entidades territoriales indígenas; que por ser propietario estaría impedido para intervenir en la discusión de una ley sobre impuesto predial; o que por encajar en la definición legal de víctima del conflicto estaría impedido para intervenir en los debates a un proyecto de ley que establece de manera general las reglas de resarcimiento a las víctimas de la violencia en Colombia. En todos estos casos, ciertamente, podría el congresista derivar de la ley en cuya discusión interviene un beneficio personal, pero no por la circunstancia de ser miembro del Congreso ni porque la ley se dirija a un grupo de personas tan restringido y exclusivo (y por tanto excluyente) que convierta al congresista en un destinatario predilecto. En los anteriores ejemplos las leyes no se dirigen a todos los colombianos sino a grupos muy significativos: los abogados, los indígenas, los propietarios de inmuebles, las víctimas del conflicto. No todos los congresistas forman parte necesariamente de estos grupos, pero por la amplitud social de dichos sectores en la nación y la generalidad de las prescripciones de la ley a ellos dirigida, normalmente algunos de los congresistas podrían quedar incluidos. Pues bien, en estos casos no cabe la figura de conflicto de intereses, pues a pesar de que un congresista podría convertirse en destinatario de alguna de las disposiciones legales, tal hecho no obedece a que la ley busque favorecerlo directa, exclusiva y especialmente."

En consecuencia, se considera que la ley y la jurisprudencia han dado los criterios orientadores que determinan circunstancias en las cuales se podría estar incurso en un conflicto de interés. Para lo cual será necesario que respecto del asunto objeto de conocimiento de parte del congresista (discusión o votación) se reporte un beneficio en el que concurran tres características simultáneas, a saber, ser actual, particular y directo. Define la Ley también las circunstancias bajo las cuales se considera que no existe un conflicto de interés, en esa medida, se señala que aun cuando el congresista pueda reportar un beneficio, pero este se funde en el interés general, en el interés de sus electores, se dará lugar a que no exista tal conflicto.

IX. Consideraciones Finales

La incorporación de inteligencia artificial en defensa y seguridad no puede quedar sometida únicamente a decisiones administrativas, lineamientos internos o criterios de adquisición tecnológica. Cuando una tecnología puede incidir en decisiones sobre vida, libertad, vigilancia, uso de fuerza, selección de objetivos, perfilamiento o responsabilidad de mando, corresponde al legislador trazar límites claros.

Colombia tiene la oportunidad de adoptar una regulación temprana, prudente y equilibrada. La propuesta no desconoce las necesidades legítimas de defensa nacional ni impide el desarrollo de capacidades tecnológicas propias. Por el contrario, diferencia entre usos permitidos, usos de alto riesgo y usos prohibidos; fortalece la soberanía tecnológica; habilita capacidades defensivas y humanitarias; y fija una línea democrática fundamental: ninguna máquina debe decidir autónomamente quién vive, quién muere, quién es objetivo, quién es vigilado o quién pierde su libertad.

Este proyecto permite que Colombia mantenga liderazgo regional en la discusión sobre armas autónomas, al tiempo que amplía el debate hacia una agenda más completa de inteligencia artificial en defensa, Fuerza Pública y seguridad. La regulación propuesta es compatible con la Constitución, el Derecho Internacional Humanitario, la protección de los derechos humanos y la necesidad de construir capacidades estatales responsables frente a tecnologías emergentes.



DAVID ALEJANDRO TORO RAMÍREZ
Representante a la Cámara
Pacto Histórico

X. REFERENCIAS

Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems [GGE]. (2026, 3 de septiembre). Report of the 2024-2025-2026 sessions of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (CCW/GGE.1/2026/CRP.1/Rev.1). Naciones Unidas. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-

Human Rights Watch, & Harvard Law School International Human Rights Clinic. (2025, April 28). A *hazard to human rights: Autonomous weapons systems and digital decision-making.* Human Rights Watch. https://www.hrw.org/report/2025/04/28/a-hazard-to-human-rights/autonomous-weapons-systems-and-digital-decision-making

International Committee of the Red Cross. (2021, May 12). ICRC position on autonomous weapon systems. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems

International Committee of the Red Cross. (2025). Autonomous weapon systems and international humanitarian law: Selected issues. https://www.icrc.org/en/article/autonomous-weapon-systems-and-international-humanitarian-law-selected-issues

North Atlantic Treaty Organization. (2024, July 10). Summary of NATO's revised Artificial Intelligence (AI) Strategy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

Russell, S., Segerie, C.-R., Iliadis, N., & Zoumpalova, T. (2025, September 22). AI governance through global red lines can help prevent unacceptable risks. OECD.AI Policy Observatory. https://oecd.ai/en/wonk/ai-governance-through-global-red-lines-can-help-prevent-unacceptable-risks

The Future Society. (2025, July 3). Global red lines for AI: A three-part series. https://thefuturesociety.org/airedlines/

The Future Society. (2026, February 12). Defining and governing unacceptable AI risks. https://thefuturesociety.org/athens-2025-ai-red-lines-report/

The Future Society. (2026). Where do we draw the line? Inside the IASEAI expert workshop on AI red lines. https://thefuturesociety.org/ai-red-lines-iaseai-workshop/

United Nations General Assembly. (2024, July 1). Lethal autonomous weapons systems: Report of the Secretary-General (A/79/88). United Nations. https://digitallibrary.un.org/record/4059475

United States Congress. (2026). AI Guardrails Act of 2026, S. 4113, 119th Cong., 2nd Sess.

United States Department of Defense. (2022, June). Responsible Artificial Intelligence Strategy and Implementation Pathway. https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.pdf

* * *

PROYECTO DE LEY NÚMERO 366 DE 2026

por medio de la cual se establecen objetivos y criterios para prevenir riesgos sistémicos derivados de dependencias críticas de inteligencia artificial en la actividad financiera, bursátil y aseguradora.

Bogotá, D. C., septiembre de 2026

Secretario General

MIGUEL ÁNGEL SÁNCHEZ VÁSQUEZ

Cámara de Representantes Ciudad

Referencia: Radicación de proyecto de ley

En ejercicio de la facultad de iniciativa legislativa, presento a consideración de la Cámara de Representantes el Proyecto de Ley, *por medio de la cual se establecen objetivos y criterios para prevenir riesgos sistémicos derivados de dependencias críticas de inteligencia artificial en la actividad financiera, bursátil y aseguradora*. El cual busca establecer objetivos y criterios de intervención que fortalezcan la continuidad de funciones esenciales y permitan prevenir la propagación de fallas asociadas a dependencias críticas de inteligencia artificial.

