



INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL PARA REGULAR Y FOMENTAR EL USO DE LA INTELIGENCIA ARTIFICIAL (IA) EN MÉXICO.

Los que suscriben, Senadoras y Senadores integrantes de la Comisión de Análisis, Seguimiento y Evaluación sobre la aplicación y desarrollo de la Inteligencia Artificial en México, de la LXVI Legislatura del Congreso de la Unión, y con fundamento en lo dispuesto por la fracción II del artículo 71 de la Constitución Política de los Estados Unidos Mexicanos; y por la fracción I, del numeral 1 del artículo 8, así como por el artículo 164 del Reglamento de Senado de la República, se somete a la consideración de esta Asamblea la presente Iniciativa con Proyecto de Decreto por el que se expide la Ley General para regular y fomentar el uso de la Inteligencia Artificial (IA) En México.

EXPOSICIÓN DE MOTIVOS

I. Consideraciones Generales

La inteligencia artificial se ha consolidado como una infraestructura productiva y decisional de carácter transversal, con impactos profundos y verificables en la organización de los procesos económicos, sociales, administrativos y políticos del siglo XXI. Lejos de constituir una innovación prospectiva o una herramienta meramente experimental, la inteligencia artificial es hoy una realidad plenamente incorporada a múltiples ámbitos de la vida pública y privada, con efectos directos e inmediatos en la toma de decisiones, la organización institucional, la provisión de servicios públicos, los mercados digitales, la seguridad, la educación, la salud, los procesos democráticos y el ejercicio efectivo de los derechos humanos.

En este sentido, la inteligencia artificial no puede comprenderse adecuadamente como un simple fenómeno tecnológico aislado. Se trata de un sistema general de mediación productiva y decisional que opera entre datos, poder público,

mercado y ciudadanía, reconfigurando de manera estructural la forma en que se asignan recursos, se evalúan conductas, se anticipan riesgos y se adoptan decisiones con efectos jurídicos y materiales trascendentes. Su despliegue introduce nuevas formas de intermediación entre información y decisión que inciden directamente en la organización de la producción, la competitividad económica y el funcionamiento de los mercados laborales.

En la actualidad, los sistemas de inteligencia artificial ya intervienen de manera significativa en procesos de identificación y verificación de identidad, evaluación crediticia, asignación de beneficios sociales, vigilancia digital, selección y evaluación de personal, generación automatizada de contenidos, análisis predictivo, administración pública digital, control fronterizo y seguridad nacional, entre otros ámbitos de alta sensibilidad social y jurídica. Esta expansión acelerada ha generado beneficios relevantes en términos de eficiencia, innovación y productividad; sin embargo, también ha puesto de manifiesto riesgos estructurales asociados a la opacidad algorítmica, la discriminación automatizada, la afectación a la privacidad, la vulneración de la integridad cognitiva, la reconfiguración y desaparición de ocupaciones y tareas, y la concentración de poder tecnológico.

Desde una perspectiva funcional y jurídica, la inteligencia artificial constituye además una infraestructura productiva de decisión automatizada, en la medida en que sus resultados influyen —de forma directa o indirecta— en actos administrativos, políticas públicas, servicios esenciales y dinámicas económicas y laborales con consecuencias jurídicas relevantes. La automatización de decisiones, recomendaciones o clasificaciones incide no sólo en la acción del Estado, sino también en la organización del trabajo, la asignación de funciones, la evaluación del desempeño y el acceso a oportunidades económicas, alterando los equilibrios tradicionales entre discrecionalidad humana, responsabilidad institucional y control democrático.

Asimismo, la inteligencia artificial impacta de manera directa en la transformación de los modelos productivos y del mercado laboral, al modificar la forma en que se produce valor, se organizan las cadenas productivas y se estructuran las

relaciones entre capital, trabajo y conocimiento. Estos procesos plantean desafíos relevantes en materia de desaparición de tareas, reconversión laboral, capacitación continua y protección social; pero también abren oportunidades concretas para elevar la productividad, fortalecer sectores estratégicos, generar empleos de mayor valor agregado y facilitar la transición hacia economías más innovadoras y competitivas. La adecuada gobernanza de la inteligencia artificial resulta, por tanto, un elemento clave para que esta transformación productiva contribuya a la inclusión y a la movilidad social.

Ante este escenario, resulta jurídicamente insostenible que el desarrollo y uso de la inteligencia artificial permanezcan al margen de un marco normativo integral. La ausencia de regulación no equivale a neutralidad tecnológica, sino que implica una renuncia tácita del Estado a su deber constitucional de proteger derechos, garantizar seguridad jurídica y orientar el desarrollo tecnológico conforme al interés público. En este sentido, la adopción de una Ley General en materia de inteligencia artificial no constituye una opción política discrecional, sino una obligación jurídica derivada del mandato constitucional de protección de los derechos humanos, de la seguridad nacional y del orden democrático.

La experiencia comparada demuestra que los Estados con sistemas democráticos consolidados han reconocido esta necesidad regulatoria. La Unión Europea ha asumido un enfoque basado en riesgos, orientado a prevenir impactos adversos sobre los derechos fundamentales, garantizar la seguridad y establecer obligaciones diferenciadas según el nivel de dichos riesgos de los sistemas de IA (Comisión Europea, 2024).¹ Este modelo parte del reconocimiento explícito de que la inteligencia artificial, por su capacidad de automatizar decisiones con efectos jurídicos y materiales, requiere controles normativos *ex ante* y *ex post*.

De manera convergente, el Gobierno de los Estados Unidos ha reconfigurado su política federal en materia de inteligencia artificial. En la Orden Ejecutiva

¹ Comisión Europea. (2024). *Ley de IA de la Unión Europea (EU AI Act)*. <https://artificialintelligenceact.eu/the-act/>

Removing Barriers to American Leadership in Artificial Intelligence,² emitida en enero de 2025, se dispuso la revisión y revocación de políticas y directrices previas consideradas obstáculos para la innovación y el liderazgo tecnológico del país. Dicha Orden instruyó, además, la elaboración de un plan de acción federal, orientado a consolidar el liderazgo estadounidense en inteligencia artificial dentro de los límites del marco legal y presupuestario vigente. En cumplimiento de este mandato, en julio de 2025 la Casa Blanca presentó el documento *America's AI Action Plan*,³ que define una hoja de ruta integral para asegurar la primacía de Estados Unidos en el desarrollo y adopción de la inteligencia artificial. El Plan se estructura en torno a tres ejes principales: acelerar la innovación mediante la reducción de cargas regulatorias y el fortalecimiento del sector privado; construir la infraestructura estratégica necesaria —incluyendo centros de datos, semiconductores y capacidad energética—; y liderar la diplomacia y la seguridad internacional en materia de IA.

En un registro distinto, China ha optado por una estrategia regulatoria incremental y pragmática frente a la inteligencia artificial. En lugar de avanzar de inmediato hacia una ley general y comprensiva, el gobierno chino ha priorizado el uso de programas piloto, estándares técnicos y medidas sectoriales específicas, manteniendo así un amplio margen de flexibilidad regulatoria para una tecnología aún en rápida evolución. Este enfoque busca permitir el aprendizaje institucional a partir de la experiencia práctica y de modelos internacionales antes de consolidar un marco normativo unificado.⁴

Por otro lado, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha propuesto una convergencia internacional hacia principios comunes de gobernanza de la inteligencia artificial, centrados en la transparencia, la rendición de cuentas, la robustez técnica y el respeto a los derechos humanos.

² Gobierno de los Estados Unidos. (2025). *Removing Barriers to American Leadership in Artificial Intelligence*. <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>

³ Gobierno de los Estados Unidos. (2025). *AI Action Plan*. <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

⁴ Hu, B., & Au, A. (2025). *China resets the path to comprehensive AI governance*. East Asia Forum. <https://eastasiaforum.org/2025/12/25/china-resets-the-path-to-comprehensive-ai-governance/>

En el análisis de la OCDE sobre el estado de implementación de sus principios sobre IA, se destaca que los países que avanzan en marcos regulatorios integrales logran mayor confianza social, mejores condiciones para la innovación responsable y una reducción de riesgos sistémicos asociados al uso indiscriminado de estas tecnologías.⁵ En el caso de México, país miembro de este bloque, la acelerada adopción de sistemas de inteligencia artificial en sectores estratégicos ha ocurrido en un contexto de fragmentación normativa, vacíos regulatorios y ausencia de criterios homogéneos. Actualmente, la escasa regulación aplicable se encuentra dispersa en distintos ordenamientos sectoriales, sin un marco general que establezca principios rectores, mecanismos de gobernanza, obligaciones diferenciadas por nivel de riesgo ni salvaguardas específicas frente a impactos estructurales como los sesgos algorítmicos, la violencia digital, la afectación a los neuroderechos y la eliminación masiva de puestos de trabajo.

Esta situación genera un doble riesgo: por un lado, expone a las personas a decisiones automatizadas opacas, potencialmente discriminatorias o arbitrarias; y, por otro, produce un entorno de inseguridad jurídica para desarrolladores, proveedores y usuarios de sistemas de inteligencia artificial, lo que dificulta la innovación responsable, la inversión productiva y la planeación de largo plazo. En consecuencia, resulta indispensable dotar al Estado mexicano de una Ley General que permita regular y fomentar de manera transversal el desarrollo, implementación y uso de la inteligencia artificial, garantizando la protección de los derechos humanos, la seguridad nacional, la soberanía tecnológica y el desarrollo económico sostenible.

En este marco, la presente Ley General para Regular y Fomentar el Uso de la Inteligencia Artificial en México se concibe como un instrumento normativo de carácter horizontal, flexible y basado en riesgos, que reconoce el carácter transversal de la inteligencia artificial y su impacto estructural en la sociedad, la economía y el trabajo. Desde estas Consideraciones Generales, se establece

⁵ Organización para la Cooperación y el Desarrollo Económicos. (2020). *State of implementation of the OECD AI Principles*. <https://www.oecd.org/going-digital/ai/state-of-implementation-of-the-oecd-ai-principles.pdf>

que la regulación de la inteligencia artificial no busca frenar la innovación, sino encauzarla de manera responsable, ética y jurídicamente sólida, asegurando que el progreso tecnológico se traduzca en beneficios sociales, productivos y democráticos, sin comprometer la dignidad humana ni los valores constitucionales.

Ahora bien, es importante mencionar que, en el proceso de construcción de la presente Ley General, resulta particularmente relevante destacar los insumos éticos y de política pública generados en el ámbito nacional para orientar el desarrollo y uso responsable de la inteligencia artificial. En este sentido, adquieren especial importancia los *Principios de Chapultepec: Declaración de Ética y Buenas Prácticas para el Uso y Desarrollo de la Inteligencia Artificial en México*, presentados el 29 de enero de 2026 en la Ciudad de México por la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI) y la Agencia de Transformación Digital y Telecomunicaciones (ATDT), en el marco del foro “La inteligencia artificial en la vida pública de México”.⁶

En dicha Declaración se establecen como principios orientadores los siguientes enunciados:

1. La inteligencia artificial debe ampliar derechos, nunca reducirlos.
2. Toda decisión apoyada por inteligencia artificial debe tener responsables humanos, sustentada en marcos institucionales claros.
3. Si una decisión no puede explicarse, no debe automatizarse.
4. La inteligencia artificial se gobierna mejor cuando se decide en colectivo.
5. La inteligencia artificial solo es valiosa si genera bienestar para las personas.
6. Antes de automatizar, hay que comprender a quién y qué afecta.
7. La tecnología estratégica debe responder a las necesidades del país.
8. El desarrollo de la inteligencia artificial requiere fortalecer la educación y el conocimiento en el país.

⁶ Secretaría de Ciencia, Humanidades, Tecnología e Innovación & Agencia de Transformación Digital y Telecomunicaciones (2026). *Principios de Chapultepec: Declaración de Ética y Buenas Prácticas para el Uso y Desarrollo de la Inteligencia Artificial*. <https://www.youtube.com/live/ix7k3FSqy30>

9. La inteligencia artificial no puede ser ajena a la diversidad cultural y lingüística del país.
10. Los datos son un bien público que deben cuidarse con responsabilidad.

En atención a la relevancia sustantiva de estos principios y a su función estructurante dentro del diseño normativo de la presente Ley General, se estimó jurídicamente pertinente elevarlos de su carácter meramente orientador a su incorporación expresa en un artículo específico, el 12 Bis. Ello con el objeto de dotarlos de fuerza normativa directa y evitar que quedaran reducidos a un referente únicamente declarativo o interpretativo. Esta decisión responde a una lógica de técnica legislativa que reconoce a los principios no solo como criterios orientadores, sino como mandatos jurídicos transversales que informan la interpretación, aplicación y desarrollo integral del ordenamiento en materia de inteligencia artificial.

La incorporación de los diez principios en un artículo autónomo permite, además, asegurar coherencia sistemática entre los fundamentos éticos nacionales y las disposiciones operativas de la Ley, al tiempo que proporciona un anclaje claro para la actuación de las autoridades competentes, pero también la de desarrolladores, proveedores y usuarios de sistemas de inteligencia artificial actuando en México. Asimismo, esta técnica evita la dispersión normativa y fortalece una potencial exigibilidad jurídica de los principios, permitiendo que estos sean invocados tanto en la elaboración de políticas públicas y lineamientos técnicos, como en procedimientos administrativos, actos de supervisión, control y, en su caso, en la determinación de responsabilidades. Con ello, se garantiza que el desarrollo, uso, fomento y regulación de la inteligencia artificial en México se encuentren permanentemente guiados por un marco ético claro, coherente con los valores constitucionales, el interés público y una visión de Estado orientada al bienestar social, la protección de derechos y la gobernanza democrática de la tecnología.

La presente Ley General traduce estos *Principios* en criterios normativos estructurados, que orientan el contenido material de sus Títulos. Así, el principio conforme al cual la IA debe ampliar derechos y nunca reducirlos se refleja en la

definición de un núcleo axiológico expreso en el Título Segundo, dedicado a los principios éticos, los derechos humanos y los neuroderechos, y se proyecta transversalmente en los Títulos Noveno y Décimo, que incorporan un enfoque de regulación basada en riesgos, así como en el Título Séptimo, que establece obligaciones específicas para prevenir sesgos algorítmicos, violencia digital y exclusión estructural.

El principio de responsabilidad humana en toda decisión apoyada por inteligencia artificial, previsto en el artículo 160 Bis, establece de manera expresa que dicho apoyo tecnológico no exime ni atenúa la responsabilidad correspondiente. Este principio se refleja en el resto de la arquitectura normativa a través del Título Décimo Primero, que define los derechos y obligaciones de los distintos sujetos que intervienen en el ciclo de vida de los sistemas de IA, conforme a su grado de control y responsabilidad. Asimismo, se refuerza mediante los mecanismos de transparencia y rendición de cuentas del Título Décimo Segundo, los procedimientos administrativos, de supervisión y corrección del Título Décimo Tercero y el régimen de infracciones y sanciones del Título Décimo Cuarto, garantizando que la automatización decisional no sustituya ni diluya la responsabilidad humana.

Por su parte, el principio conforme al cual una decisión que no puede explicarse no debe automatizarse se traduce en exigencias normativas distribuidas a lo largo del ordenamiento. En el Título Segundo opera como criterio rector; en el Título Noveno, mediante la evaluación de impacto algorítmico y la clasificación de riesgos; y en el Título Décimo Segundo, a través de registros y obligaciones de información. Dicho principio se refuerza en el Título Décimo Tercero, mediante mecanismos de auditoría, supervisión y revisión administrativa, y se complementa con el Título Décimo Primero, al reconocer derechos de las personas usuarias y obligaciones específicas para los sujetos que intervienen en el ciclo de vida de los sistemas de IA, conforme a su grado de responsabilidad y control. Finalmente, el Título Décimo Cuarto prevé las consecuencias jurídicas frente al incumplimiento de los deberes de transparencia, trazabilidad y explicabilidad.

El principio de gobernanza colectiva se incorpora de manera institucional en el Título Tercero, que diseña un modelo de coordinación multinivel y participación social, y se vincula con el Título Cuarto, que establece la Estrategia Nacional de Inteligencia Artificial como instrumento de política pública y planeación de largo plazo, reconociendo que la legitimidad y eficacia de la regulación dependen de procesos deliberativos amplios y orientados al interés público.

El principio conforme al cual la inteligencia artificial solo es valiosa si genera bienestar para todas las personas se refleja en el Título Cuarto, al orientar la Estrategia Nacional y la política pública hacia el valor público, la ampliación de derechos y la mejora del acceso a servicios esenciales; en el Título Sexto, mediante alfabetización, ciudadanía digital y formación de capacidades para un uso crítico y beneficioso; y en el Título Octavo, al vincular el fomento a la innovación con objetivos de desarrollo social y productivo.

El principio conforme al cual, antes de automatizar, es indispensable comprender a quién y a qué afecta una decisión se operacionaliza, en primer término, a través del Título Noveno, que incorpora la evaluación de impacto y la gestión continua de riesgos, así como del Título Décimo, que establece controles diferenciados para los sistemas de alto riesgo y las aplicaciones prohibidas. Dicho principio se articula, además, con el Título Cuarto, relativo a la planeación, evaluación y criterios de política pública y, en su dimensión de impactos sociales diferenciados, con el Título Séptimo.

Respecto del principio conforme al cual la tecnología estratégica debe responder a las necesidades del país, éste se proyecta en el Título Cuarto, al establecer la Estrategia Nacional de Inteligencia Artificial como instrumento rector de visión de largo plazo; en el Título Quinto, al ordenar la conducción institucional y la coordinación entre autoridades competentes; y en el Título Octavo, al incorporar mecanismos de fomento, financiamiento e innovación orientados al fortalecimiento de capacidades nacionales y a la soberanía tecnológica.

Por su parte, el principio conforme al cual el desarrollo de la inteligencia artificial requiere fortalecer la educación y el conocimiento en el país se refleja de manera

directa en el Título Sexto, a través de disposiciones en materia de alfabetización y ciudadanía digital, formación docente, desarrollo de talento especializado y programas de capacitación para los sectores público y privado. Dicho principio se complementa con el Título Octavo, al fomentar la investigación científica y tecnológica, la innovación y la cooperación para la generación de conocimiento, incluyendo enfoques interdisciplinarios que integren ciencias, tecnologías, humanidades y saberes sociales.

El principio conforme al cual la inteligencia artificial no puede ser ajena a la diversidad cultural y lingüística del país se vincula, en primer término, con el Título Séptimo, al establecer obligaciones de inclusión y no discriminación que exigen considerar la diversidad social y cultural en el diseño y despliegue de los sistemas de IA. Asimismo, se relaciona con el Título Sexto, al prever disposiciones de formación y cultura digital con enfoque incluyente. Dicho principio también se alinea con el Título Cuarto, en la medida en que la política pública y la Estrategia Nacional permiten orientar acciones para recuperar, fortalecer y preservar las lenguas indígenas, así como construir acervos lingüísticos que posibiliten el entrenamiento y uso de sistemas de IA desde la realidad cultural de México.

Finalmente, el principio conforme al cual los datos constituyen un bien público que debe cuidarse con responsabilidad se traduce normativamente en el Título Segundo, al incorporar salvaguardas en materia de privacidad, protección de datos personales y ciberseguridad como parte del núcleo de derechos aplicables a la inteligencia artificial; en el Título Décimo Segundo, mediante obligaciones de transparencia, rendición de cuentas, datos abiertos responsables y mecanismos de acceso ciudadano a la información; y en el Título Noveno, al reconocer que la calidad, representatividad y seguridad de los datos constituyen factores determinantes en la evaluación y gestión de riesgos de los sistemas de inteligencia artificial a lo largo de todo su ciclo de vida.

De esta forma, los *Principios de Chapultepec* operan como eje articulador del capitulado, permitiendo que cada Título de la Ley responda a un fundamento ético específico y asegurando que el marco normativo resultante sea coherente,

exigible y alineado con los valores constitucionales, el interés público y una visión de Estado en materia de inteligencia artificial.

En este contexto, la regulación de la inteligencia artificial no constituye una reacción coyuntural ni una apuesta circunstancial del legislador, sino una expresión necesaria de la función esencial del Estado: orientar el progreso tecnológico conforme a los valores constitucionales, garantizar la dignidad humana y asegurar que el desarrollo científico esté al servicio de la sociedad. La ausencia de regulación no implica neutralidad, sino abandono de responsabilidades públicas frente a riesgos que ya se manifiestan de manera concreta y verificable en la vida democrática, económica y social.

Como advirtiera Norberto Bobbio, *“el problema de fondo relativo a los derechos humanos no es hoy tanto el de justificarlos como el de protegerlos”* (Bobbio, 1991: 15).⁷ En el ámbito de la inteligencia artificial, esta afirmación adquiere plena vigencia: el desafío contemporáneo no radica únicamente en reconocer nuevos derechos frente a tecnologías emergentes, sino en dotar al orden jurídico de instrumentos eficaces que permitan hacerlos exigibles, previniendo daños, corrigiendo asimetrías y asegurando un desarrollo tecnológico compatible con el Estado constitucional y democrático de derecho.

II. Justificación Constitucional

La expedición de una Ley General para Regular y Fomentar el Uso de la Inteligencia Artificial en México encuentra sustento directo en el bloque de constitucionalidad mexicano, particularmente en la obligación del Estado de reconocer, garantizar y proteger derechos humanos frente a riesgos emergentes derivados del uso intensivo de tecnologías digitales.

En primer término, el artículo 1º constitucional, que establece el principio *pro persona*, ordena interpretar las normas de derechos humanos favoreciendo en todo tiempo la protección más amplia, y dispone el deber de todas las

⁷ Bobbio, N. (1991). *El tiempo de los derechos*, p. 15.

autoridades de promover, respetar, proteger y garantizar tales derechos, así como prevenir, investigar, sancionar y reparar sus violaciones. En consecuencia, cuando la inteligencia artificial incide en libertades, igualdad, privacidad, integridad personal o acceso a servicios públicos, el Estado no puede permanecer en un plano meramente declarativo: debe regular para proteger.

En el mismo eje, el texto constitucional reconoce que la vida democrática contemporánea se desarrolla en un entorno informacional y digital que incide directamente en el ejercicio efectivo de los derechos fundamentales. El artículo 6º garantiza el derecho a la información y el libre acceso a información plural y oportuna, así como la libertad de buscar, recibir y difundir información e ideas por cualquier medio; además, establece la obligación del Estado de garantizar el acceso a las tecnologías de la información y comunicación, incluida la banda ancha e Internet.

Esto es constitucionalmente relevante porque la inteligencia artificial —en particular la IA generativa, los sistemas de recomendación y la moderación automatizada— puede alterar los flujos informativos, amplificar desinformación, moldear percepciones públicas y afectar el derecho a recibir información veraz, plural y oportuna. Por su parte, el artículo 7º refuerza la inviolabilidad de la libertad de difusión de ideas, prohibiendo restricciones indirectas mediante controles o tecnologías que impidan la circulación de opiniones e información. De ahí que el diseño legal deba prever salvaguardas frente a usos dolosos, intencionales o perjudiciales de la inteligencia artificial que afecten la deliberación pública, la libertad de expresión y la integridad del debate democrático, incluidos aquellos supuestos vinculados con procesos democráticos y electorales, así como con la desinformación en dichos contextos.

A su vez, la regulación de la inteligencia artificial se justifica como una exigencia de seguridad jurídica y debido proceso, conforme a los artículos 14 y 16 de la Constitución. El artículo 14 proscribela aplicación retroactiva de la ley en perjuicio de persona alguna y exige que toda privación de derechos se realice mediante juicio seguido ante tribunales previamente establecidos, en el que se cumplan las formalidades esenciales del procedimiento. Por su parte, el artículo

16 dispone que nadie puede ser molestado sino en virtud de mandamiento escrito que funde y motive la causa legal del procedimiento, y reconoce expresamente el derecho a la protección de los datos personales —acceso, rectificación, cancelación y oposición—, estableciendo que la ley fijará los supuestos de excepción por razones de seguridad nacional, orden público, seguridad y salud públicas, o derechos de terceros.

En este marco, cuando sistemas de inteligencia artificial intervienen en decisiones de alto impacto —por ejemplo, en salud y servicios públicos, en vigilancia y ciberseguridad, en asignación de beneficios, en diseño de infraestructura, en perfiles de riesgo o en decisiones automatizadas— resulta constitucionalmente imprescindible asegurar:

- 1) trazabilidad y fundamentación de decisiones públicas;
- 2) controles de legalidad;
- 3) garantías de impugnación; y
- 4) protección reforzada de datos, particularmente ante tratamientos masivos y automatizados.

La dimensión económica también reviste una relevancia constitucional directa. El artículo 28 establece la prohibición de monopolios y el deber del Estado de promover la competencia y el funcionamiento eficiente de los mercados, lo cual adquiere especial importancia en la economía digital. En este contexto, la inteligencia artificial puede generar dinámicas de concentración derivadas de economías de escala, efectos de red y ventajas asociadas al uso intensivo de datos, con impactos potenciales sobre la libre competencia, la innovación y los derechos de los consumidores. Desde esta perspectiva, un marco jurídico en materia de inteligencia artificial no busca inhibir la actividad empresarial ni el desarrollo tecnológico, sino ofrecer certidumbre, reducir asimetrías informativas y favorecer condiciones de competencia leal, contribuyendo a mercados digitales más dinámicos, abiertos y orientados al interés público.

La construcción normativa bajo el carácter de ley general se sustenta en el artículo 73, que faculta al Congreso para expedir leyes generales que establezcan bases y distribución de competencias, permitiendo un marco

nacional uniforme con implementación coordinada entre Federación, entidades federativas y municipios, conforme a un diseño de gobernanza multinivel. Esta técnica es especialmente idónea para la inteligencia artificial por su carácter transversal: su uso cruza sectores (salud, educación, seguridad, economía, procesos electorales, telecomunicaciones, trabajo, medio ambiente, y otros) y niveles de gobierno, y exige mínimos comunes normativos para prevenir fragmentación regulatoria, vacíos de supervisión y desigualdad de estándares en el territorio nacional.

En suma, el Estado mexicano se encuentra obligado a adoptar un marco jurídico general que materialice el mandato del artículo 1º, garantice derechos informacionales y de libertad (6º y 7º), preserve la seguridad jurídica y la protección de datos (14 y 16), y ordene los mercados digitales bajo criterios de competencia (28), mediante un instrumento general habilitado por la competencia legislativa del Congreso (73).⁸

Por otra parte, es importante mencionar que la Suprema Corte de Justicia de la Nación (SCJN) ha sostenido de manera reiterada que el contenido de los derechos fundamentales no es estático, sino que debe interpretarse de forma evolutiva y contextual, atendiendo a las transformaciones sociales, tecnológicas y económicas que inciden en su ejercicio efectivo. En este sentido, el Tribunal Constitucional ha reconocido que el principio de legalidad y la protección de derechos exigen que el legislador anticipe riesgos estructurales cuando nuevas tecnologías pueden afectar de manera masiva o sistemática a las personas, incluso antes de que se materialicen daños concretos (SCJN, 2014).⁹

Bajo esta lógica, la inteligencia artificial constituye un nuevo entorno de riesgo constitucionalmente relevante, en tanto su diseño y uso inciden en derechos cuya protección ha sido expresamente reconocida por la Constitución y desarrollada por la jurisprudencia: el derecho a la igualdad y no discriminación,

⁸ Constitución Política de los Estados Unidos Mexicanos. (1917, última reforma vigente). *Artículos 1, 6, 7, 14, 16, 28 y 73.* www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

⁹ Suprema Corte de Justicia de la Nación. (2014). *Derechos humanos. Su interpretación conforme al principio pro persona.* Tesis aislada, Décima Época. Semanario Judicial de la Federación.

la protección de datos personales, la libertad de expresión, el acceso a la información, el debido proceso y la seguridad jurídica. La omisión legislativa frente a estos riesgos no es neutra, sino que puede traducirse en una falla estructural del deber de garantía del Estado, particularmente cuando decisiones automatizadas sustituyen, alteran o condicionan decisiones humanas con efectos jurídicos o materiales relevantes.

Desde la doctrina constitucional, Luigi Ferrajoli ha advertido que el constitucionalismo contemporáneo impone al legislador no solo deberes de abstención, sino deberes positivos de regulación, especialmente frente a poderes fácticos capaces de afectar derechos fundamentales de manera difusa o asimétrica. En palabras del autor, *“cuando los poderes tecnológicos y económicos desbordan los límites del control jurídico, la ausencia de regulación se convierte en una forma de irresponsabilidad constitucional”* (Ferrajoli, 2011: 45).¹⁰ Esta reflexión resulta plenamente aplicable al fenómeno de la inteligencia artificial, cuyo despliegue sin reglas claras puede generar concentraciones de poder, opacidad decisional y vulneraciones sistemáticas de derechos.

En coherencia con este marco, el articulado de la presente Ley General se concibe como un instrumento de concreción normativa de los mandatos constitucionales previamente expuestos. Así, el glosario técnico contenido en el Título Primero no cumple una función meramente definitoria, sino que constituye una garantía de seguridad jurídica, al precisar conceptos como inteligencia artificial, sistemas de alto riesgo, sesgo algorítmico, explicabilidad y evaluación de impacto algorítmico, entre otros. Estas definiciones permiten operativizar los artículos 1º, 6º, 7º y 16 constitucionales, al asegurar que la protección de derechos humanos, la libertad de información, la privacidad y el debido proceso se apliquen de manera efectiva en entornos automatizados y técnicamente complejos.

¹⁰ Ferrajoli, L. (2011). *Poderes salvajes: La crisis de la democracia constitucional*. Trotta, p. 45.

De igual forma, el enfoque de regulación basada en riesgos, desarrollado a lo largo del articulado, constituye la traducción normativa del principio pro persona y del deber de prevención que deriva del artículo 1º constitucional. Al establecer obligaciones diferenciadas según el nivel de impacto de los sistemas de inteligencia artificial, la Ley garantiza una intervención estatal proporcional, razonable y justificada, evitando tanto la sobrerregulación innecesaria como la omisión frente a usos de alto riesgo que puedan afectar derechos fundamentales, procesos democráticos, la ciberseguridad o la prestación de servicios públicos esenciales.

Por otra parte, los mecanismos de gobernanza, coordinación interinstitucional y la Estrategia Nacional en materia de inteligencia artificial, previstos en los Títulos correspondientes, encuentran su sustento directo en el artículo 73 constitucional, al configurar una ley general que distribuye competencias, fija bases mínimas comunes y promueve la interoperabilidad normativa entre niveles de gobierno. Este diseño responde a la naturaleza transversal de la inteligencia artificial y previene la fragmentación regulatoria, asegurando coherencia, eficacia y responsabilidad institucional.

Finalmente, las disposiciones relativas a competencia económica, mercados digitales y prevención de concentraciones indebidas, desarrolladas en el articulado, materializan el mandato del artículo 28 constitucional, al reconocer que la inteligencia artificial puede convertirse en un factor de distorsión del mercado cuando se concentra en pocos actores con control de datos, infraestructuras y modelos algorítmicos. La Ley, en consecuencia, no solo protege derechos individuales, sino que resguarda el interés público en la economía digital, fomentando una innovación abierta, competitiva y socialmente responsable.

Por último, la presente Ley General se configura como una norma de desarrollo constitucional, que no crea derechos *ex novo*, sino que actualiza y hace exigibles los derechos ya reconocidos por la Constitución frente a los desafíos que plantea la inteligencia artificial. De esta manera, el legislador cumple con su deber de

garantía, prevención y regulación, asegurando que el progreso tecnológico se encuentre subordinado al Estado constitucional y democrático de derecho.

III. Motivación Técnica y Legislativa

El desarrollo, adopción y despliegue de sistemas de inteligencia artificial en México se ha producido de manera acelerada y, en muchos casos, desarticulada, en un entorno normativo caracterizado por la dispersión, la insuficiencia regulatoria y la ausencia de criterios técnicos homogéneos para su diseño, implementación, supervisión y evaluación. Si bien el orden jurídico mexicano cuenta con disposiciones aplicables de manera indirecta en ámbitos como la protección de datos personales, las telecomunicaciones, la competencia económica, la salud, la educación, el trabajo, la seguridad pública o la seguridad nacional, dichas normas han sido concebidas para contextos tecnológicos distintos y responden a lógicas sectoriales, fragmentadas y predominantemente reactivas. Esta situación impide ofrecer una respuesta jurídica integral frente a una tecnología que opera de manera transversal, sistémica y acumulativa.

Desde una perspectiva técnica, esta fragmentación normativa genera efectos adversos tanto para la protección de derechos como para el desarrollo ordenado de la innovación. Por un lado, las personas quedan expuestas a decisiones automatizadas cuyo funcionamiento resulta opaco, difícilmente explicable y, en ocasiones, imposible de impugnar de manera efectiva. Por otro, desarrolladores, proveedores, operadores y usuarios de sistemas de inteligencia artificial enfrentan altos niveles de incertidumbre jurídica, derivados de la inexistencia de reglas claras sobre responsabilidades, estándares técnicos mínimos, obligaciones de diligencia y criterios de evaluación de riesgos. Esta combinación de vulnerabilidad ciudadana e inseguridad regulatoria constituye uno de los principales déficits que la presente Ley General busca atender.

La motivación técnica de esta iniciativa parte del reconocimiento de que la inteligencia artificial ha dejado de ser un conjunto de aplicaciones aisladas para convertirse en una infraestructura productiva y decisional, integrada de manera

creciente en procesos estratégicos de la vida económica, social y administrativa del país. Los sistemas de inteligencia artificial participan hoy en actividades de planeación, logística, evaluación, predicción, optimización y asignación de recursos, tanto en el sector público como en el privado. Su incorporación modifica sustantivamente la forma en que se toman decisiones, se gestionan riesgos, se organizan cadenas productivas y se distribuyen oportunidades económicas.

Adicionalmente, el marco jurídico vigente no incorpora de manera expresa principios comunes que orienten el desarrollo y uso de la inteligencia artificial conforme a valores constitucionales y democráticos. La ausencia de principios como la explicabilidad, la responsabilidad algorítmica, la supervisión humana significativa, la no discriminación, la rendición de cuentas y la protección de la propiedad intelectual e industrial dificulta una aplicación coherente del derecho frente a tecnologías cuyo funcionamiento técnico resulta complejo y, en muchos casos, opaco incluso para personas expertas. La OCDE ha señalado que la falta de principios transversales debilita la confianza pública en la inteligencia artificial y reduce la eficacia de los sistemas de gobernanza tecnológica (OCDE, 2020).¹¹

Otro elemento crítico es la inexistencia de un enfoque normativo basado en riesgos. En el derecho mexicano vigente no se distingue entre sistemas de inteligencia artificial de bajo impacto y aquellos que, por su finalidad o contexto de uso, pueden afectar de manera significativa derechos humanos, procesos democráticos, la salud pública o la seguridad nacional. Esta ausencia conduce a dos escenarios igualmente problemáticos: la sobrerregulación indiscriminada de usos de bajo riesgo o, por el contrario, la falta de controles suficientes sobre aplicaciones de alto riesgo. La experiencia comparada sugiere que los enfoques regulatorios basados en riesgos permiten articular un equilibrio razonable entre innovación y protección de derechos, mediante la asignación de obligaciones proporcionales y diferenciadas (Comisión Europea, 2024). En paralelo, la

¹¹ Organización para la Cooperación y el Desarrollo Económicos. (2020). *State of implementation of the OECD AI Principles*. <https://www.oecd.org/going-digital/ai/state-of-implementation-of-the-oecd-ai-principles.pdf>

inteligencia artificial plantea desafíos inéditos en materia de seguridad nacional y soberanía digital. El control de datos estratégicos, el uso de sistemas automatizados en infraestructuras críticas, la dependencia tecnológica de proveedores extranjeros y la utilización de IA en contextos de ciberseguridad, defensa y control de la información exigen una respuesta normativa que trascienda enfoques sectoriales aislados.

En este contexto, la creación de una Ley General en materia de inteligencia artificial se justifica como el instrumento legislativo idóneo para coordinar, armonizar y orientar la regulación presente y futura. Desde una perspectiva técnica y legislativa, la presente Ley General no sustituye ni invade ámbitos normativos existentes; los articula y complementa, proporcionando una base normativa uniforme que previene vacíos, reduce la fragmentación y fortalece la capacidad institucional del Estado para gestionar tecnologías de alto impacto. De este modo, la Ley se configura como un instrumento de política pública normativa que garantiza seguridad jurídica, fomenta la innovación responsable y asegura que el desarrollo de la inteligencia artificial se encuentre alineado con los derechos humanos, el interés público y la soberanía tecnológica nacional.