Cordialmente,

DAVID ALEJANDRO TORO RAMÍREZ
Representante a la Cámara
Pacto Histórico



PROYECTO DE LEY NÚMERO 366 DE 2026 CÁMARA

por medio de la cual se establecen objetivos y criterios para prevenir riesgos sistémicos derivados de dependencias críticas de inteligencia artificial en la actividad financiera, bursátil y aseguradora.

El Congreso de Colombia

DECRETA:

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1°. ***Objeto.*** La presente ley establece las normas generales, los objetivos y los criterios a los cuales debe sujetarse el Gobierno nacional para prevenir y gestionar los riesgos sistémicos derivados de dependencias críticas de inteligencia artificial en la actividad financiera, bursátil y aseguradora, de conformidad con el literal d) del numeral 19 del artículo 150 de la Constitución Política. Su finalidad es proteger la continuidad de las funciones esenciales, a los consumidores financieros y a los inversionistas, y preservar la estabilidad y la confianza en el sistema.

Artículo 2°. ***Ámbito de aplicación.*** Las disposiciones que se expidan en desarrollo de esta ley se aplicarán a las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia, respecto de las actividades financiera, bursátil y aseguradora que desarrollen y de las dependencias críticas de inteligencia artificial que utilicen, directamente o mediante terceros.

Artículo 3°. ***Criterios de identificación de las dependencias críticas***. Para efectos de esta ley, se entenderá por sistema de inteligencia artificial un sistema basado en máquinas que, a partir de las entradas que recibe y para objetivos explícitos o implícitos, infiere cómo generar predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.

Una dependencia será crítica cuando la interrupción, degradación, alteración de resultados

o indisponibilidad de un sistema de inteligencia artificial, de un modelo, de datos o de un servicio tecnológico que lo soporte materialmente pueda comprometer una función esencial y no exista una alternativa efectiva de continuidad o sustitución dentro de tiempos compatibles con su prestación.

El Gobierno nacional atenderá, para determinar la criticidad, al impacto sobre consumidores e inversionistas; la naturaleza, escala e interconexión de las operaciones; la concentración de proveedores, modelos y subproveedores; la capacidad real de sustitución; y la posibilidad de afectación simultánea de varias entidades.

Serán funciones esenciales aquellas cuya interrupción o ejecución defectuosa pueda afectar gravemente la prestación de los servicios de la entidad, el cumplimiento de sus obligaciones frente a consumidores e inversionistas o la estabilidad del sistema. La infraestructura general de nube, comunicaciones o procesamiento quedará comprendida únicamente en cuanto soporte materialmente una dependencia crítica de inteligencia artificial.

Artículo 4°. ***Objetivos y criterios de intervención***. En desarrollo de esta ley, el Gobierno nacional se sujetará a los siguientes objetivos y criterios:

1. Prevenir la propagación de fallas y las afectaciones simultáneas derivadas de dependencias comunes, y fortalecer la continuidad y la recuperación de las funciones esenciales.

2. Aplicar exigencias proporcionales a la criticidad, la exposición al riesgo, la complejidad y la capacidad operativa de las entidades, con atención a los costos de cumplimiento y a sus efectos sobre la competencia y la inclusión financiera.

3. Preservar la responsabilidad de los órganos de administración de las entidades vigiladas y asegurar que las decisiones sobre dependencias críticas cuenten con información suficiente y responsables identificables.

4. Aplicar neutralidad tecnológica y permitir soluciones equivalentes de mitigación. La utilización de inteligencia artificial o de un proveedor común no constituirá, por sí sola, una infracción ni dará lugar a la obligación de contratar múltiples proveedores.

5. Integrar las medidas a los sistemas de administración de riesgos, continuidad, seguridad de la información y tercerización existentes, evitando duplicidades de reportes, pruebas y controles.

6. Respetar la protección de datos personales, las reservas legales, la propiedad intelectual, la libre competencia y el debido proceso.

TÍTULO II

CRITERIOS PARA LA GESTIÓN Y SUPERVISIÓN DEL RIESGO

Artículo 5°. ***Identificación y trazabilidad.*** El Gobierno nacional establecerá criterios para que las entidades identifiquen y mantengan actualizada la información sobre sus dependencias críticas, las funciones esenciales que soportan, los responsables de su gestión, los proveedores directos y los subproveedores materiales conocidos o razonablemente identificables mediante la debida diligencia.

La identificación deberá permitir evaluar las dependencias comunes de modelos, datos e infraestructura, incluso cuando existan distintos proveedores contractuales. La debida diligencia comprenderá las limitaciones de acceso a información y las medidas adoptadas frente a ellas; tales limitaciones no eximirán a la entidad de evaluar y gestionar el riesgo.

Artículo 6°. ***Evaluación de concentraciones y exposición común***. El Gobierno nacional establecerá criterios para la evaluación individual y agregada de las dependencias críticas, atendiendo a su concentración, interconexión, sustituibilidad y capacidad de ocasionar afectaciones simultáneas entre entidades.

La Superintendencia Financiera de Colombia, dentro de sus competencias legales, utilizará la información disponible y podrá requerir a las entidades vigiladas la información adicional necesaria para identificar exposiciones comunes, incluidas aquellas que trasciendan los límites de un conglomerado financiero. Los requerimientos deberán ser pertinentes, proporcionales y articulados con los reportes existentes.

El tratamiento, la conservación y el acceso a esta información se sujetarán a las reservas y demás garantías previstas en la ley. La divulgación de análisis agregados deberá evitar la revelación de datos protegidos y de vulnerabilidades cuya exposición comprometa la seguridad de las entidades o del sistema.

Artículo 7°. ***Pruebas de resiliencia***. El Gobierno nacional establecerá criterios para incorporar, en las pruebas de continuidad y de gestión de riesgos, escenarios de interrupción, degradación, alteración de resultados e indisponibilidad de las dependencias críticas, incluidos escenarios de falla simultánea de componentes o proveedores comunes cuando la exposición lo justifique.

La intensidad y periodicidad de las pruebas corresponderán al nivel de riesgo. Podrán emplearse simulaciones y otros mecanismos equivalentes que permitan comprobar las capacidades de respuesta sin poner en riesgo los servicios en producción ni los derechos de consumidores e inversionistas. Los resultados deberán orientar medidas de mejoramiento verificables.