En concordancia con lo anterior, la motivación técnica y legislativa de la presente Ley General se ve reforzada por los diagnósticos empíricos y especializados obtenidos a partir de seis conversatorios en materia de IA, así como diversas mesas de análisis y ejercicios de deliberación técnica realizados en el seno de la Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México, del Senado de la República, durante el periodo 2024–2025. Dichos espacios constituyeron un insumo sustantivo para identificar, desde una perspectiva plural y multisectorial, las principales debilidades del marco jurídico vigente frente al uso creciente de sistemas de inteligencia artificial.

De manera reiterada, los 72 panelistas invitados a los conversatorios —provenientes de la academia, el sector privado, organismos internacionales, cuerpos diplomáticos, sociedad civil especializada y dependencias federales, y mismos que en conjunto produjeron 251 intervenciones— coincidieron en que

México carece actualmente de un marco normativo integral y articulado que permita abordar la inteligencia artificial como una tecnología transversal, con impactos simultáneos en ámbitos como los derechos humanos, la economía digital, la seguridad, la educación, la salud y los procesos democráticos. Esta carencia se traduce en respuestas regulatorias fragmentadas, reactivas y sectoriales, incapaces de anticipar riesgos sistémicos o de ofrecer certeza jurídica a los distintos actores del ecosistema.

Uno de los principales hallazgos de los conversatorios fue la ausencia de criterios comunes para identificar, gestionar y promover el buen uso de la inteligencia artificial, particularmente en el sector público. Se señaló que, en la práctica institucional, no existen metodologías compartidas para evaluar impactos algorítmicos, ni mecanismos obligatorios de auditoría, trazabilidad o supervisión humana en aplicaciones de alto riesgo, especialmente en ámbitos como la seguridad pública, la salud, los sistemas de bienestar social, la educación y los procesos electorales. Esta situación genera un escenario de asimetría regulatoria, en el que tecnologías con efectos potencialmente graves operan sin controles diferenciados ni obligaciones proporcionales.

Asimismo, los diagnósticos derivados de las transcripciones de los conversatorios y demás ejercicios de *escucha activa*, evidenciaron una preocupación transversal por la reproducción de sesgos, discriminación y exclusión mediante sistemas automatizados. Se documentó que el uso de inteligencia artificial entrenada con datos históricos o no representativos tiende a amplificar desigualdades estructurales, afectando de manera desproporcionada a mujeres, personas con discapacidad, comunidades indígenas, personas migrantes y otros grupos en situación de vulnerabilidad. Esta constatación técnica refuerza la necesidad de incorporar principios explícitos de equidad, no discriminación y evaluación de impacto algorítmico en un marco legal de alcance general.¹²

¹² Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México. (2025). *Transcripciones y relatorías de los conversatorios en materia de inteligencia*

Otro elemento central identificado en los conversatorios fue la insuficiente capacidad institucional del Estado para supervisar tecnologías complejas y volátiles, como la IA, derivada tanto de la falta de atribuciones claras como de la inexistencia de mecanismos formales de coordinación interinstitucional. Diversos expertos subrayaron que la dispersión de competencias entre dependencias y niveles de gobierno dificulta la respuesta oportuna frente a incidentes algorítmicos, fallas sistémicas o usos indebidos de la inteligencia artificial, particularmente cuando estos involucran infraestructuras críticas, ciberseguridad o información estratégica.

En materia de seguridad nacional y soberanía digital, los conversatorios pusieron de relieve la dependencia creciente de tecnologías, modelos y plataformas desarrolladas fuera del país, así como la concentración del control de datos y capacidades de cómputo en un número reducido de actores globales. Esta situación fue identificada como un riesgo estratégico, que exige una respuesta normativa capaz de fortalecer capacidades nacionales, establecer salvaguardas sobre el uso de datos estratégicos y promover un desarrollo tecnológico alineado con el interés público y la autonomía del Estado mexicano.

Finalmente, los insumos recogidos coincidieron en que la ausencia de una ley general dificulta la planeación de políticas públicas coherentes en materia de inteligencia artificial, limita la inversión y debilita la confianza social en estas tecnologías. En este sentido, los conversatorios, mesas y otros ejercicios de deliberación con el ecosistema de la IA en México respaldaron de manera consistente la conveniencia de un marco normativo horizontal, basado en riesgos y principios, que sirva como eje articulador para regulaciones sectoriales futuras y como referencia común para autoridades, desarrolladores, proveedores y usuarios.

En conjunto, los diagnósticos derivados de los conversatorios confirman que la expedición de la presente Ley General no responde únicamente a una

artificial. Senado de la República.

https://comisiones.senado.gob.mx/inteligencia_artificial/images/noticias/Transcripciones_2024-2025.pdf

construcción teórica o a la adopción acrítica de modelos internacionales, sino a necesidades reales, documentadas y verificables detectadas por el ecosistema de la IA en México. Estos insumos técnicos y empíricos fortalecen la motivación legislativa y justifican la adopción de un instrumento normativo integral que permita anticipar riesgos, proteger derechos, fortalecer capacidades institucionales y orientar el desarrollo tecnológico de manera responsable y soberana.¹³

IV. Experiencia Internacional Comparada

El análisis de la experiencia internacional en materia de inteligencia artificial evidencia una convergencia normativa clara hacia modelos de regulación que reconocen el carácter transversal, estratégico y de alto impacto de estas tecnologías. Si bien los enfoques adoptados por distintos Estados y organismos internacionales presentan variaciones institucionales y técnicas, es posible identificar ejes comunes que orientan la gobernanza contemporánea de la inteligencia artificial: la protección de los derechos fundamentales, la seguridad y confiabilidad de los sistemas, y la construcción de marcos institucionales de supervisión y rendición de cuentas.

En el ámbito de la Unión Europea, la Ley de IA representa el esfuerzo más avanzado de regulación integral y vinculante. Este instrumento parte del reconocimiento de que la inteligencia artificial puede generar peligros sistémicos y propone un enfoque basado en riesgos, que clasifica los sistemas conforme a su impacto potencial sobre los derechos fundamentales, la seguridad y el orden público. El modelo europeo prioriza la prevención *ex ante*, la transparencia, la trazabilidad y la responsabilidad de los actores involucrados, sin impedir el desarrollo de la innovación tecnológica (Comisión Europea, 2024).¹⁴ Este

¹³ Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México. (2025). *Informe de los conversatorios 2024–2025*. Senado de la República.

¹⁴ Comisión Europea. (2024). *Ley de IA de la Unión Europea (EU AI Act)*. <https://artificialintelligenceact.eu/the-act/>

enfoque confirma la tendencia a sustituir esquemas puramente autorregulatorios por marcos jurídicos obligatorios, orientados a salvaguardar el interés público.

Por su parte, el Reino Unido ha optado por un enfoque regulatorio basado en principios transversales, aplicables a través de las autoridades sectoriales existentes. Si bien no se ha adoptado una ley única de inteligencia artificial, el modelo británico enfatiza valores como la seguridad, la equidad, la transparencia, la explicabilidad y la rendición de cuentas, promoviendo su integración progresiva en la actuación de los reguladores (UK Government, 2023).¹⁵ Este esquema demuestra que, incluso en contextos de flexibilidad regulatoria, existe un consenso sobre la necesidad de orientar el desarrollo de la IA mediante principios comunes, especialmente cuando se trata de tecnologías con impacto social significativo.

En los Estados Unidos, la política pública en materia de inteligencia artificial adoptó en 2025 un enfoque marcadamente estratégico y competitivo, en el que la IA es concebida como un vector central de poder económico, científico y geopolítico. Su *AI Action Plan (2025)* despliega una agenda operativa que combina desregulación selectiva, fortalecimiento de capacidades estatales y una estrecha articulación con el sector privado. El Plan prioriza la adopción acelerada de IA en el propio gobierno federal —incluidas agencias civiles, de defensa e inteligencia—, impulsa inversiones en interpretabilidad, control y robustez de modelos avanzados, y establece mecanismos de evaluación, respuesta a incidentes y protección de infraestructuras críticas. Asimismo, vincula el desarrollo de la IA con la política industrial, la seguridad energética, la formación de la fuerza laboral y la proyección internacional de estándares tecnológicos, confirmando que, aun sin un esquema regulatorio único de carácter general, la gobernanza de la IA es tratada como un asunto de planificación estatal de largo plazo y de coordinación interinstitucional del más alto nivel.

En el caso de China, la gobernanza de la inteligencia artificial ha seguido una trayectoria gradual y administrativa, caracterizada por la combinación de

¹⁵ UK Government. (2023). *A pro-innovation approach to AI regulation*.
<https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach>

regulaciones específicas, estándares técnicos y supervisión estatal intensiva, sin la adopción —hasta ahora— de una ley general única en la materia. Desde 2023, el Estado chino ha establecido un marco específico para los servicios de inteligencia artificial generativa, complementado posteriormente con normas obligatorias de etiquetado de contenidos generados por IA y con estándares nacionales de ciberseguridad aplicables al entrenamiento de modelos, la anotación de datos y la prestación de servicios. Este esquema se apoya en un enfoque de supervisión diferenciada, que somete a mayores controles a los sistemas con capacidad de influir en la opinión pública o movilizar socialmente, e integra la IA dentro de un entramado más amplio de normas sobre protección de datos, seguridad de la información, ética científica y propiedad intelectual.¹⁶

A nivel multilateral, la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO constituye el primer instrumento normativo global adoptado por consenso de los 193 Estados miembros. Esta Recomendación articula un marco ético basado en derechos humanos, dignidad, diversidad cultural, igualdad de género, sostenibilidad y responsabilidad, y exhorta a los Estados a traducir dichos principios en políticas públicas y marcos legales efectivos (UNESCO, 2021). El documento subraya que la ausencia de regulación puede profundizar desigualdades existentes y generar impactos adversos irreversibles, particularmente para grupos históricamente marginados.¹⁷

En conjunto, estas experiencias revelan una tendencia global común: la inteligencia artificial ya no es concebida únicamente como una herramienta técnica, sino como un fenómeno que requiere gobernanza democrática, seguridad jurídica y protección reforzada de derechos fundamentales. Los modelos analizados coinciden en la necesidad de marcos normativos que articulen principios, obligaciones y mecanismos de supervisión, adaptados a los riesgos específicos de cada contexto nacional.

¹⁶ White & Case. (2025). *AI Watch: Global regulatory tracker - China*. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china>

¹⁷ UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

En este marco, el modelo mexicano se alinea con las mejores prácticas internacionales al adoptar un enfoque horizontal, basado en riesgos y sustentado en derechos humanos; sin embargo, incorpora elementos innovadores que responden tanto a las particularidades constitucionales, sociales y culturales del país como a la vanguardia en investigación científica y desarrollo tecnológico. De manera destacada, la presente Ley incorpora de forma explícita la protección de los neuroderechos, reconociendo la necesidad de salvaguardar la integridad cognitiva, la privacidad mental y la autonomía de la voluntad frente a tecnologías capaces de intervenir, influir o condicionar procesos neuronales y cognitivos. Esta previsión resulta particularmente relevante ante el uso creciente de sistemas de inteligencia artificial en contextos de persuasión algorítmica, interfaces cerebro-computadora, análisis conductual y toma automatizada de decisiones, donde la frontera entre el tratamiento de datos y la afectación directa de la esfera mental se vuelve cada vez más difusa. Asimismo, integra un Título específico sobre perspectiva de género, inclusión y no discriminación, atendiendo la evidencia internacional que demuestra que los sistemas de inteligencia artificial tienden a reproducir y amplificar sesgos estructurales.

De este modo, la experiencia internacional comparada no se adopta como un modelo a transcribir, sino como un referente analítico que confirma la pertinencia y oportunidad de la presente Ley General. El diseño normativo propuesto permite a México insertarse en la convergencia global hacia una gobernanza responsable de la inteligencia artificial, al tiempo que fortalece su soberanía tecnológica, su compromiso con los derechos humanos y su capacidad para orientar el desarrollo tecnológico conforme al interés público.

En este contexto de convergencia global, la regulación de la inteligencia artificial se inscribe en una evolución natural del constitucionalismo contemporáneo, que reconoce que el ejercicio efectivo de los derechos fundamentales depende cada vez más de la capacidad del Estado para gobernar tecnologías complejas. Como señala Jürgen Habermas, *“el progreso técnico no es en sí mismo emancipador; solo lo es cuando se encuentra institucionalmente integrado en un orden jurídico que garantice la autonomía y la dignidad de las personas”*. Esta reflexión resulta particularmente pertinente en el ámbito de la inteligencia artificial, donde la

ausencia de reglas claras puede transformar la innovación en un factor de exclusión o dominación.¹⁸

Bajo estas premisas, la presente Ley General se concibe como un instrumento que permite a México incorporarse a la tendencia internacional de gobernanza responsable de la inteligencia artificial, no mediante la simple adopción de modelos externos, sino a través de un diseño normativo propio que articula derechos humanos, seguridad, inclusión y soberanía tecnológica.

V. Consideraciones Metodológicas

“La calidad de una ley no depende únicamente de su contenido normativo, sino del método mediante el cual ha sido concebida, discutida y sistematizada; una legislación sin metodología es, en esencia, una decisión sin racionalidad.” — **Manuel Atienza**.¹⁹

La Ley General para Regular y Fomentar el Uso de la Inteligencia Artificial en México se construyó a partir de una metodología legislativa rigurosa, deliberada y plural, orientada a asegurar que el marco normativo propuesto responda no solo a una necesidad política inmediata, sino a un proceso racional de análisis jurídico, técnico y social, acorde con los principios de buena regulación, seguridad jurídica y coherencia normativa. Esta metodología permitió estructurar un marco constitucionalmente sólido y socialmente pertinente, capaz de atender la complejidad, transversalidad y dinamismo que caracterizan a la inteligencia artificial como infraestructura decisional y productiva contemporánea.

La adopción de una metodología explícita responde a la convicción de que la regulación de tecnologías complejas no puede sustentarse en aproximaciones intuitivas, fragmentarias o exclusivamente sectoriales, sino en un proceso sistemático de integración de insumos normativos, técnicos y científicos, que

¹⁸ Habermas, J. (1996). *Between facts and norms: Contributions to a discourse theory of law and democracy*. MIT Press.

¹⁹ Atienza, M. (2013). *Curso de argumentación jurídica*. Trotta.

permita traducir diagnósticos especializados en disposiciones jurídicas claras, operables y coherentes.

A. Insumos Legislativos

Como primer eje metodológico, en el proceso de elaboración de la presente Ley General se realizó un análisis exhaustivo de diversas iniciativas legislativas presentadas en materia de inteligencia artificial, tecnologías emergentes y neurotecnologías, en esta y anteriores legislaturas, que abordan la necesidad de establecer un marco normativo nacional que garantice el desarrollo ético, seguro y responsable de dichas tecnologías, así como la protección reforzada de los derechos humanos frente a sus impactos.

Entre los insumos legislativos examinados destacan aquellas propuestas que reconocen, de manera expresa, que la inteligencia artificial no constituye únicamente un fenómeno tecnológico, sino un factor con incidencia directa en la dignidad humana, la autonomía personal, la integridad cognitiva, la privacidad, la seguridad nacional y el funcionamiento de los sistemas democráticos. Estos planteamientos coinciden en señalar que la ausencia de reglas claras, criterios homogéneos y mecanismos de supervisión incrementa los riesgos asociados al uso indebido, opaco o discriminatorio de sistemas automatizados, particularmente cuando éstos inciden en decisiones con efectos jurídicos o materiales relevantes.

Asimismo, se identificaron iniciativas que subrayan la necesidad de avanzar hacia una regulación que fomente el desarrollo tecnológico y la innovación, sin desatender la obligación del Estado de establecer límites, salvaguardas y mecanismos de supervisión efectivos, especialmente en sectores estratégicos y en actividades que involucren datos personales, información sensible o decisiones automatizadas con efectos jurídicos relevantes. Estas propuestas enfatizan la importancia de equilibrar el impulso a la economía digital y a la productividad con la preservación de la soberanía tecnológica, la seguridad jurídica y la protección del interés público.

El examen comparado de dichas iniciativas permitió advertir coincidencias sustantivas en torno a la urgencia de contar con un marco jurídico nacional de carácter general que supere enfoques fragmentados o estrictamente sectoriales, incorpore principios comunes aplicables a todos los sistemas de inteligencia artificial y adopte un enfoque preventivo basado en la identificación, evaluación y gestión de riesgos. Al mismo tiempo, se detectaron vacíos normativos y dispersión conceptual que dificultan la aplicación uniforme de estándares de protección y la coordinación entre autoridades.

En atención a lo anterior, la presente Ley General retoma, sistematiza y articula las aportaciones más relevantes de los trabajos legislativos previos, integrándolos en un diseño normativo coherente, transversal y de alcance general, que permite armonizar la promoción de la innovación tecnológica con la tutela efectiva de los derechos humanos, la seguridad nacional y el desarrollo democrático del país. De esta forma, la Ley no parte de un vacío, sino de un proceso acumulativo de reflexión parlamentaria que se consolida en un instrumento jurídico integral y sistemático.

El análisis metodológico de estos insumos legislativos se realizó bajo criterios de sistematización normativa, identificando puntos de coincidencia —como la preocupación por la protección de derechos humanos, la innovación responsable y la supervisión estatal—, así como vacíos normativos relevantes detectados por una porción de estos insumos, entre ellos la ausencia de un enfoque basado en riesgos, la falta de definiciones técnicas uniformes, la inexistencia de mecanismos de gobernanza multiactor y multinivel y, en algunos casos, la omisión de aspectos emergentes como los neuroderechos, la perspectiva de género y la discriminación algorítmica.

Este ejercicio comparativo no tuvo como finalidad reproducir o fusionar iniciativas de manera mecánica, sino extraer aprendizajes legislativos, depurar enfoques y construir una propuesta normativa que superara las limitaciones detectadas, articulando los aportes existentes dentro de un marco general coherente y constitucionalmente habilitado, conforme a la técnica de ley general prevista en el artículo 73 constitucional.

B. Insumos Técnicos y Científicos

Como segundo eje metodológico, la construcción del dictamen se apoyó en un proceso participativo amplio, sustentado en insumos técnicos y científicos provenientes de la Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México, a través de la realización de conversatorios, mesas de trabajo y ejercicios de deliberación especializada durante los años 2024 y 2025.