Artículo 8°. ***Continuidad, recuperación y salida***. El Gobierno nacional establecerá criterios para que las entidades cuenten con estrategias viables y probadas de continuidad, recuperación y, cuando corresponda, sustitución o salida de sus dependencias críticas.

Estas estrategias considerarán tiempos de recuperación compatibles con la función esencial, alternativas operativas, preservación y recuperación

de información, portabilidad técnicamente factible y jurídicamente permitida, y transición ordenada. Podrán incluir procedimientos manuales u otras soluciones tecnológicas cuando resulten suficientes y proporcionales al riesgo.

La sola existencia de un contrato de respaldo no acreditará capacidad de recuperación. Deberán evaluarse la independencia material de la alternativa, sus limitaciones y las condiciones necesarias para activarla.

Artículo 9°. ***Gestión contractual y de terceros.*** El Gobierno nacional establecerá criterios para que la contratación asociada a dependencias críticas asegure, de manera proporcional al riesgo, información suficiente para su gestión y supervisión, niveles de servicio, notificación de incidentes y cambios materiales, condiciones de continuidad y terminación, y cooperación para una transición ordenada.

La evaluación de las cadenas de subcontratación comprenderá los servicios que soporten materialmente la dependencia crítica. La utilización de contratos estandarizados, proveedores extranjeros o subcontratistas no trasladará la responsabilidad de la entidad vigilada. Cuando no sea posible obtener determinadas condiciones contractuales, deberán evaluarse las restricciones, adoptarse medidas equivalentes de mitigación y determinarse si el riesgo residual es compatible con la continuidad de la función esencial.

Artículo 10. ***Incidentes y cambios materiales***. El Gobierno nacional establecerá criterios para el reporte oportuno de incidentes asociados a dependencias críticas que comprometan o puedan comprometer materialmente funciones esenciales o generar afectaciones simultáneas, así como para el seguimiento de cambios que modifiquen significativamente su perfil de riesgo.

La Superintendencia Financiera de Colombia desarrollará estos criterios dentro de sus competencias, aprovechando los canales existentes y definiendo umbrales, contenido y plazos proporcionales. El reporte no implicará autorización previa general para utilizar sistemas de inteligencia artificial ni para efectuar actualizaciones tecnológicas ordinarias.

Artículo 11. ***Supervisión y medidas de mitigación***. La Superintendencia Financiera de Colombia verificará el cumplimiento de las disposiciones expedidas en desarrollo de esta ley en ejercicio de sus atribuciones legales. Las medidas de corrección o mitigación que adopte deberán estar motivadas, guardar relación con el riesgo identificado y observar los principios de necesidad y proporcionalidad.

Las actuaciones administrativas y las consecuencias del incumplimiento se sujetarán a las competencias, los procedimientos y los regímenes sancionatorios legalmente aplicables. Esta ley no crea nuevas sanciones ni habilita medidas distintas de las autorizadas por el ordenamiento.

TÍTULO III

DISPOSICIONES FINALES

Artículo 12. ***Desarrollo y transición.*** El Gobierno nacional expedirá las disposiciones de desarrollo de esta ley dentro de los doce (12) meses siguientes a su promulgación. En ellas establecerá plazos de adecuación diferenciados y razonables según la criticidad, la complejidad de las dependencias y los ciclos contractuales, sin suspender las obligaciones de gestión de riesgos actualmente exigibles.

La Superintendencia Financiera de Colombia impartirá las instrucciones que correspondan dentro de sus competencias. En el desarrollo y aplicación de esta ley se reconocerán los controles, pruebas y reportes existentes que satisfagan objetivos equivalentes, evitando cargas duplicadas.

Artículo 13. ***Vigencia y articulación normativa***. La presente ley rige a partir de su promulgación y deroga las que le sean contrarias.

DAVID ALEJANDRO TORO RAMÍREZ
Representante a la Cámara
Pacto Histórico

EXPOSICIÓN DE MOTIVOS

El presente documento desarrolla el objeto, los antecedentes, el marco constitucional y legal, la justificación, el impacto fiscal, la descripción del articulado, las circunstancias de conflicto de intereses y las consideraciones finales de la iniciativa.

I. OBJETO DEL PROYECTO

El proyecto establece un marco legal de prevención frente a las fallas de sistemas de inteligencia artificial que, por su utilización en funciones esenciales o por la existencia de dependencias comunes, pueden afectar simultáneamente a entidades financieras, intermediarios del mercado de valores y aseguradoras. Busca que la adopción de estas herramientas esté acompañada de capacidad demostrable para identificar dependencias, contener incidentes y mantener o recuperar los servicios que necesitan los ciudadanos y la economía.

La intervención se concentra en las dependencias críticas. Un asistente interno de uso accesorio y un modelo del que depende una operación esencial no justifican las mismas exigencias. El articulado orienta al Gobierno nacional y conserva el papel de la Superintendencia Financiera de Colombia dentro de sus atribuciones vigentes. La continuidad, la sustituibilidad y la exposición común constituyen los criterios para graduar las medidas.

II. ANTECEDENTES

El ordenamiento colombiano cuenta con una tradición de intervención prudencial fundada en la protección del interés público. El Estatuto Orgánico del Sistema Financiero incorpora objetivos de protección de usuarios, confianza y seguridad de las instituciones; a su vez, la Ley 964 de 2005 incluye expresamente la prevención y el manejo del

riesgo sistémico entre los objetivos de intervención en el mercado de valores. Esta última también exige considerar la evolución tecnológica y los costos y beneficios de la regulación. El proyecto desarrolla esa orientación en una fuente específica de exposición tecnológica.[1],[2]

En el ámbito administrativo, la Superintendencia Financiera reexpidió la Circular Básica Jurídica mediante la Circular Externa 006 de 2025. Su repositorio normativo también presenta la Circular Básica Financiera expedida mediante la Circular Externa 004 de 2026. Estas actualizaciones hacen necesario examinar el contenido de las obligaciones existentes antes de proponer nuevas cargas.[3],[4]

El Sistema Integral de Administración de Riesgos ya contempla análisis de tercerización, identificación de procesos críticos, obligaciones contractuales, planes de contingencia y continuidad, pruebas y seguimiento. Incluso exige gestionar el riesgo asociado a proveedores que prestan servicios a varias entidades. La sección de agregación incorpora la perspectiva de la entidad y de la consolidación correspondiente. Por tanto, la propuesta no parte de un vacío normativo absoluto: concentra su aporte en dar una orientación legal explícita a la identificación de dependencias comunes de IA, incluidas cadenas indirectas y exposiciones que atraviesan entidades sin vínculo de control.[5]

El paso propuesto responde a la progresiva incorporación de modelos y servicios externos a la actividad supervisada. Su construcción conserva la regulación de riesgos existente, añade criterios para observar la dimensión colectiva de las dependencias y encarga el desarrollo técnico a las autoridades competentes. El legislador fija las prioridades y los límites; la regulación administrativa determina umbrales, formatos, periodicidad y condiciones de aplicación.