Los conversatorios de la Comisión de IA constituyeron un espacio institucional de diálogo multisectorial, en el que participaron especialistas de la academia, representantes del sector privado, organizaciones de la sociedad civil, autoridades federales, organismos internacionales, cuerpos diplomáticos y expertos en derechos humanos, ética digital, ciberseguridad, economía digital y políticas públicas.²⁰ Las transcripciones de dichos ejercicios permitieron documentar diagnósticos precisos sobre el estado actual del ecosistema de inteligencia artificial en México, así como identificar riesgos, oportunidades y necesidades regulatorias concretas.²¹

También se integró como insumo central una Propuesta de Marco Normativo en materia de Inteligencia Artificial, concebida como una síntesis estructurada de las conclusiones derivadas de los conversatorios, así como un conjunto de características sustantivas para el diseño de una Ley General de IA y una ruta de trabajo para su discusión y eventual aprobación legislativa.²² Dicho marco permitió ordenar y traducir aportaciones técnicas complejas en criterios normativos claros, definiendo principios, mecanismos de gobernanza, esquemas

²⁰ Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México. (2025). *Informe de los conversatorios 2024–2025*. Senado de la República.

https://comisiones.senado.gob.mx/inteligencia_artificial/images/noticias/Informe_2024-2025.pdf

²¹ Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México. (2025). *Transcripciones de los conversatorios en materia de inteligencia artificial*. Senado de la República.

https://comisiones.senado.gob.mx/inteligencia_artificial/images/noticias/Transcripciones_2024-2025.pdf

²² Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México. (2025). *Propuesta de Marco Normativo*.

https://comisiones.senado.gob.mx/inteligencia_artificial/images/noticias/Propuesta.pdf

de evaluación de riesgos y pautas de coordinación institucional, en coherencia con estándares internacionales y con el contexto constitucional mexicano.

El proceso metodológico también incluyó el análisis del ecosistema digital nacional, considerando factores como la concentración de datos, el acceso a infraestructura tecnológica, la brecha digital, el desarrollo de capacidades nacionales y la dependencia de tecnologías extranjeras. Estos elementos resultaron fundamentales para incorporar en el articulado de esta Ley General consideraciones relativas a seguridad nacional, soberanía tecnológica y desarrollo económico sostenible, evitando una regulación desconectada de la realidad productiva y tecnológica del país.

De manera complementaria, se incorporaron referencias internacionales verificables, provenientes de organismos multilaterales y experiencias regulatorias comparadas, no con la finalidad de trasplantar modelos normativos; más bien, para identificar tendencias, buenas prácticas y estándares mínimos en materia de gobernanza, ética y regulación de la inteligencia artificial. En este sentido, los insumos internacionales fueron utilizados como herramientas de contraste y validación metodológica, reforzando la solidez técnica del dictamen.²³

En conjunto, estos insumos técnicos y científicos permitieron que la presente iniciativa se construyera como un producto legislativo informado, basado en evidencia empírica, deliberación plural y análisis especializado. La metodología adoptada garantiza que las disposiciones de la Ley General no respondan a intereses aislados ni a visiones unidimensionales. Por el contrario, reflejan una integración transversal de conocimientos, orientada a proteger derechos, fortalecer capacidades institucionales y promover un desarrollo responsable de la inteligencia artificial en México.

VI. Análisis de Impacto

²³ UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

El análisis de impacto constituye un elemento esencial de la presente Exposición de Motivos, en tanto permite valorar de manera razonada las consecuencias jurídicas, sociales, económicas y democráticas derivadas tanto de la ausencia de regulación como de la adopción de un marco normativo integral en materia de inteligencia artificial. Este análisis parte de un presupuesto metodológico claro: la inteligencia artificial ya incide en decisiones públicas y privadas de alto impacto y, por ello, su despliegue requiere evaluación diferenciada de riesgos y beneficios, así como criterios verificables de responsabilidad y rendición de cuentas.

A. Riesgos de la ausencia de regulación

La evidencia nacional e internacional muestra que la ausencia de regulación o la existencia de marcos normativos fragmentados en materia de inteligencia artificial generan riesgos significativos para los derechos humanos, la seguridad pública y la estabilidad democrática. A falta de un marco jurídico general, los sistemas de IA tienden a desplegarse bajo lógicas predominantemente comerciales o técnicas, sin mecanismos efectivos de rendición de cuentas, supervisión pública ni evaluación sistemática de impactos. Lo anterior reduce la capacidad del Estado para prevenir daños e incrementa la incertidumbre para las personas y para los actores que participan en el desarrollo y uso de estas tecnologías.

Entre los principales riesgos identificados se encuentran:

1. La adopción de sistemas opacos o no explicables en ámbitos de alto impacto, como justicia, seguridad, salud y servicios públicos;
2. la utilización masiva de datos personales y sensibles sin salvaguardas adecuadas;
3. la automatización de decisiones que afectan derechos sin supervisión humana significativa; y
4. la proliferación de prácticas discriminatorias derivadas de sesgos algorítmicos no detectados ni corregidos.

Los diagnósticos derivados de los conversatorios legislativos y de organismos internacionales coinciden en que los sistemas de IA, cuando no son regulados, tienden a reproducir y amplificar desigualdades sociales preexistentes, debido a la forma en que son diseñados, entrenados y desplegados, particularmente cuando se basan en conjuntos de datos históricos que reflejan sesgos.²⁴ En estos casos, la aparente “neutralidad” técnica puede ocultar decisiones de diseño, selección de datos o criterios de optimización que, en la práctica, consolidan exclusiones o tratos diferenciados injustificados.

Asimismo, la ausencia de un marco regulatorio incrementa los riesgos para la seguridad nacional y la ciberseguridad, al permitir la adopción indiscriminada de tecnologías críticas sin criterios comunes de evaluación de riesgos, resiliencia, interoperabilidad ni control institucional. Esta situación puede derivar en dependencias tecnológicas externas, brechas de seguridad y vulnerabilidades sistémicas con impactos potencialmente graves para el Estado y la sociedad, particularmente cuando los sistemas se incorporan a infraestructura crítica, servicios públicos o procesos que requieren altos estándares de integridad y continuidad operativa.²⁵

B. Beneficios de una regulación transversal y basada en riesgos

Frente a este escenario, la adopción de una Ley General, horizontal y basada en riesgos genera beneficios claros y medibles. En primer lugar, proporciona certeza jurídica a los distintos actores del ecosistema de inteligencia artificial, al establecer principios comunes, definiciones técnicas uniformes y obligaciones diferenciadas conforme al nivel de riesgo de los sistemas.

En segundo término, fortalece la protección de los derechos humanos, al incorporar de manera transversal principios como la dignidad humana, la no discriminación, la transparencia algorítmica, la explicabilidad y la supervisión

²⁴ Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

²⁵ OCDE. (2020). *State of implementation of the OECD AI Principles*. <https://www.oecd.org/going-digital/ai/state-of-implementation-of-the-oecd-ai-principles.pdf>

humana significativa, alineando el desarrollo tecnológico con el mandato constitucional y los compromisos internacionales del Estado mexicano.

Adicionalmente, una regulación adecuada favorece la innovación responsable, al evitar enfoques prohibitivos o reactivos, y al establecer mecanismos como evaluaciones de impacto, *sandboxes regulatorios* y esquemas de gobernanza que permiten el desarrollo tecnológico bajo condiciones de seguridad, ética y confianza pública. La experiencia comparada demuestra que los marcos regulatorios claros y proporcionales no inhiben la innovación, sino que la orientan y legitiman socialmente, reduciendo incertidumbre y riesgos reputacionales, y favoreciendo una adopción más amplia y sostenible.²⁶

Desde una perspectiva económica, la Ley General busca impulsar al sector privado como motor de innovación y generación de empleo, fortaleciendo la competitividad y la soberanía tecnológica del país. Al establecer reglas claras y previsibles, la Ley fomenta el desarrollo de capacidades nacionales, reduce asimetrías regulatorias y crea condiciones para que empresas mexicanas — incluidas *startups* y pequeñas y medianas empresas— puedan escalar, atraer inversión y competir en mercados globales. De este modo, se promueve un ecosistema digital más dinámico, interoperable y resiliente, orientado al crecimiento económico, la creación de nuevos empleos y el aprovechamiento productivo de la inteligencia artificial en beneficio del desarrollo nacional, con especial atención a su impacto en el mercado laboral y en la reconversión de habilidades.

C. Impacto diferenciado en grupos en situación de vulnerabilidad

Un elemento central del análisis de impacto es el reconocimiento de que los efectos de la inteligencia artificial no son neutros ni homogéneos, y que se distribuyen de manera diferenciada entre la población. Estudios han documentado que mujeres, personas con discapacidad, comunidades indígenas, niñas, niños y adolescentes, personas adultas mayores y otros grupos

²⁶ Comisión Europea. (2024). *Ley de IA de la Unión Europea (EU AI Act)*.
<https://artificialintelligenceact.eu/the-act/>

históricamente discriminados enfrentan mayores riesgos frente al uso no regulado de sistemas automatizados.²⁷ Esta evidencia obliga a considerar, desde el diseño normativo, medidas específicas de prevención, evaluación y corrección.

La evidencia técnica demuestra que los sesgos algorítmicos pueden manifestarse en ámbitos como el acceso a servicios públicos, el empleo, el crédito, la vigilancia, la moderación de contenidos y la participación en espacios digitales, generando exclusión, estigmatización o violencia digital. En particular, el uso de tecnologías como los sistemas de reconocimiento facial, los modelos generativos y los sistemas de perfilamiento automatizado han mostrado impactos desproporcionados en mujeres y minorías, incluyendo la proliferación de *deepfakes*, la generación y difusión de contenidos sexuales falsos, no consentidos o ilícitos, el acoso digital y diversas prácticas discriminatorias (UNESCO, 2021; AI Now Institute, 2019).²⁸

En este contexto, el análisis de impacto justifica de manera expresa la incorporación de un Título específico en materia de perspectiva de género, inclusión y no discriminación, como una respuesta normativa proporcional a los riesgos identificados. Dicho Título reconoce que la igualdad sustantiva y la no discriminación deben ser criterios rectores en el diseño, entrenamiento, implementación y supervisión de los sistemas de inteligencia artificial, incorporando obligaciones de prevención y mecanismos de detección de sesgos a lo largo del ciclo de vida del sistema.

Adicionalmente, el análisis de impacto revela que la inteligencia artificial no constituye una tecnología neutral, sino un artefacto socio-técnico cuya operación se encuentra profundamente condicionada por decisiones humanas, estructuras institucionales y contextos históricos. Los sistemas de IA tienden a reflejar, reproducir e incluso amplificar patrones de desigualdad preexistentes cuando se

²⁷ Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. Proceedings of Machine Learning Research, 81, 1–15. <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

²⁸ UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. <https://unesdoc.unesco.org/ark:/48223/pf0000380455>; AI Now Institute. (2019). *Discriminating systems: Gender, race, and power in AI*. <https://ainowinstitute.org>

diseñan, entrenan o despliegan sin salvaguardas normativas adecuadas. La literatura especializada ha demostrado que la automatización de procesos decisionales, lejos de eliminar la subjetividad, puede cristalizar sesgos estructurales bajo una apariencia de objetividad técnica, generando impactos negativos acumulativos y de difícil corrección en grupos históricamente discriminados.²⁹

Desde esta perspectiva, la evaluación de impacto no solo cumple una función preventiva, sino también correctiva y orientadora, al permitir identificar sectores, poblaciones y contextos particularmente expuestos a los efectos adversos de la inteligencia artificial. Ello resulta especialmente relevante en ámbitos como el acceso a servicios públicos, el empleo, la seguridad, la justicia, la participación política y el entorno digital, donde la adopción acrítica de sistemas automatizados puede erosionar garantías fundamentales y profundizar brechas de género, socioeconómicas y territoriales, contraviniendo el mandato constitucional de igualdad sustantiva y no discriminación (UNESCO, 2021).

D. Justificación del Título Séptimo

La creación del Título Séptimo, *De la Perspectiva de Género, Inclusión y No Discriminación en la Inteligencia Artificial*, responde, por tanto, a un enfoque preventivo y estructural, sustentado en evidencia empírica y diagnósticos técnicos. Este Título permite abordar de manera específica los riesgos de reproducción de desigualdades, violencia digital y exclusión algorítmica, estableciendo obligaciones diferenciadas, mecanismos de evaluación y acciones afirmativas orientadas a garantizar que el desarrollo de la inteligencia artificial contribuya a la reducción y no a la profundización de brechas sociales.

De esta forma, el análisis de impacto confirma que la Ley General no solo es jurídicamente necesaria, sino socialmente responsable, al incorporar un enfoque de derechos humanos, perspectiva de género e inclusión como elementos indispensables para una gobernanza democrática de la inteligencia artificial en

²⁹ Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

México. En consecuencia, el análisis de impacto confirma que la regulación de la inteligencia artificial no puede limitarse a criterios de eficiencia tecnológica o innovación económica, sino que debe asumir una función garantista, preventiva y estructural, orientada a corregir asimetrías, proteger derechos y asegurar que el desarrollo tecnológico contribuya al bienestar social. Bajo esta lógica, la incorporación de un enfoque diferenciado para grupos en situación de vulnerabilidad y la creación de un Título específico en materia de perspectiva de género, inclusión y no discriminación constituyen una exigencia normativa derivada de la evidencia empírica y del mandato constitucional de igualdad sustantiva.

VII. Consideraciones sobre el Contenido de la Ley

El contenido de la Ley General para Regular y Fomentar el Uso de la Inteligencia Artificial en México se estructura de manera sistemática y progresiva, a fin de ofrecer un marco normativo coherente, integral y funcional que responda a la complejidad técnica, jurídica y social de la inteligencia artificial. Cada Título cumple una función específica dentro de la arquitectura normativa, permitiendo que los principios, mecanismos de gobernanza, instrumentos de política pública y obligaciones regulatorias se articulen de forma armónica.

Título Primero. Disposiciones Generales

El Título Primero cumple una función estructural esencial al establecer las bases conceptuales, normativas y de interpretación de la Ley General para Regular y Fomentar el Uso de la Inteligencia Artificial en México. En él se define el objeto de la Ley, su naturaleza de orden público e interés social, así como su carácter general y horizontal, lo que permite su aplicación transversal a múltiples sectores sin sustituir la regulación sectorial existente o futura, sino sirviendo como marco de referencia común.

Otro elemento central de este Título es la incorporación de un glosario técnico que cumple una función de seguridad jurídica, coherencia normativa y operatividad regulatoria. La precisión conceptual resulta indispensable en un

campo caracterizado por la rápida evolución tecnológica y por la utilización de términos técnicos con significados variables. Al fijar definiciones claras —como inteligencia artificial, sistemas de alto riesgo, evaluación de impacto algorítmico, sesgo algorítmico o neuroderechos—, la Ley reduce ambigüedades interpretativas, facilita la aplicación del enfoque basado en riesgos y asegura una lectura uniforme del articulado por autoridades, operadores jurídicos, desarrolladores, proveedores y usuarios.

Asimismo, el Título Primero integra de manera explícita el marco constitucional e internacional, asegurando que la interpretación y aplicación de la Ley se realicen en armonía con la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales en materia de derechos humanos y los estándares internacionales relevantes. De este modo, el Título Primero no solo introduce el contenido de la Ley, sino que define su orientación axiológica y metodológica, asegurando que todo el sistema normativo se construya sobre principios de legalidad, derechos humanos, seguridad jurídica y soberanía tecnológica.

Título Segundo. Principios Éticos, Derechos Humanos y Neuroderechos

El Título Segundo establece el núcleo axiológico de la Ley, al reconocer de manera expresa que la regulación de la inteligencia artificial debe estar anclada, de forma prioritaria, en la protección de los derechos humanos y en la observancia de principios éticos exigibles. Este Título parte de una premisa fundamental: la inteligencia artificial no es un instrumento neutral, sino una tecnología capaz de influir de manera directa en decisiones, oportunidades y trayectorias vitales de las personas, por lo que su desarrollo y uso deben someterse a límites normativos claros, según su nivel de riesgo.

En este sentido, el Título Segundo consagra un catálogo amplio de principios rectores de la regulación de la inteligencia artificial, entre los que destacan la dignidad humana, la legalidad, la transparencia, la rendición de cuentas, la no discriminación, la supervisión humana significativa, la protección reforzada de

grupos en situación de vulnerabilidad, la regulación basada en riesgos y la tutela de los derechos laborales, culturales, creativos y de propiedad industrial e intelectual, incluidos los relativos a la voz, la imagen, la identidad, la obra y la autoría. Estos principios no constituyen meras declaraciones programáticas: son criterios jurídicos vinculantes que orientan la interpretación del resto del articulado y la actuación de los distintos sujetos regulados.

Una innovación sustantiva de este Título es el reconocimiento explícito de los neuroderechos, que amplía el horizonte tradicional de protección jurídica frente a tecnologías capaces de incidir en procesos cognitivos, emocionales o neuronales. Al incorporar derechos como la privacidad mental, la integridad cognitiva, la autonomía de la voluntad y la protección frente a interferencias no consentidas, la Ley adopta un enfoque preventivo y prospectivo, anticipándose a riesgos emergentes derivados de la convergencia entre inteligencia artificial y neurotecnologías. De este modo, el Título Segundo consolida una regulación centrada en la persona, alineada con los desarrollos más avanzados del derecho internacional de los derechos humanos y de la ética tecnológica contemporánea.

Título Tercero. Gobernanza y Coordinación Multinivel en Inteligencia Artificial

El Título Tercero desarrolla un modelo de gobernanza institucional diseñado para responder a la complejidad, transversalidad y dinamismo de la inteligencia artificial. La experiencia comparada y los diagnósticos técnicos coinciden en que uno de los principales riesgos regulatorios en esta materia es la fragmentación normativa y la dispersión de competencias entre autoridades. Frente a ello, este Título establece un esquema de gobernanza multinivel, que articula de manera coordinada a la Federación, las entidades federativas y los municipios, respetando el diseño constitucional del federalismo mexicano.

La Federación asume la conducción de la política nacional en materia de inteligencia artificial, la definición de lineamientos generales y la supervisión de sistemas de alto riesgo, mientras que las entidades federativas y los municipios participan activamente en la implementación, adaptación y aplicación de la

regulación conforme a sus contextos territoriales y capacidades institucionales. Este diseño evita tanto la centralización excesiva como la dispersión normativa, permitiendo una aplicación homogénea de la Ley sin desconocer las realidades locales.

Adicionalmente, el Título Tercero incorpora mecanismos de coordinación interinstitucional y participación social mediante la creación de instancias como el Sistema Nacional de Inteligencia Artificial y un Consejo Consultivo Nacional de carácter multisectorial. Estas figuras permiten integrar a la academia, el sector privado, la sociedad civil, a los tres niveles de gobierno y a los organismos autónomos pertinentes en la discusión, evaluación y seguimiento de las políticas públicas en la materia. De este modo, la gobernanza de la inteligencia artificial se concibe como un proceso colaborativo, transparente y sujeto a rendición de cuentas, reforzando la legitimidad democrática de la regulación.

Título Cuarto. Estrategia Nacional y Política Pública en Inteligencia Artificial

El Título Cuarto introduce la Estrategia Nacional de Inteligencia Artificial como el instrumento rector de la política pública en la materia, reconociendo que la regulación normativa resulta insuficiente si no se acompaña de planificación estratégica, coordinación institucional y evaluación permanente. La Estrategia Nacional se concibe como una política de Estado, orientada a establecer una visión de largo plazo para el desarrollo, fomento y uso de la inteligencia artificial en México, más allá de coyunturas políticas o sexenales.

Este Título también articula la regulación con la planeación pública, al establecer objetivos, ejes estratégicos, líneas de acción e indicadores de impacto que permiten evaluar de manera sistemática los efectos sociales, económicos, ambientales y en derechos humanos de la adopción de la inteligencia artificial. Asimismo, prevé la vinculación de la Estrategia Nacional con los programas sectoriales, las políticas de transformación digital, los esquemas de datos abiertos y las estrategias de inclusión digital, evitando duplicidades y contradicciones entre instrumentos de planeación.

La incorporación de la Estrategia Nacional responde, además, a la necesidad de fortalecer la soberanía tecnológica, reducir brechas digitales, impulsar el desarrollo de capacidades nacionales y orientar la innovación hacia objetivos de interés público. De este modo, el Título Cuarto consolida una visión integral de la inteligencia artificial como herramienta de desarrollo sostenible, innovación responsable y fortalecimiento institucional, asegurando que el avance tecnológico se encuentre alineado con los valores constitucionales y con la protección efectiva de los derechos fundamentales.

Título Quinto. De las Instituciones Rectoras en Materia de Inteligencia Artificial

El Título Quinto establece la arquitectura institucional necesaria para garantizar una conducción eficaz, coherente y especializada de la política pública en materia de inteligencia artificial. Su inclusión responde a la evidencia recogida durante el proceso legislativo y técnico emprendido por la Comisión de Inteligencia Artificial del Senado, de que la regulación de la IA no puede operar de manera desarticulada ni depender de una sola lógica administrativa, sino que requiere una clara delimitación de competencias entre la función estratégica de fomento científico-tecnológico y la función operativa de transformación digital del Estado.

En este sentido, el Título Quinto subraya la necesidad de una Autoridad Nacional en Inteligencia Artificial (nombre genérico para efectos de esta iniciativa) y distingue de manera expresa las atribuciones de la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI), como instancia responsable de la política nacional de investigación, desarrollo e innovación en inteligencia artificial, de aquellas conferidas a la Agencia de Transformación Digital y Telecomunicaciones (ATDT), como autoridad técnica y operativa encargada de la adopción, implementación y supervisión de sistemas de IA en el sector público. Esta diferenciación responde a estándares internacionales de buena gobernanza tecnológica, que recomiendan separar las funciones de promoción científica de las funciones de despliegue operativo y control técnico, a fin de evitar conflictos de interés, duplicidades institucionales y vacíos regulatorios.

El Título Quinto incorpora un modelo de coordinación interinstitucional obligatoria, reconociendo que la inteligencia artificial es un fenómeno transversal que impacta simultáneamente la política científica, la innovación productiva, la gestión administrativa, la seguridad de la información y los derechos humanos. Por ello, se prevé un esquema de cooperación permanente entre la SECIHTI y la ATDT, bajo principios de coherencia normativa, interoperabilidad técnica y protección reforzada de derechos fundamentales, asegurando que la transformación digital del Estado mexicano se encuentre alineada con la política científica nacional y con los objetivos de la Estrategia Nacional de Inteligencia Artificial. Consecuentemente, se propone que la coordinación prevista en este Capítulo se realice en el marco del Sistema Nacional de Inteligencia Artificial, bajo la conducción de la Autoridad Nacional en Inteligencia Artificial.

Esta construcción institucional atiende directamente a los diagnósticos derivados de los conversatorios legislativos y de los insumos técnicos analizados, en los que se advirtió que uno de los principales riesgos para una regulación eficaz de la IA es la fragmentación de responsabilidades, así como la ausencia de autoridades claramente identificables para la rendición de cuentas. Por ende, el Título Quinto dota al marco normativo de certeza institucional, fortaleciendo la capacidad del Estado para conducir el desarrollo tecnológico con enfoque de derechos, seguridad y soberanía digital.

Título Sexto. Educación, Capacitación y Cultura Digital en Inteligencia Artificial

El Título Sexto reconoce que la regulación de la inteligencia artificial no puede limitarse al control normativo de sistemas y tecnologías, sino que debe incorporar una dimensión formativa y cultural, orientada a fortalecer las capacidades de la sociedad, del sector público y del sector productivo para interactuar de manera crítica, informada, innovadora y responsable con sistemas algorítmicos.

Desde esta perspectiva, el Título Sexto parte del principio de que la alfabetización y la ciudadanía digitales constituyen condiciones indispensables para el ejercicio efectivo de derechos humanos en entornos mediados por

inteligencia artificial. La incorporación de contenidos relativos a IA en los sistemas educativos y en los programas de capacitación responde a la evidencia empírica que demuestra que la falta de comprensión sobre el funcionamiento, riesgos y límites de los sistemas algorítmicos incrementa la vulnerabilidad de las personas frente a fenómenos como la desinformación, la discriminación algorítmica, la opacidad decisional y el uso indebido de datos personales.

En este marco, el Título Sexto establece obligaciones específicas para las autoridades educativas federales y locales, a fin de integrar de manera transversal contenidos sobre inteligencia artificial, ética digital, derechos humanos, neuroderechos y ciberseguridad en los planes y programas de estudio de los distintos niveles educativos. Esta previsión normativa responde a un enfoque de prevención estructural, orientado a cerrar brechas digitales, reducir asimetrías de conocimiento y garantizar que el desarrollo tecnológico no profundice desigualdades existentes.

El Título Sexto también reconoce la necesidad de formación especializada de talento científico, técnico y profesional, así como de capacitación permanente para servidoras y servidores públicos responsables del uso de sistemas de inteligencia artificial. Esta dimensión resulta especialmente relevante en el sector público, donde el uso de sistemas algorítmicos puede tener impactos directos en derechos, servicios esenciales y procedimientos administrativos. Por ello, el articulado prevé estándares mínimos de capacitación, certificaciones y esquemas de evaluación de competencias, en concordancia con recomendaciones internacionales sobre uso responsable de IA en el Estado.

Finalmente, el Título Sexto incorpora una visión incluyente al prever programas específicos dirigidos a grupos en situación de vulnerabilidad, reconociendo que la brecha digital no es únicamente tecnológica; también es social, educativa y territorial. De este modo, la Ley articula una política de educación y capacitación en inteligencia artificial que no solo acompaña el desarrollo normativo, sino que lo sostiene y legitima socialmente, al fortalecer las capacidades colectivas necesarias para una adopción democrática, ética y responsable de la inteligencia artificial en México.

Título Séptimo. De la Perspectiva de Género, Inclusión y No Discriminación en la Inteligencia Artificial

El Título Séptimo se incorpora como una respuesta normativa expresa a uno de los desafíos más complejos y documentados de la inteligencia artificial contemporánea: su capacidad para reproducir, intensificar y automatizar desigualdades estructurales preexistentes cuando no se regula bajo criterios explícitos de igualdad sustantiva, inclusión y no discriminación. A diferencia de otros ámbitos regulatorios, en el entorno algorítmico los sesgos no siempre son visibles ni intencionales, sino que se originan en datos históricos, patrones sociales discriminatorios o decisiones de diseño aparentemente neutras, lo que exige una intervención jurídica específica.

La creación de un Título específico en este sentido obedece a la constatación de que la transversalización genérica de la perspectiva de género resulta insuficiente frente a fenómenos como la violencia digital facilitada por IA, la producción de *deepfakes* con contenido sexual, la generación y difusión de material sexual no consentido —incluida la pornografía infantil, donde el consentimiento es nulo e irrelevante—, la exclusión automatizada en procesos de selección laboral o crediticia, y la invisibilización sistemática de mujeres, personas con discapacidad, pueblos indígenas y diversidades sexuales en los sistemas de datos. Este Título transforma los mandatos constitucionales de igualdad y no discriminación en obligaciones tecnológicas concretas, imponiendo deberes de prevención, evaluación y corrección de sesgos algorítmicos, así como de identificación y mitigación de usos dolosos, a lo largo de todo el ciclo de vida de los sistemas de inteligencia artificial.

Por último, el Título Séptimo reconoce que la inclusión no se limita a evitar daños, sino que implica garantizar la participación de mujeres y grupos históricamente excluidos en el diseño, desarrollo, uso, fomento y toma de decisiones sobre tecnologías emergentes. Con ello, la Ley no solo busca mitigar impactos negativos, sino reconfigurar el ecosistema de la inteligencia artificial desde una lógica de justicia social, asegurando que el avance tecnológico contribuya a reducir y no a profundizar las brechas estructurales existentes.

Título Octavo. Fomento al Desarrollo, Innovación y Capacidades Nacionales en Inteligencia Artificial

El Título Octavo introduce una dimensión estratégica esencial para el equilibrio del marco normativo: el reconocimiento de que la regulación de la inteligencia artificial debe ir acompañada de una política activa de fomento al desarrollo científico, tecnológico y productivo, particularmente en contextos nacionales marcados por asimetrías tecnológicas y dependencia de soluciones extranjeras. Este Título parte de la premisa de que una regulación exclusivamente restrictiva puede inhibir la innovación, debilitar el ecosistema nacional y limitar la capacidad del Estado para incidir de manera soberana en el desarrollo tecnológico.

En este sentido, el Título Octavo establece bases normativas para promover la investigación científica, la formación de talento especializado, la innovación responsable y la colaboración entre sectores público, privado, académico y social. El fomento a capacidades nacionales se concibe como un componente indispensable de la soberanía tecnológica, entendida no solo como control de infraestructuras, sino como la capacidad efectiva del país para desarrollar, adaptar, gobernar y aprovechar tecnologías estratégicas conforme a sus propios valores constitucionales y prioridades de desarrollo.

Este Título articula la regulación con el desarrollo económico sostenible, reconociendo que la inteligencia artificial puede convertirse en un motor de crecimiento, productividad e inclusión si se orienta adecuadamente. De este modo, la Ley evita una dicotomía falsa entre regulación e innovación, y propone un modelo en el que ambas se refuerzan mutuamente: la regulación aporta certeza jurídica y legitimidad social, mientras que el fomento tecnológico fortalece la viabilidad y pertinencia del marco normativo.

Título Noveno. Evaluación, Clasificación y Gestión de Riesgos en Sistemas de Inteligencia Artificial

El Título Noveno desarrolla el enfoque regulatorio basado en riesgos, que constituye uno de los pilares conceptuales y técnicos de la Ley. Este enfoque parte del reconocimiento de que no todos los sistemas de inteligencia artificial

presentan el mismo nivel de impacto ni requieren el mismo grado de intervención estatal, por lo que una regulación eficaz debe ser diferenciada, proporcional y contextualizada.

La evaluación y clasificación de riesgos permite identificar de manera anticipada aquellos sistemas cuya finalidad, contexto de uso o alcance pueden afectar de forma significativa derechos humanos, seguridad pública, procesos democráticos, salud o medio ambiente, entre otros temas. En estos casos, la Ley prevé obligaciones reforzadas de evaluación de impacto, supervisión y mitigación, mientras que para sistemas de menor riesgo se establecen principios generales de seguridad y transparencia. Esta lógica evita tanto la sobrerregulación como la desprotección normativa, dotando al marco jurídico de flexibilidad y racionalidad técnica.

Además, la gestión de riesgos se concibe como un proceso dinámico y continuo, no como una evaluación aislada previa al despliegue tecnológico. Con ello, la Ley reconoce que los riesgos asociados a la inteligencia artificial pueden evolucionar con el tiempo, en función de nuevos datos, cambios de contexto o usos no previstos, lo que exige mecanismos permanentes de seguimiento y actualización.

Título Décimo. De las Aplicaciones Prohibidas y de Alto Riesgo de la Inteligencia Artificial

Este Título responde a la naturaleza cambiante y evolutiva de la inteligencia artificial mediante el establecimiento de un régimen jurídico diferenciado para aplicaciones prohibidas y sistemas de alto riesgo, así como de mecanismos de control, mitigación y gestión de riesgos.

La Ley parte de la premisa de que la regulación de tecnologías emergentes no puede agotarse en reglas uniformes o estáticas, sino que debe identificar y clasificar aquellas aplicaciones que, por su finalidad, contexto de uso o impacto, resultan incompatibles con los derechos humanos, así como aquellas que requieren obligaciones reforzadas de supervisión, evaluación y control. A través

de este enfoque, el Estado establece capacidades institucionales de detección temprana de riesgos, corrección de fallas sistémicas y adaptación regulatoria progresiva, garantizando la protección efectiva de los derechos, la seguridad pública y la estabilidad democrática.

Este Título consolida una visión de regulación viva basada en riesgos, en la que el Estado asume un papel activo no solo como regulador, sino también como impulsor y facilitador del desarrollo responsable de la inteligencia artificial, actuando como gestor permanente de su impacto social, económico y democrático. Este enfoque permite acompañar la innovación y el crecimiento del ecosistema productivo, al tiempo que establece salvaguardas claras frente a usos de alto impacto o potencialmente lesivos.

Título Décimo Primero. Derechos y Obligaciones de Desarrolladores, Operadores, Proveedores y Usuarios

El Título Décimo Primero articula un régimen equilibrado de derechos y obligaciones que reconoce la pluralidad de actores que intervienen a lo largo del ciclo de vida de los sistemas de inteligencia artificial. Este Título parte del principio de que la protección efectiva de los derechos de las personas usuarias exige una asignación clara y proporcional de responsabilidades entre quienes diseñan, entrenan, proveen, implementan y operan sistemas algorítmicos.

En este marco, se reconocen derechos como el acceso a información comprensible, la explicación de decisiones automatizadas, la posibilidad de impugnación y la garantía de supervisión humana significativa, particularmente en contextos de alto impacto. De manera paralela, se establecen obligaciones de diligencia técnica, transparencia, trazabilidad y responsabilidad algorítmica para desarrolladores, proveedores y operadores, conforme a su grado de control e intervención, consolidando así un modelo de rendición de cuentas distribuida acorde con la complejidad tecnológica de la inteligencia artificial.

Título Décimo Segundo. Transparencia, Rendición de Cuentas y Datos Abiertos

El Título Décimo Segundo profundiza en la transparencia algorítmica como un requisito esencial para la legitimidad democrática del uso de la inteligencia artificial, especialmente cuando se emplea en funciones públicas o en servicios de interés general. La opacidad algorítmica se reconoce como un riesgo estructural que puede erosionar la confianza social y dificultar la protección efectiva de derechos.

Este Título incorpora mecanismos como registros de sistemas de IA, obligaciones de información y esquemas de acceso razonable a datos, equilibrando la transparencia con la protección de secretos industriales y derechos de propiedad intelectual. De este modo, la Ley fortalece el control público y la rendición de cuentas sin desalentar la innovación responsable.

Título Décimo Tercero. Procedimientos Administrativos en Materia de Inteligencia Artificial

El Título Décimo Tercero traduce los principios sustantivos de la Ley en procedimientos administrativos claros y técnicamente informados, garantizando su aplicación efectiva. Asimismo, establece reglas para auditorías, certificaciones, evaluaciones de impacto y atención de quejas, privilegiando un enfoque preventivo y correctivo orientado a la mejora continua, con pleno respeto a la propiedad intelectual e industrial, los secretos comerciales y los activos intangibles de las empresas.

La previsión de procedimientos específicos dota de seguridad jurídica tanto a las autoridades como a los particulares, reduce la incertidumbre regulatoria, evita arbitrariedades y fortalece la confianza en la actuación estatal, creando condiciones propicias para la innovación, la inversión y el desarrollo responsable de soluciones de inteligencia artificial en México.

Título Décimo Cuarto. Infracciones, Responsabilidades y Sanciones

El Título Décimo Cuarto completa la arquitectura normativa mediante un régimen sancionador proporcional y gradual, orientado a garantizar el cumplimiento de la Ley y la protección efectiva de derechos. Este Título parte del reconocimiento de

que la regulación de la inteligencia artificial debe distinguir entre errores técnicos, fallas de diligencia y conductas dolosas, evitando desincentivos innecesarios para la innovación y el desarrollo empresarial, pero estableciendo consecuencias jurídicas claras frente a prácticas que generen daños graves, discriminación o afectaciones a la seguridad nacional.

En este sentido, el régimen sancionador se concibe como un último recurso, complementado por medidas de corrección, reparación integral y garantías de no repetición, privilegiando la subsanación temprana y el cumplimiento voluntario. Con ello, se busca asegurar que la innovación responsable y la inversión tecnológica encuentren un entorno de certeza jurídica, sin que el incumplimiento grave o reiterado quede impune.

VIII. Consideraciones Finales

La inteligencia artificial representa una de las transformaciones tecnológicas más profundas de la época contemporánea, no sólo por su capacidad de automatizar tareas o procesar grandes volúmenes de información, sino por su impacto estructural en la forma en que se toman decisiones, se organizan los procesos productivos, se configuran los mercados y se ejercen los derechos. Su despliegue progresivo en la vida pública y privada plantea desafíos inéditos para el derecho, las instituciones y la democracia, que no pueden ser atendidos mediante aproximaciones fragmentarias, sectoriales o meramente reactivas.

A lo largo de la presente Ley General se parte del reconocimiento de que la inteligencia artificial ha dejado de ser un fenómeno marginal para convertirse en una infraestructura productiva y decisional, integrada de manera creciente en ámbitos estratégicos como la administración pública, la economía digital, el mercado laboral, la provisión de servicios, la seguridad, la educación y la salud. Esta condición estructural exige una respuesta legislativa a la altura de su impacto, capaz de ofrecer certezas jurídicas, proteger derechos y orientar el desarrollo tecnológico conforme al interés público.

Las Consideraciones Finales de esta Ley constituyen una reafirmación del propósito central que guio su diseño normativo: asegurar que el desarrollo,

implementación y uso de la inteligencia artificial en México se realicen de manera responsable, transparente y compatible con los valores constitucionales. En este sentido, la regulación no se concibe como un obstáculo a la innovación, sino como una condición necesaria para que ésta sea socialmente aceptable, económicamente sostenible y jurídicamente legítima.