III. MARCO CONSTITUCIONAL Y LEGAL

3.1. Interés público y distribución de competencias

La actividad financiera, bursátil y aseguradora está calificada constitucionalmente como de interés público. El artículo 150, numeral 19, literal d), atribuye al Congreso la expedición de normas generales y de los objetivos y criterios que debe observar el Gobierno para regularla. Los artículos 189, numerales 24 y 25, y 335 complementan ese esquema de intervención y vigilancia. En consecuencia, la iniciativa se formula como una ley marco sectorial: las exigencias técnicas se desarrollarán dentro de esa distribución de competencias.[6]

La finalidad de proteger la prestación de servicios esenciales y contener la propagación de fallas justifica la intervención propuesta. Sus límites están en la proporcionalidad, la libertad económica, el debido proceso y la protección de información reservada. La definición de criticidad evita extender automáticamente las exigencias a cualquier uso de IA. Las soluciones equivalentes y la ausencia de una obligación general de contratar varios proveedores permiten ponderar los costos frente al riesgo efectivamente identificado.[7]

El proyecto no atribuye al Banco de la República la supervisión de sistemas de IA de las entidades vigiladas. Las competencias monetarias, cambiarias y crediticias de su Junta Directiva y las funciones constitucionales del Banco tienen un objeto propio. La posible relevancia macroeconómica de un incidente no basta para convertirlas en una competencia general de supervisión tecnológica. La iniciativa mantiene, en consecuencia, la supervisión de las entidades destinatarias dentro de las competencias existentes de la Superintendencia Financiera.[8]

IV. JUSTIFICACIÓN DEL PROYECTO

4.1. El problema público: una falla individual puede convertirse en una exposición compartida

La inteligencia artificial ofrece oportunidades de eficiencia, análisis y detección de riesgos. Aldasoro y sus coautores examinan su aplicación en intermediación, seguros, gestión de activos y pagos, y destacan tanto esos beneficios como los problemas

1 Presidencia de la República de Colombia (1993, 2 de abril). Decreto número 663 de 1993: Estatuto Orgánico del Sistema Financiero. Arts. 46, 48 y 326. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1348

2 Congreso de la República de Colombia (2005, 8 de julio). Ley 964 de 2005. Arts. 1 y 4. https://normograma.dian.gov.co/dian/compilacion/docs/ley_0964_2005.htm

3 Superintendencia Financiera de Colombia (2025, 25 de junio). Circular Básica Jurídica: Circular Externa 006 de 2025. https://www.superfinanciera.gov.co/publicaciones/10115528/circular-basica-juridica-ce-00625/

4 Superintendencia Financiera de Colombia (2026). Circular Básica Financiera: Circular Externa 004 de 2026. Parte 1, capítulo 1, sección 2, numerales 1.1.2.134–1.1.2.137, y sección 4, numerales 1.1.4.1–1.1.4.2. https://www.superfinanciera.gov.co/publicaciones/10116084/circular-basica-financiera-circular-externa-004-de-2026/

5 Superintendencia Financiera de Colombia (2026). Circular Básica Financiera: Circular Externa 004 de 2026. Parte 1, capítulo 1, sección 2, numerales 1.1.2.134–1.1.2.137, y sección 4, numerales 1.1.4.1–1.1.4.2. https://www.superfinanciera.gov.co/publicaciones/10116084/circular-basica-financiera-circular-externa-004-de-2026/

6 Asamblea Nacional Constituyente (1991). Constitución Política de Colombia. Arts. 15, 29, 150.19.d, 154, 158, 169, 182, 189.24 y 189.25, 333, 335, 371 y 372. https://www.funcionpublica.gav.co/eva/gestornormativo/norma.php?i=4125

7 Asamblea Nacional Constituyente (1991). Constitución Política de Colombia. Arts. 15, 29, 150.19.d, 154, 158, 169, 182, 189.24 y 189.25, 333, 335, 371 y 372. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

8 Asamblea Nacional Constituyente (1991). Constitución Política de Colombia. Arts. 15, 29, 150.19.d, 154, 158, 169, 182, 189.24 y 189.25, 333, 335, 371 y 372. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

de concentración, interconexión y gobernanza que acompañan la transformación. Su trabajo permite situar la prevención y la gestión de interdependencias como condiciones de una adopción sostenible.[9]

El informe del Financial Stability Board de 2024 identifica cuatro grupos de vulnerabilidades relevantes para la estabilidad: dependencias de terceros y concentración, correlaciones entre comportamientos, riesgos cibernéticos y problemas de modelos, datos y gobernanza. Advierte además necesidades de información y de evaluación de la suficiencia de los marcos existentes. La convergencia de estas exposiciones explica que una entidad pueda gestionar su contrato individual y, aun así, compartir con muchas otras un punto de falla que ninguna observa por completo.[10]

Para efectos del proyecto, cabe distinguir dos mecanismos. En el primero, varias entidades pierden simultáneamente acceso a un servicio o componente común. En el segundo, el servicio continúa disponible, pero produce resultados alterados o sistemáticamente defectuosos que se incorporan a decisiones esenciales. Esta distinción es una inferencia de diseño normativo: justifica probar tanto la disponibilidad como la degradación y la integridad de los resultados, sin afirmar que todos los errores de un modelo son sistémicos.

Un ejemplo hipotético ilustra el problema: dos entidades contratan aplicaciones diferentes que utilizan un mismo modelo de un tercero. La diversidad comercial aparente no asegura independencia técnica. Si el componente común falla, ambas alternativas pueden quedar afectadas. De allí que el articulado exija evaluar las dependencias materiales y la capacidad real de recuperación, en lugar de medir resiliencia únicamente por el número de contratos celebrados.