Desde una perspectiva estratégica, la Ley coloca a México en una posición de vanguardia internacional, al adoptar un enfoque horizontal, basado en riesgos, preventivo y centrado en derechos humanos, alineado con las tendencias regulatorias más avanzadas. A diferencia de modelos sectoriales o fragmentados, el marco propuesto ofrece una arquitectura normativa coherente que permite anticipar riesgos, orientar la innovación y fortalecer la capacidad institucional del Estado frente a tecnologías de alto impacto.

Asimismo, la Ley es plenamente compatible con los compromisos internacionales asumidos por el Estado mexicano, en particular con el Tratado entre México, Estados Unidos y Canadá (T-MEC), los principios y recomendaciones de la OCDE y la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO. Esta compatibilidad no se limita a una armonización formal; también se traduce en la adopción sustantiva de estándares relativos a transparencia, rendición de cuentas, gobernanza, protección de derechos fundamentales y promoción de una innovación responsable.

Un elemento distintivo del marco normativo propuesto es su contribución directa a la preservación y fortalecimiento de la soberanía digital y tecnológica. Al establecer bases claras para el desarrollo de capacidades nacionales, la protección de datos estratégicos, la evaluación de riesgos en infraestructuras críticas y la coordinación interinstitucional, la Ley reduce dependencias tecnológicas externas y fortalece la autonomía del Estado mexicano en la toma de decisiones vinculadas al desarrollo, uso y fomento de la inteligencia artificial.

En términos de impacto esperado, la Ley genera beneficios concluyentes, entre los que destacan: el incremento de la certeza jurídica para desarrolladores,

operadores, proveedores y usuarios; la reducción de riesgos asociados a decisiones automatizadas opacas o discriminatorias; el fortalecimiento de la confianza social en el uso de tecnologías emergentes; y la mejora en la calidad, eficiencia y equidad de los servicios públicos apoyados en sistemas de inteligencia artificial.

Desde una perspectiva económica, el marco normativo fomenta un entorno propicio para la innovación y la competitividad al establecer reglas claras, previsibles y proporcionales que incentivan el desarrollo tecnológico responsable, la inversión y la colaboración entre sectores. Asimismo, brinda certeza y protección a la propiedad intelectual e industrial, a los secretos comerciales y a los activos intangibles, reconociéndolos como motores clave de la innovación y de la creación de valor. La regulación propuesta no inhibe la innovación, sino que la legitima y la orienta hacia objetivos de interés público, desarrollo sostenible y bienestar social, fortaleciendo al mismo tiempo la capacidad de las empresas mexicanas para competir y escalar en mercados globales.

Estas Consideraciones Finales permiten afirmar que la Ley General constituye una respuesta normativa equilibrada, que conjuga protección de derechos, seguridad nacional, desarrollo económico e inclusión social. Su diseño integral asegura que la inteligencia artificial se convierta en un instrumento al servicio de la sociedad, y no en un factor de exclusión, concentración de poder o erosión democrática.

Por todo lo expuesto en la presente Exposición de Motivos, se concluye que la creación de la Ley General para Regular y Fomentar el Uso de la Inteligencia Artificial en México resulta jurídicamente viable, técnicamente necesario y socialmente pertinente.

En virtud de lo anterior, la aprobación de esta Ley General se justifica plenamente en atención a seis objetivos fundamentales:

1. Garantizar el respeto y la protección de los derechos humanos y los neuroderechos, incluida la salvaguarda de la dignidad humana frente a los procesos de automatización y reconfiguración del trabajo;
2. Fortalecer la seguridad nacional y la soberanía tecnológica;
3. Impulsar la innovación responsable y el desarrollo económico sostenible;
4. Prevenir sesgos, violencia digital y discriminación algorítmica;
5. Crear mecanismos de gobernanza plural, transparente y con rendición de cuentas;
6. Insertar a México en la vanguardia normativa internacional en materia de inteligencia artificial.

Con ello, el legislador cumple su deber constitucional de anticipar riesgos, proteger derechos y orientar el progreso tecnológico conforme al interés público, consolidando un marco jurídico que asegura que la inteligencia artificial se desarrolle y utilice al servicio de la sociedad, la democracia y el Estado constitucional de derecho.

Por lo expuesto, fundado y motivado con anterioridad, es que se somete a consideración del H. Pleno la siguiente iniciativa con:

PROYECTO DE DECRETO

ÚNICO. Se expide la **LEY GENERAL PARA REGULAR Y FOMENTAR EL USO DE LA INTELIGENCIA ARTIFICIAL (IA) EN MÉXICO** para quedar como sigue:

LEY GENERAL PARA REGULAR Y FOMENTAR EL USO DE LA INTELIGENCIA ARTIFICIAL (IA) EN MÉXICO

Título Primero. Disposiciones Generales

Capítulo I. Objeto, naturaleza y finalidad de la Ley

Capítulo II. Definiciones y terminología

Capítulo III. Ámbito de aplicación

Título Segundo. Principios Éticos, Derechos Humanos y Neuroderechos

Capítulo I. Principios rectores de la IA

Capítulo II. Derechos humanos aplicables a la IA

Capítulo III. Reconocimiento y protección de los neuroderechos

Capítulo IV. Privacidad, protección de datos y ciberseguridad

Título Tercero. Gobernanza y Coordinación Multinivel en IA

Capítulo I. De las Competencias de la Federación

Capítulo II. De las Competencias de las entidades federativas

Capítulo III. De las Competencias de los municipios

Capítulo IV. De la Coordinación Nacional e Interinstitucional

Capítulo V. De la Gobernanza Sectorial y Participación Social

Título Cuarto. Estrategia Nacional y Política Pública en IA

Capítulo I. Estrategia Nacional de Inteligencia Artificial

Capítulo II. Programas sectoriales y evaluación de impacto

Capítulo III. Vinculación con políticas de transformación digital y datos abiertos

Título Quinto. De las Instituciones Rectoras en materia de Inteligencia Artificial

Capítulo I. De la Secretaría de Ciencia, Humanidades, Tecnología e Innovación

Capítulo II. De la Agencia de Transformación Digital y Telecomunicaciones

Capítulo III. De la Coordinación entre la Secretaría y la Agencia

Título Sexto. Educación, Capacitación y Cultura Digital en IA

Capítulo I. Alfabetización digital y ciudadanía digital

Capítulo II. Formación docente y desarrollo de talento especializado

Capítulo III. Programas de capacitación para los sectores público y privado

Título Séptimo. De la Perspectiva de Género, Inclusión y No Discriminación en la Inteligencia Artificial

Capítulo I. Disposiciones generales

Capítulo II. Prevención y Mitigación de Sesgos Algorítmicos

Capítulo III. Violencia Digital, Deepfakes y Protección Reforzada de las Mujeres

Capítulo IV. Participación de Mujeres y Grupos Subrepresentados en el Ecosistema de IA

Capítulo V. Ciberseguridad con enfoque de Género

Capítulo VI. Inclusión Digital de Grupos en Situación de Vulnerabilidad

Capítulo VII. Obligaciones del Estado y del sector privado

Capítulo VIII. Transversalidad, Monitoreo y Actualización.

Título Octavo. Fomento al Desarrollo, Innovación y Capacidades Nacionales en Inteligencia Artificial

Capítulo I. Fomento a la investigación científica y tecnológica

Capítulo II. Financiamiento e incentivos fiscales

Capítulo III. Ecosistema emprendedor y startups de IA

Capítulo IV. Transferencia tecnológica y cooperación internacional

Capítulo V. Fondo Nacional para el Desarrollo de la Inteligencia Artificial

Título Noveno. Evaluación, Clasificación y Gestión de Riesgos en Sistemas de Inteligencia Artificial

Capítulo I. Evaluación de impacto algorítmico

Capítulo II. Regulación de sistemas de IA de alto riesgo

Capítulo III. Certificación, estándares y auditorías

Capítulo IV. Supervisión continua y actualización normativa

Título Décimo. De las Aplicaciones Prohibidas y de Alto Riesgo de la Inteligencia Artificial

Capítulo I. De las Aplicaciones Prohibidas de la Inteligencia Artificial

Capítulo II. De los Sistemas de Alto Riesgo

Capítulo III. Del Control, Mitigación y Gestión de Riesgos

Título Décimo Primero. Derechos y Obligaciones de Desarrolladores, Operadores, Proveedores y Usuarios

Capítulo I. Derechos de los usuarios frente a la IA

Capítulo II. Obligaciones de proveedores y desarrolladores

Capítulo III. Responsabilidad civil, administrativa y penal

Título Décimo Segundo. Transparencia, Rendición de Cuentas y Datos Abiertos

Capítulo I. Registro Nacional de Sistemas de IA

Capítulo II. Publicidad de algoritmos y decisiones automatizadas

Capítulo III. Acceso ciudadano a información y mecanismos de rendición de cuentas

Título Décimo Tercero. Procedimientos Administrativos en Materia de IA

Capítulo I. Registro, certificación y autorización de sistemas de IA

Capítulo II. Procedimientos de auditoría y supervisión

Capítulo III. Procedimientos de queja, reparación y atención a usuarios afectados

Título Décimo Cuarto. Infracciones, Responsabilidades y Sanciones

Capítulo I. Clasificación de infracciones

Capítulo II. Procedimiento sancionador

Capítulo III. Medidas de reparación y sanciones aplicables

Transitorios

LEY GENERAL PARA REGULAR Y FOMENTAR EL USO DE LA INTELIGENCIA ARTIFICIAL EN MÉXICO

TÍTULO PRIMERO

Disposiciones Generales

Capítulo I. Objeto, naturaleza y finalidad de la Ley

Artículo 1. La presente Ley es de orden público, interés social y observancia general en todo el territorio nacional. Su objeto es regular, fomentar y supervisar el desarrollo, implementación y uso de los sistemas de inteligencia artificial, en congruencia con la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales de los que México sea parte y la legislación aplicable.

Artículo 2. La Ley tiene naturaleza general y establece un marco normativo horizontal, flexible y basado en principios, que servirá de referencia para la regulación sectorial específica en ámbitos como salud, educación, seguridad, trabajo, medio ambiente, datos personales, propiedad intelectual, entre otros.

Artículo 3. La finalidad de esta Ley es:

- I. Garantizar que la inteligencia artificial se desarrolle y utilice en respeto a los derechos humanos, las libertades fundamentales y los valores democráticos;
- II. Promover la innovación tecnológica nacional y el fortalecimiento de la soberanía digital, con inclusión de todos los actores del ecosistema;
- III. Establecer mecanismos de gobernanza plural que integren a la Federación, entidades federativas, municipios, sector privado, académico y social;

- IV. Proteger la seguridad nacional, la estabilidad democrática, la privacidad, los neuroderechos y la integridad cognitiva de las personas;
- V. Impulsar un desarrollo sostenible, responsable y con perspectiva de equidad, evitando sesgos y discriminación algorítmica;
- VI. Garantizar la compatibilidad de la legislación mexicana con los marcos internacionales relevantes, especialmente en el ámbito regional de América del Norte.

Capítulo II. Definiciones y terminología

Artículo 4. Para efectos de la presente Ley, se entenderá por:

I. Algoritmo. Conjunto de instrucciones, reglas o procesos lógicos que permiten a un sistema de inteligencia artificial procesar datos y generar resultados, inferencias o decisiones automatizadas.

II. Auditoría algorítmica. Proceso de revisión técnica, ética y jurídica de un sistema de inteligencia artificial, en desarrollo o en operación, destinado a verificar su cumplimiento de los principios de transparencia, explicabilidad, trazabilidad, no discriminación y respeto a los derechos humanos.

III. Autonomía funcional de la IA. Capacidad de un sistema de inteligencia artificial para ejecutar tareas, tomar decisiones o generar resultados sin intervención humana directa en cada operación, dentro de parámetros previamente definidos por desarrolladores o usuarios autorizados.

IV. Biometría y datos biométricos. Datos personales relativos a características físicas, fisiológicas o conductuales de una persona que permiten su identificación única, tales como huellas dactilares, patrones faciales, voz, iris o marcha, utilizados para entrenamiento, validación o operación de sistemas de inteligencia artificial.

V. Ciberdefensa. Conjunto de acciones y capacidades técnicas, operativas y estratégicas orientadas a proteger la infraestructura digital crítica y los sistemas de inteligencia artificial frente a amenazas que comprometan la seguridad nacional o la seguridad pública.

- VI. Ciberseguridad.** Conjunto de políticas, procesos, medidas y tecnologías orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información, así como la resiliencia de los sistemas de inteligencia artificial, ante amenazas, ataques o accesos no autorizados.
- VII. Datos abiertos.** Información generada por instituciones públicas que puede ser utilizada, reutilizada y redistribuida libremente por cualquier persona, sin restricciones de uso o licencia, garantizando transparencia, rendición de cuentas y acceso público.
- VIII. Datos personales.** Cualquier información concerniente a una persona física identificada o identificable, conforme a lo establecido en la legislación aplicable en materia de protección de datos personales.
- IX. Datos sensibles.** Datos personales que afectan directamente la esfera más íntima de la persona titular, y cuya utilización indebida puede generar discriminación, vulneración de derechos o un riesgo grave para su seguridad, por lo que requieren un nivel de protección reforzado.
- X. Desarrollador.** Persona física o moral que diseña, entrena, ajusta, prueba o modifica modelos, algoritmos o sistemas de inteligencia artificial, incluyendo la definición de su arquitectura, datos de entrenamiento o parámetros técnicos, con independencia de que posteriormente los comercialice, implemente o ponga a disposición de terceros.
- XI. Desinformación digital.** Contenido falso, manipulado o fuera de contexto, generado o difundido mediante inteligencia artificial o a través de medios digitales, con el propósito de afectar la opinión pública, los procesos electorales, los derechos de las personas o la seguridad nacional.
- XII. Evaluación de impacto algorítmico.** Proceso sistemático, previo y posterior a la implementación de un sistema de inteligencia artificial, destinado a identificar, prevenir, mitigar y monitorear los riesgos éticos, sociales, ambientales, de derechos humanos y de seguridad asociados a su diseño, desarrollo o uso, garantizando su conformidad con los principios y la legislación aplicable.

- XIII. Explicabilidad.** Cualidad de un sistema de inteligencia artificial que facilita la comprensión de los procesos y criterios utilizados en la generación de resultados, inferencias o decisiones, de manera clara, verificable y auditable por personas o autoridades competentes.
- XIV. Falsificación digital (deepfake).** Contenido sintético o manipulado, generado mediante inteligencia artificial, que reproduce o altera la imagen, voz o comportamiento de una persona con apariencia de veracidad, con el potencial de afectar su identidad, reputación, derechos o procesos democráticos.
- XV. Fines prohibidos de la IA.** Aplicaciones de inteligencia artificial que, por su naturaleza o impacto, están expresamente prohibidas por esta Ley, incluyendo la manipulación cognitiva coercitiva, la puntuación social estatal, el uso de sistemas de identificación biométrica masiva sin base legal, y cualquier otra que vulnere derechos humanos o la seguridad nacional.
- XVI. Gobernanza de la IA.** Conjunto de mecanismos institucionales, normativos y sociales que regulan, coordinan y supervisan el desarrollo, implementación, uso y evaluación de la inteligencia artificial, con base en principios de inclusión, transparencia, rendición de cuentas y desarrollo sostenible.
- XVII. Grupo vulnerable o en situación de riesgo algorítmico.** Personas o colectivos cuya situación socioeconómica, de género, discapacidad, edad, etnia, condición migratoria u otras características los expone de manera desproporcionada a impactos adversos derivados del uso de sistemas de inteligencia artificial.
- XVIII. Inclusión digital.** Condición de acceso social equitativo, seguro y no discriminatorio a la infraestructura, conectividad, dispositivos, herramientas y competencias digitales necesarias para el uso y beneficio de la inteligencia artificial.
- XIX. Infraestructura crítica digital.** Conjunto de sistemas, redes, plataformas, centros de datos, modelos y servicios tecnológicos cuya interrupción o afectación pueda comprometer la seguridad nacional, la continuidad institucional, la prestación de servicios esenciales o la integridad del ecosistema digital.
- XX. Inteligencia artificial (IA).** Sistema socio-técnico basado en modelos computacionales o matemáticos que, a partir del procesamiento de datos, señales

o instrucciones, realiza funciones de aprendizaje, razonamiento, predicción, clasificación, generación de contenidos o comprensión del lenguaje, con el objetivo de producir resultados, decisiones o acciones que, de efectuarse exclusivamente por personas, requerirían inteligencia o juicio humano; pudiendo operar de manera autónoma, semiautónoma o asistida, y cuyo comportamiento y resultados dependen de su diseño, entrenamiento, uso y contexto de aplicación.

- XXI. Inteligencia artificial generativa.** Subcampo de la inteligencia artificial orientado a la creación autónoma o asistida de texto, imágenes, audio, video u otros contenidos sintéticos o modificados, mediante el uso de modelos de propósito general entrenados con grandes volúmenes de datos.
- XXII. Interoperabilidad.** Capacidad de distintos sistemas de inteligencia artificial, plataformas o infraestructuras digitales para compartir información y operar de manera conjunta, eficaz, segura y confiable, asegurando la compatibilidad técnica, semántica y normativa entre sectores, instituciones y niveles de gobierno.
- XXIII. Mitigación algorítmica.** Conjunto de medidas técnicas, normativas u operativas destinadas a reducir o eliminar riesgos asociados al diseño, funcionamiento o impacto de los sistemas de inteligencia artificial.
- XXIV. Modelo de propósito general (GPAI).** Modelo de inteligencia artificial entrenado con grandes volúmenes de datos para desempeñar múltiples tareas, sin estar diseñado exclusivamente para un uso específico, y que puede integrar funciones generativas, predictivas o de razonamiento.
- XXV. Modelo fundacional.** Infraestructura algorítmica de gran escala que sirve como base para el desarrollo de aplicaciones de inteligencia artificial, entrenada mediante aprendizaje profundo u otras técnicas avanzadas.
- XXVI. Neuroderechos.** Derechos destinados a proteger la identidad personal, la privacidad mental, la integridad cognitiva, la autonomía de la voluntad y la libertad de pensamiento frente al uso de neurotecnologías o sistemas de inteligencia artificial que, de manera directa o indirecta, recolecten, procesen o interfieran en información neuronal o en los procesos mentales de las personas.
- XXVII. Neurotecnología.** Tecnología, dispositivo o sistema que registra, decodifica, estimula, altera o influye en la actividad cerebral o en procesos cognitivos, con o sin apoyo de inteligencia artificial.