4.2. Evidencia colombiana y límites de lo que puede concluirse

La publicación de Jiménez, Mendoza y Moreno, divulgada por la Superintendencia Financiera en 2026, ofrece evidencia local concreta. Su población objetivo comprendió 47 establecimientos de crédito con cartera vigente a marzo de 2025. De ellos, 38 reportaron modelos de IA o aprendizaje automático, con un total de 346 modelos. El examen detallado se concentró en 91 modelos seleccionados por su utilización en las etapas del crédito. Estos resultados muestran que la discusión ya tiene un referente operativo en Colombia.[11]

El alcance de ese ejercicio debe respetarse: se refiere a riesgo de crédito, no a la totalidad del sector bursátil y asegurador; tampoco mide la probabilidad de una crisis causada por IA ni constituye un mapa completo de concentración de proveedores. La propia publicación distingue las opiniones de sus autores de la posición oficial de la Superintendencia. La inferencia legislativa razonable es que la adopción observada justifica mejorar la identificación preventiva de dependencias, sin atribuir al estudio estimaciones de pérdidas, incidentes nacionales o cuotas de mercado que no contiene.[12]

La propuesta permite obtener información comparable sobre criticidad, sustituibilidad y componentes comunes, aprovechando los canales de supervisión. Con ello se busca que la intensidad de las medidas descanse en exposición verificable. El uso de IA no se convierte en una presunción de inseguridad y el desconocimiento parcial de una cadena tecnológica tampoco puede sustituir el deber de debida diligencia.

4.3. Evidencia académica y experiencia de supervisión

Gensler y Bailey analizan cómo el aprendizaje profundo puede generar fragilidades por dependencia de datos, modelos e infraestructura compartidos y por dificultades de explicación y supervisión. Su aporte al proyecto consiste en mostrar por qué el desempeño de cada aplicación, considerado aisladamente, no agota la evaluación de estabilidad del conjunto.[13]

Kleinberg y Raghavan estudian teóricamente la llamada monocultura algorítmica: bajo las condiciones de su modelo, la adopción de un mismo algoritmo puede afectar el resultado colectivo aunque sea atractivo para cada participante. El trabajo examina decisiones de selección y asignación, de modo que no debe presentarse como prueba directa

9 Aldasoro, I., Gambacorta, L., Korinek, A., Shreeti, V., & Stein, M. (2024, junio). Intelligent financial system: How AI is transforming finance. BIS Working Papers, n.º 1194. Bank for International Settlements. https://www.bis.org/publications/working-paper-1194-intelligent-financial-system-how-ai-transforming-finance

10 Financial Stability Board (2024, 14 de noviembre*). The financial stability implications of artificial intelligence*. Resumen ejecutivo y secciones sobre vulnerabilidades y marcos de politíca. https://www.fsb.org/up1oads/P14l12024.pdf

11 . Jiménez, A. E., Mendoza, S. D., & Moreno, I. E. (2026*). Caracterización de las prácticas identificadas y desarrollos realizados en IA para la gestión del riesgo de crédito*. pp. 2–6. Superintendencia Financiera de Colombia. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=108224 9

12 Jiménez, A. E., Mendoza, S. D., & Moreno, I. E. (2026). *Caracterización de las prácticas identificadas y desarrollos realizados en IA para la gestión del riesgo de crédito*. pp. 2–6. Superintendencia Financiera de Colombia. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=108224 9

13 Gensler, G., & Bailey, L. (2020). *Deep learning and financial stability*. MIT Sloan Research Paper n.º 6223-20. MIT Sloan School of Management. https://mitsloan.mit.edu/shared/ods/documents?PublicationDocumentID=7644

14 Kleinberg, J., & Raghavan, M. (2021). *Algorithmic monoculture and social welfare.* Prepublicación arXiv:2101.05853. https://arxiv.org/abs/2101.05853

de una crisis financiera. Sí aporta una advertencia analítica útil: la calidad individual y la diversidad de decisiones son dimensiones diferentes. El proyecto recoge esa precaución mediante la evaluación de exposiciones comunes, sin prohibir modelos compartidos.[14]

La encuesta del Banco de Inglaterra y la Financial Conduct Authority de 2024 recibió 118 respuestas. El 75 % de los participantes declaró utilizar IA y aproximadamente un tercio de los casos de uso correspondía a implementaciones de terceros. Los tres proveedores de modelos más mencionados representaban el 44 % de los proveedores nombrados en esa categoría. Son datos de los encuestados y de sus menciones, no cuotas mundiales de mercado ni resultados extrapolables a Colombia. Muestran, sin embargo, la utilidad práctica de preguntar por adopción y dependencias de manera conjunta.[15]

La combinación de estudios teóricos, un ejercicio colombiano y una encuesta de supervisores extranjeros ofrece razones convergentes para prevenir, pero no permite cuantificar aquí un beneficio fiscal ni una reducción porcentual de pérdidas. La decisión legislativa se sustenta en la relevancia del servicio protegido, la posibilidad de afectaciones comunes y la necesidad de una respuesta proporcionada ante información incompleta.

4.4. Aporte de la sociedad civil y protección del interés público

Finance Watch, organización de la sociedad civil especializada en finanzas, plantea en el informe de Thierry Philipponnat de 2025 problemas de responsabilidad, opacidad y capacidad efectiva de supervisión del uso de IA. Su posición es una contribución experta al debate de política pública; no tiene fuerza normativa ni sustituye la evidencia empírica. Resulta pertinente su insistencia en que la prestación automatizada de un servicio financiero conserve responsables identificables y posibilidades reales de control.[16]

El articulado traduce esa preocupación en una regla institucional concreta: las entidades vigiladas conservan sus responsabilidades, aunque utilicen modelos externos, contratos estandarizados o cadenas de subcontratación. Para un consumidor o inversionista, la complejidad técnica del proveedor no elimina el impacto de una interrupción. La continuidad debe ser evaluable y los controles deben permitir identificar quién decide, quién responde y cómo se recupera la función afectada.

4.5. Orientaciones de organismos internacionales

La caja de herramientas del Financial Stability Board de 2023 sobre terceros propone identificar servicios críticos, examinar dependencias y cadenas de suministro, y desarrollar capacidades de supervisión y gestión de concentraciones. Su carácter es orientador y admite diferencias entre jurisdicciones. El proyecto adopta esa lógica de identificación y evaluación agregada, pero canaliza los requerimientos a través de las entidades ya vigiladas.[17]

Los principios de resiliencia operativa del Comité de Basilea de 2021 articulan gobierno, continuidad, pruebas, interdependencias, terceros, incidentes y tecnología. Su contribución es vincular la continuidad con la capacidad de prestar operaciones críticas durante una perturbación. Son estándares de referencia para la supervisión bancaria, cuya implementación depende de cada jurisdicción, y respaldan el enfoque de integrar las pruebas a los sistemas de riesgos existentes.[18]

Para seguros existe un referente específico: el documento de la Asociación Internacional de Supervisores de Seguros de julio de 2025 sobre supervisión de IA. Sus apartados sobre terceros exigen atención a información, subcontratación, concentración, planes de salida y contingencia; también identifican posibles implicaciones sistémicas cuando un proveedor sirve a varias aseguradoras. Se trata de orientaciones de aplicación de principios supervisores, no de una nueva ley internacional. Su pertinencia evita justificar todo el proyecto únicamente con experiencias bancarias.[19]

La agenda continúa en desarrollo. El Financial Stability Board publicó en junio de 2026 un informe de consulta sobre prácticas de adopción responsable de IA, con atención a gobierno y gestión durante el ciclo de vida. Se cita en esa calidad, sin atribuirle obligatoriedad ni carácter de recomendación final.

El diseño legislativo debe precisamente permitir que la regulación técnica evolucione sin modificar la ley ante cada cambio de arquitectura o de proveedor.[20]

---

14 Kleinberg, J., & Raghavan, M. (2021). *Algorithmic monoculture and social welfare.* Prepublicación arXiv:2101.05853. https://arxiv.org/abs/2101.05853

15 Bank of England & Financial Conduct Authority (2024, 21 de noviembre). *Artificial intelligence in UK financial services – 2024.* Secciones sobre adopción y dependencias de terceros. https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024

16 Philipponnat, T. (2025, marzo). *Artificial intelligence in finance: How to trust a black box?*. pp. 24–25 y 39. Finance Watch. https://www.finance-watch.org/wp-content/uploads/2025/03/Artificial_intelligence_in_finance_report_final.pdf

17 Financial Stability Board (2023, 4 de diciembre). Enhancing third-party risk management and oversight: A toolkit for financial institutions and financial authorities. https://www.fsb.org/uploads/P041223-1.pdf

18 Basel Committee on Banking Supervision (2021, marzo). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/publications/202103-guidelines-principles-operational-resilience

19 International Association of Insurance Supervisors (2025, julio). Application paper on the supervision of artificial intelligence. Sección 3.5, párrs. 48–51, pp. 22–24. https://www.iais.org/uploads/2025/07/Application-Paper-on-the-supervision-of-artificial-intelligence.pdf

20 Financial Stability Board (2026, 10 de junio). Sound practices for responsible adoption of artificial intelligence (AI): Consultation report. Documento de consulta; no constituye una norma vinculante.
https://www.fsb.org/2026/06/sound-practices-for-responsible-adoption-of-artificial-intelligence-ai-consultation-report/

4.6. Experiencia comparada: normas vinculantes y diferencias de alcance Unión Europea. El Reglamento (UE) 2022/2554, conocido como DORA y aplicable desde el 17 de enero de 2025, establece un marco de resiliencia operativa digital para las entidades comprendidas en su ámbito. Incluye pruebas, gestión de riesgos de terceros, evaluación de concentración, condiciones contractuales y estrategias de salida. También prevé vigilancia de determinados proveedores críticos. Es una regulación general de riesgos de tecnologías de información y comunicaciones, no una ley exclusivamente sobre IA. Sus artículos 28 a 31 ofrecen una referencia normativa concreta para dependencias que pueden soportar sistemas de IA.[21]

Reino Unido. Las autoridades financieras publicaron en noviembre de 2024 el régimen de terceros críticos PS16/24, con reglas vigentes desde el 1 de enero de 2025 y aplicación a proveedores designados por el Tesoro. La supervisión de servicios sistémicos, las pruebas y el manejo de incidentes complementan las responsabilidades de las entidades financieras. Este diseño incorpora competencias directas sobre determinados terceros que el presente proyecto colombiano no reproduce. La participación del Banco de Inglaterra responde a la organización jurídica británica y no constituye fundamento para asignar una función equivalente al Banco de la República.[22]

Australia. El estándar prudencial CPS 230 de APRA regula riesgo operacional, continuidad y proveedores materiales. La versión consultada rige desde el 1° de julio de 2026. Su enfoque vincula operaciones críticas con tolerancias de interrupción, gestión de proveedores y capacidad de recuperación. Es un estándar supervisor aplicable a entidades reguladas por APRA, con reglas y excepciones propias; no una ley general sobre IA. Su utilidad comparativa está en exigir resultados operativos verificables y en evaluar dependencias más allá de la contratación inicial.[23]

Estos instrumentos no obligan a Colombia a adoptar una ley idéntica, ni prueban la existencia de una norma internacional uniforme sobre IA financiera. Sí muestran una convergencia verificable: identificación de funciones críticas, responsabilidad de la entidad, información sobre dependencias, pruebas y capacidad de salida. La opción colombiana conserva ese núcleo funcional y lo adapta a la técnica de ley marco y a las atribuciones nacionales. El proyecto tiene un alcance más específico que DORA y evita trasladar automáticamente modelos extranjeros de supervisión directa de proveedores.

4.7. Necesidad, alternativas y proporcionalidad de la respuesta

La existencia de facultades administrativas previas obliga a explicar por qué intervenir mediante ley. La alternativa de desarrollar únicamente instrucciones de supervisión es jurídicamente relevante y puede atender parte del problema. También cabe promover compromisos voluntarios. Sin embargo, estos últimos no aseguran información comparable ni cobertura suficiente cuando el riesgo de una entidad depende de decisiones de otras. La decisión propuesta es establecer una orientación legislativa estable y común, con límites expresos a las cargas y desarrollo técnico flexible.

El aporte adicional consiste en conectar tres planos que deben observarse conjuntamente: la función esencial afectada, la dependencia técnica material (incluida la indirecta) y la exposición compartida entre entidades. No se pretende afirmar que la autoridad carece actualmente de toda herramienta para esos fines. Se busca que su utilización responda a criterios legales explícitos de criticidad, sustituibilidad, proporcionalidad y no duplicación, y que la dimensión colectiva no se reduzca al perímetro de cada grupo empresarial.