XXVIII. Perspectiva de género en IA. Enfoque que identifica, previene y corrige desigualdades, discriminación o impactos diferenciales entre mujeres, hombres y personas de género diverso en el diseño, desarrollo, entrenamiento, implementación y evaluación de sistemas de inteligencia artificial.

XXIX. Plataforma de registro nacional de IA. Mecanismo digital administrado por la autoridad competente para inscribir, actualizar y consultar información relevante sobre sistemas de inteligencia artificial sujetos a obligaciones de transparencia, evaluación o auditoría.

XXX. Propiedad intelectual en IA. Régimen de protección jurídica aplicable a creaciones generadas mediante IA y al uso legítimo de datos u obras empleados para su entrenamiento.

XXXI. Proveedor. Persona física o moral que pone a disposición, comercializa, distribuye, implementa, integra, mantiene u ofrece sistemas de inteligencia artificial a terceros, ya sea de manera directa o indirecta, con independencia de que haya participado o no en su desarrollo.

XXXII. Regulación basada en riesgos. Enfoque normativo que clasifica los sistemas de inteligencia artificial en niveles conforme al riesgo que representen para los derechos humanos, la seguridad, la democracia, la salud pública o el medio ambiente, a fin de proteger el interés público, imponiendo obligaciones diferenciadas y proporcionales a dicho nivel de riesgo.

XXXIII. Responsabilidad algorítmica. Obligación de determinar y atribuir a las personas físicas o morales la responsabilidad por los efectos o consecuencias derivados del diseño, entrenamiento, despliegue o uso de sistemas de inteligencia artificial, garantizando la rendición de cuentas por sus impactos.

XXXIV. Riesgo sistémico en IA. Aquel que, debido a la interconexión y dependencia entre sistemas, sectores o infraestructuras, puede generar efectos amplificados, disruptivos o en cascada que afecten al interés público, la economía, la seguridad nacional o los derechos humanos.

XXXV. Robótica. Rama tecnológica que comprende el diseño, desarrollo y uso de dispositivos mecánicos o digitales, autónomos o semiautónomos, que mediante

inteligencia artificial son capaces de ejecutar tareas físicas o cognitivas en interacción con su entorno y en condiciones de autonomía parcial o total.

XXXVI. Sandbox regulatorio. Entorno controlado para probar sistemas de IA de alto riesgo.

XXXVII. Seguridad nacional en IA. Conjunto de capacidades, medidas y acciones destinadas a prevenir, mitigar y responder a riesgos y amenazas derivados del uso indebido, malicioso o crítico de sistemas de inteligencia artificial que puedan afectar la estabilidad, integridad o continuidad del Estado mexicano.

XXXVIII. Sesgo algorítmico. Distorsión sistemática en los resultados de un sistema de inteligencia artificial, originada por deficiencias en los datos, el diseño, el entrenamiento o el procesamiento de los modelos, que puede generar discriminación, exclusión o afectaciones a derechos fundamentales.

XXXIX. Sistema autónomo crítico. Sistema de inteligencia artificial capaz de tomar decisiones que producen efectos materiales inmediatos sobre personas, bienes o infraestructura esencial, con un nivel elevado de autonomía operativa.

XL. Sistema autónomo de decisión. Aquel sistema de inteligencia artificial que genera decisiones vinculantes o con efectos significativos para personas o instituciones, sin requerir validación humana inmediata.

XLI. Sistema de IA prohibido. Sistema cuyo desarrollo, comercialización o uso está expresamente vetado por la presente Ley por representar riesgos inaceptables para la dignidad humana, los derechos fundamentales, la democracia o la seguridad nacional.

XLII. Sistema de inteligencia artificial de alto riesgo. Aquellos sistemas que, por su finalidad, contexto de uso o efectos potenciales, sean susceptibles de impactar de forma significativa en los derechos humanos, la seguridad nacional, los procesos democráticos, la salud pública, el medio ambiente o la estabilidad económica, y que, por tanto, estén sujetos a mayores obligaciones de evaluación, transparencia y supervisión.

XLIII. Soberanía y autonomía tecnológica. Capacidad del Estado mexicano para desarrollar, regular, supervisar y aprovechar tecnologías de IA sin dependencia

crítica de actores externos, garantizando seguridad nacional, continuidad operativa e interés público.

XLIV. Supervisión humana significativa. Principio conforme al cual toda decisión automatizada de alto impacto sobre personas o bienes deberá contar con la posibilidad real de intervención, revisión o validación por parte de una persona humana responsable, a fin de garantizar el control y la rendición de cuentas en el uso de sistemas de inteligencia artificial.

XLV. Trazabilidad algorítmica. Capacidad técnica y documental para reconstruir el origen de los datos, decisiones y procesos utilizados por un sistema de inteligencia artificial, a fin de permitir auditorías y responsabilidades.

XLVI. Transparencia algorítmica. Principio conforme al cual los procesos, criterios y resultados de los sistemas de inteligencia artificial deberán ser comprensibles, explicables y auditables por las autoridades competentes, los usuarios y la sociedad, a fin de garantizar la rendición de cuentas, la trazabilidad y el control público sobre las decisiones automatizadas.

XLVII. Usuario de sistemas de IA. Persona física o moral que interactúa con, opera, utiliza o se beneficia, de manera directa o indirecta, de un sistema de inteligencia artificial, con conocimiento o sin él, y que puede resultar impactada por sus decisiones, resultados o efectos.

XLVIII. Verificación algorítmica independiente. Proceso mediante el cual un tercero acreditado evalúa el desempeño, seguridad, transparencia y cumplimiento normativo de un sistema de inteligencia artificial, sin conflicto de interés alguno.

XLIX. Vigilancia y supervisión continua. Mecanismos permanentes de monitoreo, evaluación y actualización de sistemas de inteligencia artificial una vez implementados, con el fin de detectar desviaciones, riesgos emergentes o impactos no previstos.

Capítulo III. Ámbito de aplicación

Artículo 5. La presente Ley es de orden público, interés social y observancia general en todo el territorio nacional. Será aplicable a todas las personas físicas o morales, públicas o privadas, nacionales o extranjeras, que investiguen, desarrollen,

implementen, comercialicen, utilicen o supervisen sistemas de inteligencia artificial cuyos efectos se produzcan en el territorio nacional o sobre personas sujetas a la jurisdicción mexicana. Asimismo, será aplicable a las autoridades de los tres órdenes de gobierno que participen en su regulación, promoción, fomento, supervisión o vigilancia.

Artículo 6. Esta Ley también será aplicable a los sistemas de inteligencia artificial cuyo diseño, operación o efectos trasciendan el territorio nacional, cuando:

- I. Generen impactos directos o significativos en los derechos humanos, la seguridad nacional, los procesos democráticos, la salud pública, el medio ambiente o la economía mexicana; o
- II. Sean utilizados por personas o entidades extranjeras en la prestación de servicios a personas físicas o morales residentes en México, o cuyos efectos se produzcan en el territorio nacional.

Artículo 7. La presente Ley será aplicable, de manera enunciativa mas no limitativa, en los siguientes ámbitos sectoriales:

- I. Administración pública y gobierno digital: identidad digital, interoperabilidad y datos abiertos;
- II. Aduanas, comercio exterior y facilitación del comercio internacional;
- III. Agroalimentario, agrícola y pesquero;
- IV. Ambiente, cambio climático, biodiversidad y gestión hídrica;
- V. Archivos, transparencia y acceso a la información pública;
- VI. Ciencia, humanidades, tecnologías e innovación;
- VII. Ciberseguridad y seguridad de la información;
- VIII. Comercio digital, plataformas y derechos de las personas consumidoras;
- IX. Competencia económica y mercados digitales;
- X. Cultura, industrias creativas y contenidos digitales;
- XI. Datos personales, privacidad y datos sensibles;
- XII. Defensa y seguridad nacional;
- XIII. Democracia, procesos electorales y combate a la desinformación;
- XIV. Desarrollo social y atención a grupos en situación de vulnerabilidad;
- XV. Discapacidad, accesibilidad e inclusión digital;
- XVI. Educación básica, media, superior y capacitación continua;
- XVII. Energía, hidrocarburos y electricidad;
- XVIII. Estadística y geografía oficiales;
- XIX. Finanzas públicas, sistema financiero, fintech, valores, seguros y pensiones;

- XX. Justicia, seguridad pública, sistema penitenciario y procuración de justicia;
- XXI. Laboral, seguridad social y relaciones de trabajo;
- XXII. Migración, refugio y control fronterizo;
- XXIII. Minería y aprovechamiento de recursos naturales;
- XXIV. Movilidad, transporte, logística y ciudades inteligentes;
- XXV. Propiedad intelectual, derecho de autor y propiedad industrial;
- XXVI. Protección civil y gestión integral de riesgos;
- XXVII. Publicidad, comunicación social y verificación de contenidos digitales;
- XXVIII. Salud, dispositivos médicos, farmacovigilancia y salud digital;
- XXIX. Telecomunicaciones y radiodifusión;
- XXX. Turismo, patrimonio cultural y servicios asociados;
- XXXI. Urbanismo, catastro, ordenamiento territorial y vivienda.

Los ámbitos aquí mencionados no excluyen otros sectores en los que la inteligencia artificial pueda tener aplicación o impacto relevante.

Artículo 8. La aplicación de esta Ley se guiará conforme a un enfoque basado en riesgos, mediante el cual los sistemas de inteligencia artificial serán clasificados de acuerdo con su nivel de impacto en los derechos humanos, la seguridad nacional, la estabilidad democrática, la salud pública, el medio ambiente y la economía nacional.

I. Los sistemas de alto riesgo quedarán sujetos a obligaciones reforzadas de registro, evaluación, certificación, auditoría y supervisión, en los términos que establezca esta Ley y su Reglamento.

II. Los sistemas de uso limitado o personal estarán sujetos únicamente a principios básicos de seguridad, transparencia y no discriminación, en los términos que determine el Reglamento.

Artículo 9. Lo dispuesto en esta Ley se interpretará y aplicará de manera armónica con la Constitución Política de los Estados Unidos Mexicanos y, de forma enunciativa mas no limitativa, con las siguientes normas:

1. Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación
2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
3. Ley General de Transparencia y Acceso a la Información Pública

4. Ley General de Archivos
5. Ley General de Protección Civil
6. Ley General del Equilibrio Ecológico y la Protección al Ambiente
7. Ley General de Cambio Climático
8. Ley General de Salud
9. Ley General de Educación
10. Ley General de Educación Superior
11. Ley General del Sistema Nacional de Seguridad Pública
12. Ley General para Prevenir y Eliminar la Discriminación
13. Ley General de los Derechos de Niñas, Niños y Adolescentes
14. Ley General para la Inclusión de las Personas con Discapacidad
15. Ley General de Víctimas
16. Ley General de Mejora Regulatoria
17. Ley Orgánica de la Administración Pública Federal
18. Ley Federal de Protección de Datos Personales en Posesión de los Particulares
19. Ley Federal de Telecomunicaciones y Radiodifusión
20. Ley de Infraestructura de la Calidad
21. Ley Federal de Protección al Consumidor
22. Ley Federal del Derecho de Autor
23. Ley Federal de Protección a la Propiedad Industrial
24. Ley Federal de Transparencia y Acceso a la Información Pública
25. Ley del Sistema Nacional de Información Estadística y Geográfica
26. Ley Federal de Responsabilidad Ambiental
27. Ley Federal del Trabajo
28. Ley del Seguro Social
29. Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE)
30. Ley Federal de Competencia Económica

31. Ley para Regular las Instituciones de Tecnología Financiera
32. Ley de Instituciones de Crédito
33. Ley del Mercado de Valores
34. Ley de Protección y Defensa al Usuario de Servicios Financieros
35. Ley Aduanera
36. Ley de Migración
37. Ley de Seguridad Nacional
38. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público
39. Ley de Obras Públicas y Servicios Relacionados con las Mismas
40. Código Civil Federal
41. Código Penal Federal
42. Código Nacional de Procedimientos Penales
43. Código de Comercio

Artículo 10. La presente Ley se aplicará en armonía con los tratados internacionales de los que México sea parte, en particular con los instrumentos de la UNESCO, las recomendaciones de la OCDE y el Tratado entre México, Estados Unidos y Canadá (T-MEC), siempre que sean compatibles con la soberanía tecnológica, la seguridad nacional y el interés público mexicano.

TÍTULO SEGUNDO

Principios Éticos, Derechos Humanos y Neuroderechos

Capítulo I. Principios rectores de la IA

Artículo 11. El desarrollo, implementación, despliegue, uso, fomento y supervisión de los sistemas de inteligencia artificial deberán regirse por los siguientes principios rectores: respeto a los derechos humanos, a la dignidad humana y a los valores democráticos; legalidad y seguridad jurídica; transparencia, explicabilidad y trazabilidad de los sistemas; rendición de cuentas y responsabilidad de los actores involucrados; supervisión humana significativa; inclusión y accesibilidad; innovación responsable y soberanía tecnológica; protección de la privacidad y de los datos personales; equidad y no discriminación en el diseño algorítmico, así como en el uso y acceso a los sistemas de inteligencia artificial; protección reforzada de personas y grupos en situación de vulnerabilidad; protección de los derechos laborales, culturales, creativos y de propiedad industrial e intelectual, incluidos los derechos sobre la voz, la imagen, la identidad, la obra y la autoría de intérpretes, actores, artistas, escritores, locutores, periodistas,

autores, compositores y demás personas creadoras; seguridad, robustez y resiliencia técnica; sostenibilidad ambiental; orientación al bienestar social; proporcionalidad y regulación basada en riesgos; y cooperación internacional compatible con la soberanía nacional.

Artículo 12. Los principios rectores previstos en este Capítulo serán de observancia obligatoria para todas las autoridades, organismos autónomos, entidades federativas y municipios, así como para los desarrolladores, proveedores, operadores y usuarios de sistemas de inteligencia artificial, conforme a su grado de control y responsabilidad. Asimismo, servirán como criterio de interpretación e integración normativa en la aplicación de la presente Ley.

Artículo 12 Bis. Además de lo dispuesto en el artículo anterior, el desarrollo, implementación, despliegue, uso, fomento, supervisión y regulación de los sistemas de inteligencia artificial en el territorio nacional deberán observar, de manera transversal y obligatoria, y proporcional al grado de control y responsabilidad que corresponda a cada sujeto involucrado en el ciclo de vida de los sistemas de IA, los siguientes principios orientadores. Dichos principios constituirán el núcleo axiológico de la presente Ley y servirán como criterios de interpretación, integración normativa, diseño institucional, elaboración reglamentaria y evaluación de las políticas públicas en la materia.

I. La inteligencia artificial debe ampliar derechos, nunca reducirlos. Esta tecnología deberá contribuir a ampliar y fortalecer el ejercicio efectivo de los derechos humanos y libertades fundamentales, y nunca a restringirlos, menoscabarlos o sustituirlos. En ningún caso podrán desarrollarse o utilizarse sistemas de inteligencia artificial con fines de exclusión, discriminación, desinformación o regresión de derechos.

II. Toda decisión apoyada por inteligencia artificial debe tener responsables humanos, sustentada en marcos institucionales claros. De manera obligatoria deberá contar con responsables humanos claramente identificables, dentro de marcos institucionales definidos, que determinen quién diseña, quién decide, quién supervisa y quién responde por los efectos, resultados o daños derivados de su uso. La automatización no exime ni diluye la responsabilidad jurídica, administrativa, civil o penal.

III. Si una decisión no puede explicarse, no debe automatizarse. Ninguna decisión que produzca efectos jurídicos o impactos significativos sobre derechos o intereses de las personas podrá ser automatizada cuando no sea razonablemente explicable,

comprensible, revisable y, en su caso, repetible. La falta de explicabilidad suficiente constituirá un límite material a la automatización.

IV. *La inteligencia artificial se gobierna mejor cuando se decide en colectivo.* El diseño, regulación, supervisión y uso de los sistemas de inteligencia artificial deberán realizarse mediante procesos de toma de decisiones colectivas, plurales y transparentes, que incorporen mecanismos de participación de la ciudadanía, la academia, las comunidades, las organizaciones sociales, el sector productivo y las autoridades competentes, orientados al interés público.

V. *La inteligencia artificial solo es valiosa si genera bienestar para las personas.* La inteligencia artificial deberá orientarse a la generación de bienestar social, valor público y beneficios tangibles, contribuyendo a la reducción de desigualdades, la mejora de los servicios públicos, el desarrollo sostenible y la cohesión social, más allá de su eficiencia técnica o económica.

VI. *Antes de automatizar, hay que comprender a quién y qué afecta.* Previo a la automatización de procesos, decisiones o servicios, deberán evaluarse de manera anticipada y continua los posibles impactos sociales, económicos, territoriales, ambientales y culturales, así como los efectos diferenciados sobre grupos en situación de vulnerabilidad, a fin de prevenir daños, riesgos o afectaciones desproporcionadas.

VII. *La tecnología estratégica debe responder a las necesidades del país.* El desarrollo y uso de la inteligencia artificial deberá orientarse a atender las necesidades nacionales, fortalecer las capacidades públicas y productivas, y alinearse con una visión de largo plazo que preserve la soberanía tecnológica, la seguridad nacional y el interés público.

VIII. *El desarrollo de la inteligencia artificial requiere fortalecer la educación y el conocimiento en el país.* Deberá impulsarse el fortalecimiento permanente de la educación, la investigación científica y la formación interdisciplinaria, así como la divulgación del conocimiento, la capacitación continua del talento humano y la reconversión de perfiles profesionales en todos los niveles educativos.

IX. *La inteligencia artificial no puede ser ajena a la diversidad cultural y lingüística del país.* Los sistemas de inteligencia artificial deberán respetar y promover la diversidad cultural y lingüística, incluidas las lenguas indígenas y las expresiones culturales nacionales, evitando sesgos, homogeneización indebida o la exclusión de comunidades históricamente marginadas.

X. *Los datos son un bien público que deben cuidarse con responsabilidad.* Los datos que alimentan los sistemas de inteligencia artificial deberán tratarse como un bien de interés público, garantizando su calidad, representatividad, seguridad, privacidad y uso ético, así como la protección de la información sensible y la ciberseguridad a lo largo de todo su ciclo de vida.

Los principios previstos en el presente artículo deberán aplicarse de manera armónica con los derechos humanos, los neuroderechos, las obligaciones de transparencia, los mecanismos de supervisión humana significativa, los procedimientos administrativos y el régimen de responsabilidades y sanciones establecidos en esta Ley.