La opción de exigir varios proveedores en todos los casos fue descartada: podría elevar costos sin reducir el riesgo cuando ambos dependen del mismo componente. También se descarta la autorización previa de cada modelo o actualización ordinaria, porque desviaría la supervisión hacia trámites indiscriminados. En su lugar, el articulado exige estrategias equivalentes, cambios materiales y pruebas acordes con la exposición. Estas decisiones permiten concentrar la supervisión en el riesgo material y en la eficacia de los controles.

Para entidades pequeñas, la proporcionalidad significa poder acreditar controles suficientes con medios compatibles con su operación. Para exposiciones altamente críticas, exige mayor profundidad de análisis y de prueba. El criterio decisivo es la capacidad de proteger la función esencial y contener la propagación de la falla. La reglamentación deberá precisar los umbrales con información supervisora, costos de cumplimiento y consulta técnica, y reconocer controles ya existentes que cumplan la misma finalidad.

La implementación puede evaluarse mediante la cobertura del inventario de dependencias críticas, la identificación de componentes comunes, los resultados de pruebas de recuperación y la corrección de debilidades detectadas. Estos indicadores son criterios propuestos para valorar la eficacia; no constituyen metas cuantitativas ya demostradas. Su análisis deberá proteger información sensible y evitar que la mera cantidad de reportes se confunda con una mejora real de resiliencia.

V. IMPACTO FISCAL

El artículo 7° de la Ley 819 de 2003 exige explicitar el impacto fiscal de iniciativas que ordenen gasto u otorguen beneficios tributarios y su compatibilidad con el Marco Fiscal de Mediano

21 Parlamento Europeo & Consejo de la Unión Europea (2022, 14 de diciembre). Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero. Arts. 24-31 y 64. ***Diario Oficial*** de la Unión Europea, L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/spa

22 Bank of England, Prudential Regulation Authority, & Financial Conduct Authority (2024, 12 de noviembre). Operational resilience: Critical third parties to the UK financial sector. Policy Statement PS16/24; reglas con entrada en vigor el 1 de enero de 2025. https://www.bankofengland.co.uk/prudential-

23 Australian Prudential Regulation Authority (2026, 1 de julio). Prudential Standard CPS 230: Operational risk management. Versión vigente desde el 1 de julio de 2026; apartados sobre continuidad y proveedores de servicios. https://www.apra.gov.au/standards/cps-230

Plazo. El articulado no crea fondos, plantas de personal, subsidios, beneficios tributarios ni una obligación de garantizar o asumir pérdidas privadas. Tampoco incorpora una apropiación presupuestal específica.[24]

Se trae a colación lo dicho por la Corte Constitucional en la Sentencia C-502 de 2007, en la que expresó que los requisitos establecidos en el artículo 7° de la Ley 819 de 2003 se constituyen como instrumentos de racionalización de la actividad legislativa que no pueden limitar el ejercicio de la función legislativa por parte del Congreso de la República ni pueden otorgar un poder de veto al Ministerio de Hacienda y Crédito Público en relación con el trámite y aprobación de los proyectos de ley, pues ello vulneraría la autonomía del legislador y el principio de separación de las ramas del poder público. Así mismo, señaló que es el Ministerio de Hacienda y Crédito Público el principal responsable de cumplir los requisitos establecidos en el artículo 7° de la Ley 819 de 2003:

"Por todo lo anterior, la Corte considera que los primeros tres incisos del art. 7° de la Ley 819 de 2003 deben entenderse como parámetros de racionalidad de la actividad legislativa, y como una carga que le incumbe inicialmente al Ministerio de Hacienda, una vez que el Congreso ha valorado, con la información y las herramientas que tiene a su alcance, las incidencias fiscales de un determinado proyecto de ley. Esto significa que ellos constituyen instrumentos para mejorar la labor legislativa.

Es decir, el mencionado artículo debe interpretarse en el sentido de que su fin es obtener que las leyes que se dicten tengan en cuenta las realidades macroeconómicas, ***pero sin crear barreras insalvables en el ejercicio de la función legislativa ni crear un poder de veto legislativo en cabeza del ministro de Hacienda****. Y en ese proceso de racionalidad legislativa la carga principal reposa en el Ministerio de Hacienda, que es el que cuenta con los datos, los equipos de funcionarios y la experticia en materia económica. Por lo tanto, en el caso de que los congresistas tramiten un proyecto incorporando estimativos erróneos sobre el impacto fiscal, sobre la manera de atender esos nuevos gastos o sobre la compatibilidad del proyecto con el Marco Fiscal de Mediano Plazo, le corresponde al ministro de Hacienda intervenir en el proceso legislativo para ilustrar al Congreso acerca de las consecuencias económicas del proyecto. Y el Congreso habrá de recibir y valorar el concepto emitido por el Ministerio. No obstante, la carga de demostrar y convencer a los congresistas acerca de la incompatibilidad de cierto proyecto con el Marco Fiscal de Mediano Plazo recae sobre el ministro de Hacienda*" (subrayado fuera del original).

VI. DESCRIPCIÓN DEL ARTICULADO

Los trece artículos se organizan en tres títulos. El primero delimita objeto, sujetos, criticidad y objetivos. El segundo desarrolla los criterios de identificación, evaluación de exposición común, pruebas, recuperación, contratos, incidentes y supervisión. El tercero establece el desarrollo, la transición y la vigencia. Todas las disposiciones se conectan con la prevención de riesgos derivados de dependencias críticas de IA.

Artículos	Contenido y efecto esperado
1° a 4°	Definen el objeto y el perímetro supervisado, la criticidad y los principios de proporcionalidad, responsabilidad y neutralidad tecnológica.
5° y 6°	Orientan la identificación de cadenas materiales y la evaluación de concentraciones y exposiciones comunes entre entidades.
7° y 8°	Exigen orientar las pruebas y estrategias de continuidad hacia fallas plausibles y alternativas de recuperación efectivas.
9° y 10	Vinculan contratación, responsabilidad, incidentes y cambios materiales, con información útil y reportes integrados.
11	Mantiene la supervisión y las medidas de mitigación dentro de las atribuciones legales y del debido proceso.
12 y 13	Prevén desarrollo en doce meses, transición diferenciada, reconocimiento de equivalencias y articulación con el marco vigente.

VII. CONFLICTO DE INTERESES

De conformidad con los artículos 286 y 291 de la Ley 5ª de 1992, modificados por la Ley 2003 de 2019, corresponde identificar circunstancias que podrían generar un beneficio particular, actual y directo. El carácter general del proyecto no sustituye el examen individual que debe realizar cada congresista.[25]

Podrían requerir ese examen, entre otras circunstancias, la participación económica o los vínculos contractuales del congresista, su cónyuge o compañero permanente y sus parientes dentro de los grados legales con entidades vigiladas o proveedores tecnológicos, cuando una disposición les produzca un beneficio particular, actual y directo. También deberán evaluarse beneficios específicos derivados de condiciones de transición, contratación o mitigación y las circunstancias relacionadas con financiadores de campaña, conforme a las reglas legales aplicables.

La sola pertenencia de una entidad a un sector regulado no configura automáticamente un impedimento. Cada congresista deberá valorar su situación concreta, efectuar las manifestaciones exigidas y, cuando corresponda, declarar el impedimento antes de participar en la discusión o votación.

---

24 Congreso de la República de Colombia (2003, 9 de julio). Ley 819 de 2003. Art. 7°. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13712

25 Congreso de la República de Colombia (1992, 17 de junio). Ley 5a de 1992. Arts. 140, 142, 145, 286 y 291; texto consolidado, incluidas las modificaciones de la Ley 2003 de 2019. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=11368

Sobre el conflicto de interés el Consejo de Estado se ha pronunciado en Sentencia del año 2022, estableciendo que:

"Siempre que se produzca un resultado provechoso por el simple ejercicio de una función oficial, que convenga al agente o a otra persona allegada, en el orden moral o material, surgirá un conflicto de intereses. Si la ley protege el interés, será lícito; pero si se persigue con fines personales, particulares, que sobrepasen el interés social, será ilícito".

También el Consejo de Estado el año 2010 sobre el conflicto de interés, conceptuó:

"*La institución del conflicto de intereses apunta a trazar un límite entre el ejercicio legítimo de la función legislativa y el aprovechamiento de esta función por parte del congresista para obtener beneficios personales o en favor de aquellas personas allegadas que determina la ley. Así las cosas, no se presenta conflicto entre el interés personal del congresista y el interés general cuando la ley tiene por destinataria a la generalidad de la sociedad, en abstracto, hipótesis en la cual quedan incluidos los amplios sectores sociales que son objeto de determinadas leyes, como por ejemplo las minorías étnicas o culturales, las profesiones, los contribuyentes o, como el caso que nos ocupa, las víctimas de la violencia en Colombia.*

No sería razonable, por consiguiente, afirmar que por el hecho de ser abogado un congresista estaría impedido para participar en la aprobación de una ley que expida el estatuto de esa profesión; que por ser indígena estaría impedido para participar en el trámite de la ley orgánica que reglamente las entidades territoriales indígenas; que por ser propietario estaría impedido para intervenir en la discusión de una ley sobre impuesto predial; o que por encajar en la definición legal de víctima del conflicto estaría impedido para intervenir en los debates a un proyecto de ley que establece de manera general las reglas de resarcimiento a las víctimas de la violencia en Colombia. En todos estos casos, ciertamente, podría el congresista derivar de la ley en cuya discusión interviene un beneficio personal, pero no por la circunstancia de ser miembro del Congreso ni porque la ley se dirija a un grupo de personas tan restringido y exclusivo (y por tanto excluyente) que convierta al congresista en un destinatario predilecto. En los anteriores ejemplos las leyes no se dirigen a todos los colombianos sino a grupos muy significativos: los abogados, los indígenas, los propietarios de inmuebles, las víctimas del conflicto. No todos los congresistas forman parte necesariamente de estos grupos, pero por la amplitud social de dichos sectores en la nación y la generalidad de las prescripciones de la ley a ellos dirigida, normalmente algunos de los congresistas podrían quedar incluidos. Pues bien, en estos casos no cabe la figura de conflicto de intereses, pues a pesar de que un congresista podría convertirse en destinatario de alguna de las disposiciones legales, tal hecho no obedece a que la ley busque favorecerlo directa, exclusiva y especialmente."

En consecuencia, se considera que la Ley y la jurisprudencia han dado los criterios orientadores que determinan circunstancias en las cuales se podría estar incurso en un conflicto de interés. Para lo cual será necesario que respecto del asunto objeto de conocimiento de parte del congresista (discusión o votación) se reporte un beneficio en el que concurran tres características simultáneas, a saber, ser actual, particular y directo. Define la Ley también las circunstancias bajo las cuales se considera que no existe un conflicto de interés, en esa medida, se señala que aun cuando el congresista pueda reportar un beneficio, pero este se funde en el interés general, en el interés de sus electores, se dará lugar a que no exista tal conflicto.

VIII. CONSIDERACIONES FINALES

La continuidad de servicios financieros esenciales requiere que las entidades conozcan de qué dependen y puedan responder cuando esas dependencias fallen. La adopción de IA hace necesario observar tanto la exposición de cada institución como los componentes compartidos que pueden transmitir una perturbación. El proyecto ofrece objetivos legales para esa evaluación, preserva la adaptación técnica y mantiene responsables institucionales definidos.

La evidencia examinada sustenta una respuesta preventiva y proporcionada. No acredita una crisis nacional atribuible a IA ni permite prometer su eliminación mediante una ley. La finalidad alcanzable es mejorar la información, las pruebas y las capacidades de recuperación, con atención a los costos y al marco colombiano. Por estas razones se somete a consideración del Congreso de la República el presente proyecto de ley.

DAVID ALEJANDRO TORO RAMÍREZ
Representante a la Cámara
Pacto Histórico

CONTENIDO

Gaceta número 1460 - viernes, 2 de octubre de 2026

CÁMARA DE REPRESENTANTES

PROYECTO DE LEY **Págs.**

Proyecto de ley número 364 de 2026 Cámara, por medio de la cual se regula el uso de inteligencia artificial en el sector defensa y se dictan otras disposiciones..... 1

Proyecto de Ley número 366 de 2026 Cámara, por medio de la cual se establecen objetivos y criterios para prevenir riesgos sistémicos derivados de dependencias críticas de inteligencia artificial en la actividad financiera, bursátil y aseguradora..... 18

IMPRENTA NACIONAL DE COLOMBIA - 2026