Capítulo II. Derechos humanos aplicables a la IA

Artículo 13. El desarrollo, implementación, despliegue, uso, fomento y supervisión de la inteligencia artificial deberán respetar, proteger y garantizar los derechos humanos reconocidos en la Constitución, en los tratados internacionales de los que el Estado mexicano sea parte y en la legislación aplicable.

En ningún caso el desarrollo, implementación, despliegue, uso, fomento y supervisión de sistemas de inteligencia artificial podrá justificar la restricción, regresión o sustitución indebida de derechos humanos previamente reconocidos.

Artículo 14. Queda prohibida la utilización de sistemas de inteligencia artificial que tengan por objeto o efecto vulnerar de manera grave la dignidad humana, la integridad personal, la igualdad y la no discriminación, así como aquellos que afecten indebidamente la libertad de expresión o el debido proceso.

Artículo 15. Toda persona tendrá derecho a que las decisiones automatizadas o semiautomatizadas que produzcan efectos significativos sobre sus derechos o intereses sean comprensibles, explicables y revisables, y cuenten con supervisión humana significativa. Las personas deberán ser notificadas cuando una decisión, recomendación o proceso haya sido asistido por inteligencia artificial y tendrán acceso a las razones principales, a sus datos personales utilizados o a la información relevante del sistema necesaria para su interpretación, así como a los mecanismos de corrección, revisión o impugnación.

Artículo 16. Las instituciones públicas y las entidades privadas que desarrollen,

desplieguen o utilicen sistemas de inteligencia artificial de alto riesgo deberán realizar, previamente a su puesta en operación, evaluaciones de impacto en derechos humanos que incorporen un enfoque diferencial y de inclusión respecto de niñas, niños y adolescentes, personas con discapacidad, pueblos y comunidades indígenas y demás grupos en situación de vulnerabilidad. El Estado promoverá medidas de alfabetización y formación en derechos humanos en el entorno digital.

Capítulo III. Reconocimiento y protección de los neuroderechos

Artículo 17. Para efectos de esta Ley, los neuroderechos deberán interpretarse y aplicarse conforme al bloque de constitucionalidad en materia de derechos humanos, de acuerdo con lo dispuesto por el artículo 1º de la Constitución Política de los Estados Unidos Mexicanos y por los tratados internacionales aplicables.

Artículo 18. Se reconocen y protegen los siguientes neuroderechos:

- I. Identidad personal y continuidad psicológica;
- II. Privacidad mental;
- III. Integridad cognitiva y protección frente a interferencias no consentidas;
- IV. Autonomía de la voluntad;
- V. Equidad y no manipulación neurotecnológica indebida.

Artículo 19. La investigación, desarrollo, despliegue, aplicación y uso de neurotecnologías e interfaces cerebro-máquina asociadas a sistemas de inteligencia artificial se sujetarán a consentimiento previo, libre, informado y específico, así como a principios de bioseguridad, ética científica y proporcionalidad. Queda prohibida su utilización para alterar, interferir o condicionar procesos neuronales sin el consentimiento expreso de la persona.

Artículo 20. La autoridad competente establecerá protocolos específicos para la evaluación, certificación y supervisión de tecnologías que procesen, registren o interactúen con datos neuronales o información cognitiva. Asimismo, promoverá la cooperación internacional y la armonización regulatoria en la materia, respetando la soberanía tecnológica del Estado y la integridad cognitiva de las personas.

Capítulo IV. Privacidad, protección de datos y ciberseguridad

Artículo 21. Toda persona tiene derecho a la protección de sus datos personales

tratados por sistemas de inteligencia artificial, de conformidad con la Constitución, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás disposiciones aplicables.

Artículo 22. El tratamiento de datos personales mediante sistemas de inteligencia artificial observará los principios de licitud, lealtad, transparencia, finalidad específica, minimización, proporcionalidad, exactitud, conservación limitada y responsabilidad proactiva, y garantizará en todo momento el ejercicio de los derechos ARCO. En el caso de decisiones automatizadas o semiautomatizadas que produzcan efectos significativos sobre los derechos o intereses de una persona, esta tendrá derecho a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión.

Artículo 23. Los responsables deberán implementar medidas de seguridad desde el diseño y por defecto para el tratamiento de datos personales mediante sistemas de inteligencia artificial, reforzadas en el caso de sistemas de alto riesgo. Dichas medidas incluirán evaluaciones de impacto en privacidad, cifrado, seudonimización u otras técnicas de protección equivalentes, gestión de vulnerabilidades y la notificación de incidentes o brechas de seguridad de datos personales a la autoridad competente y, cuando proceda, a los titulares, en los términos que establezca el Reglamento.

Artículo 24. El Estado promoverá políticas de ciberseguridad que garanticen la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de inteligencia artificial. Asimismo, fomentará la adopción de estándares y certificaciones reconocidas, la realización de pruebas de conformidad y la implementación de mecanismos de auditoría y trazabilidad.

Artículo 25. Las autoridades competentes coordinarán acciones con las instituciones de seguridad, telecomunicaciones, justicia y protección de datos para prevenir, investigar y sancionar ataques cibernéticos, accesos no autorizados, filtraciones, así como la alteración o manipulación ilícita de datos personales asociados con sistemas de inteligencia artificial. Asimismo, deberán actuar frente a transferencias internacionales de datos personales que se realicen sin las garantías previstas en la legislación aplicable.

TÍTULO TERCERO.

De la Gobernanza y Coordinación Multinivel en Inteligencia Artificial

Capítulo I. De las Competencias de la Federación

Artículo 26. Corresponde a la Federación conducir la política nacional en materia de inteligencia artificial, establecer la normatividad general, coordinar la planeación estratégica y garantizar la observancia de los principios, derechos y obligaciones previstos en esta Ley y su Reglamento.

Artículo 27. La Federación, por conducto de las dependencias competentes, tendrá a su cargo:

- I. Expedir disposiciones de carácter general, lineamientos técnicos y normas oficiales mexicanas aplicables al desarrollo, implementación y uso de la inteligencia artificial;
- II. Determinar metodologías de evaluación y clasificación de riesgos, así como criterios para identificar sistemas de alto impacto;
- III. Establecer lineamientos en materia de seguridad, transparencia, trazabilidad, explicabilidad y auditoría algorítmica;
- IV. Promover la interoperabilidad y la compatibilidad técnica de los sistemas de inteligencia artificial en los sectores público y privado;
- V. Definir y aplicar políticas de fomento a la investigación, innovación y desarrollo tecnológico en inteligencia artificial.

Artículo 28. La Federación creará el Registro Nacional de Sistemas de Inteligencia Artificial, de carácter público, con el objeto de concentrar información sobre los sistemas de alto riesgo, los sistemas de propósito general y aquellos utilizados por las dependencias y entidades de la Administración Pública Federal, entre otros.

La inscripción en el Registro se realizará conforme al procedimiento que determine la Autoridad Nacional, una vez que el sistema haya sido clasificado conforme al procedimiento previsto en esta Ley.

Artículo 29. Compete a la Federación la vigilancia, verificación y control de los sistemas de inteligencia artificial que impliquen riesgos significativos para la seguridad nacional, los derechos humanos, la salud pública, el medio ambiente o la estabilidad democrática.

Artículo 30. La Federación representará a México en los foros y organismos internacionales en materia de inteligencia artificial, y podrá celebrar acuerdos de cooperación técnica, científica y académica, siempre que se respeten la soberanía tecnológica y los principios establecidos en esta Ley.

Capítulo II. De las Competencias de las Entidades Federativas

Artículo 31. Corresponde a las entidades federativas, en el ámbito de sus

competencias, promover el desarrollo y uso de la inteligencia artificial conforme a los principios y disposiciones de esta Ley, así como emitir legislación complementaria y desarrollar políticas públicas en coordinación con la Federación.

Artículo 32. Los gobiernos de las entidades federativas deberán:

- I. Elaborar y ejecutar políticas, estrategias y programas estatales de inteligencia artificial, en congruencia con la política nacional;
- II. Crear o designar organismos estatales especializados en tecnologías emergentes o inteligencia artificial;
- III. Fomentar la capacitación, la alfabetización digital y la formación de talento en materia de inteligencia artificial;
- IV. Promover la investigación científica, el desarrollo tecnológico y la innovación con perspectiva regional;
- V. Implementar mecanismos de cooperación con instituciones académicas, centros de investigación y el sector productivo local.

Artículo 33. Las entidades federativas podrán celebrar convenios de coordinación con la Federación, los municipios y los organismos autónomos, a fin de establecer mecanismos de intercambio de información, buenas prácticas y recursos técnicos para el desarrollo de la inteligencia artificial.

Capítulo III. De las Competencias de los Municipios

Artículo 34. Los municipios, en el ámbito de sus atribuciones, deberán promover el uso responsable, ético y transparente de la inteligencia artificial en los servicios públicos locales y en la gestión administrativa, cuando corresponda.

Artículo 35. Los ayuntamientos podrán:

- I. Aplicar tecnologías de inteligencia artificial para mejorar los servicios públicos, garantizando la protección de datos personales y promoviendo la participación ciudadana;

- II. Impulsar programas de alfabetización digital y uso ético de la inteligencia artificial en la comunidad;
- III. Coordinarse con los gobiernos estatal y federal para implementar proyectos piloto o laboratorios urbanos de innovación tecnológica; y
- IV. Fomentar la cooperación con el sector privado y académico para el desarrollo de soluciones locales basadas en inteligencia artificial.

Artículo 36. Los municipios deberán rendir informes anuales, en términos de la legislación aplicable, sobre el uso de sistemas de inteligencia artificial en el ejercicio de sus funciones, incluyendo objetivos, beneficios, riesgos identificados y medidas de protección de datos personales. Asimismo, deberán garantizar mecanismos de transparencia, supervisión y rendición de cuentas ante la población, de acuerdo con sus capacidades institucionales.

Capítulo IV. De la Coordinación Nacional e Interinstitucional

Artículo 37. Se crea el Sistema Nacional de Inteligencia Artificial, como mecanismo permanente de coordinación entre los tres órdenes de gobierno, los poderes de la Unión, los organismos constitucionales autónomos, las instituciones académicas, el sector privado y la sociedad civil.

Artículo 38. El Sistema Nacional de Inteligencia Artificial tendrá por objeto:

- I. Establecer políticas, estrategias y programas de alcance nacional;
- II. Promover la cooperación técnica y científica entre instituciones públicas y privadas;
- III. Impulsar la evaluación, certificación y supervisión de los sistemas de inteligencia artificial;
- IV. Coordinar la actualización del Glosario Reglamentario y la armonización normativa;
- V. Facilitar la interlocución internacional del Estado mexicano en la materia.

Artículo 39. La coordinación del Sistema Nacional estará a cargo de una instancia de nueva creación, que será establecida por el Ejecutivo Federal como autoridad responsable de la coordinación, articulación y seguimiento de la política nacional en materia de inteligencia artificial. Para efectos exclusivamente de esta Ley, dicha

instancia se denominará Autoridad Nacional en Inteligencia Artificial, y actuará como órgano de coordinación y apoyo técnico, con autonomía técnica y de gestión, en los términos que establezca esta Ley y su Reglamento.

Artículo 40. La Autoridad Nacional en Inteligencia Artificial integrará un Consejo Consultivo Nacional, con la participación de los sectores público, privado, académico y social, el cual emitirá opiniones y recomendaciones de carácter no vinculante en materia de ética, seguridad, innovación y derechos humanos, así como propuestas de mejora o adecuación a la legislación general o sectorial en materia de inteligencia artificial.

Capítulo V. De la Gobernanza Sectorial y Participación Social

Artículo 41. La gobernanza en materia de inteligencia artificial se orientará bajo los principios de pluralidad, inclusión, transparencia, seguridad, derechos humanos, ética, corresponsabilidad fomento y participación multisectorial.

Artículo 42. El Estado promoverá la creación de consejos sectoriales y observatorios ciudadanos de inteligencia artificial, como instancias de consulta, evaluación y seguimiento de políticas públicas y desarrollos tecnológicos en sectores estratégicos.

Artículo 43. Los consejos y observatorios deberán integrarse con representación de los sectores académico, privado, público, social y de derechos humanos.

Artículo 44. Los consejos sectoriales podrán formular recomendaciones a las autoridades competentes, emitir informes técnicos y proponer códigos de conducta o buenas prácticas para el desarrollo ético y responsable de la inteligencia artificial.

Artículo 45. La participación social en la gobernanza de la inteligencia artificial se garantizará mediante mecanismos de transparencia proactiva, acceso a la información, consulta pública, protección de denunciantes y evaluación ciudadana de los impactos sociales, económicos y tecnológicos de la inteligencia artificial.

TÍTULO CUARTO

Estrategia Nacional y Política Pública en Inteligencia Artificial

Capítulo I. Estrategia Nacional de Inteligencia Artificial

Artículo 46. La Estrategia Nacional de Inteligencia Artificial es el instrumento rector de la política pública en la materia. Su elaboración, ejecución, seguimiento

y evaluación se realizará en congruencia con la Constitución Política de los Estados Unidos Mexicanos, la Ley de Planeación y demás disposiciones aplicables.

Artículo 47. La Estrategia Nacional de Inteligencia Artificial tendrá por objeto:

- I. Establecer la visión de largo plazo para el desarrollo, uso y aprovechamiento de la inteligencia artificial en México;
- II. Definir los ejes estratégicos, prioridades y metas nacionales en materia de inteligencia artificial;
- III. Orientar la formulación de programas, políticas y proyectos en los sectores público, social y privado;
- IV. Impulsar la innovación, la competitividad y el desarrollo sostenible, con enfoque de derechos humanos, inclusión y reducción de brechas digitales;
- V. Integrar la perspectiva de género, la interculturalidad y la protección de grupos en situación de vulnerabilidad.

Artículo 48. La Estrategia Nacional de Inteligencia Artificial deberá contener, al menos:

- I. Un diagnóstico nacional sobre el estado de la inteligencia artificial, su adopción en los distintos sectores y sus impactos sociales, económicos, ambientales y en derechos humanos;
- II. La identificación de oportunidades y riesgos asociados al desarrollo y uso de la inteligencia artificial;
- III. Los ejes rectores, líneas de acción y metas nacionales en la materia;
- IV. Los mecanismos de coordinación entre los tres órdenes de gobierno, los poderes de la Unión, los organismos constitucionales autónomos y los demás actores públicos y privados del ecosistema;

V. Indicadores de resultado e impacto para el seguimiento y evaluación de la política nacional.

Artículo 49. La elaboración y actualización de la Estrategia Nacional de Inteligencia Artificial estará a cargo de la autoridad competente en la materia, en coordinación con el Sistema Nacional de Inteligencia Artificial y con la participación de representantes de los sectores académico, científico, productivo y social.

Artículo 50. La Estrategia Nacional de Inteligencia Artificial tendrá una vigencia de seis años y deberá ser revisada, al menos, a la mitad de su periodo de aplicación para introducir ajustes, actualizaciones y reorientaciones necesarias. Su aprobación corresponderá al Titular del Poder Ejecutivo Federal y será publicada en el medio de difusión oficial.

Capítulo II. Programas sectoriales y evaluación de impacto

Artículo 51. Las dependencias y entidades de la Administración Pública Federal, en el ámbito de sus atribuciones, deberán formular programas sectoriales en materia de inteligencia artificial, alineados con la Estrategia Nacional de Inteligencia Artificial y con los instrumentos de planeación nacional que resulten aplicables.

Artículo 52. Los programas sectoriales en materia de inteligencia artificial deberán incluir:

- I. Objetivos específicos, indicadores y metas sectoriales relacionadas con el desarrollo y uso de la inteligencia artificial;
- II. Proyectos y acciones prioritarias, así como los recursos humanos, materiales, tecnológicos y financieros requeridos;
- III. Medidas para promover la innovación responsable, la inclusión digital y la protección de derechos humanos;
- IV. Mecanismos de coordinación con otros sectores, órdenes de gobierno y actores relevantes;

- V. Estrategias de formación, capacitación y desarrollo de talento especializado en inteligencia artificial.

Artículo 53. Los programas sectoriales deberán incorporar, cuando correspondan, evaluaciones de impacto en derechos humanos, impacto social, económico y ambiental, así como evaluaciones de impacto algorítmico para los sistemas de inteligencia artificial de alto riesgo, en los términos que establezca esta Ley y su Reglamento.

Artículo 54. La autoridad competente establecerá un sistema de seguimiento y evaluación de la Estrategia Nacional de Inteligencia Artificial y de los programas sectoriales, que incluirá la elaboración de informes periódicos de avances, resultados e impactos, mismos que deberán hacerse públicos de manera accesible y comprensible.

Capítulo III. Vinculación con políticas de transformación digital y datos abiertos

Artículo 55. La Estrategia Nacional de Inteligencia Artificial y los programas sectoriales deberán articularse con las políticas, programas y estrategias en materia de transformación digital, gobierno digital, conectividad, inclusión digital y ciberseguridad que se encuentren vigentes.

Artículo 56. La formulación y ejecución de la política pública en inteligencia artificial deberá considerar el uso responsable de datos abiertos, la interoperabilidad de los sistemas y el aprovechamiento de la infraestructura digital existente, garantizando en todo momento la protección de datos personales y la seguridad de la información.

Artículo 57. Las dependencias y entidades de la Administración Pública deberán promover que los datos generados por sistemas de inteligencia artificial, susceptibles de ser catalogados como datos abiertos, se pongan a disposición del público en formatos accesibles, legibles por máquina y reutilizables, de conformidad con la legislación aplicable en materia de transparencia, acceso a la información y protección de datos personales.

Artículo 58. La vinculación de la Estrategia Nacional de Inteligencia Artificial con las políticas de transformación digital y de datos abiertos tendrá por finalidad:

- I. Evitar duplicidades y contradicciones entre instrumentos de planeación y políticas públicas;
- II. Potenciar el uso de la inteligencia artificial para mejorar los servicios públicos, la transparencia y la rendición de cuentas;
- III. Favorecer la innovación basada en datos, la participación ciudadana y el desarrollo de soluciones tecnológicas de alto valor público;
- IV. Contribuir a la construcción de una infraestructura digital segura, resiliente e interoperable

TÍTULO QUINTO

De las Instituciones Rectoras en Materia de Inteligencia Artificial

Capítulo I. De la Secretaría de Ciencia, Humanidades, Tecnología e Innovación

Artículo 59. Corresponde a la Secretaría de Ciencia, Humanidades, Tecnología e Innovación coordinar la política nacional en materia de investigación científica, desarrollo tecnológico e innovación relacionada con la inteligencia artificial, de conformidad con lo dispuesto en esta Ley y demás disposiciones aplicables.

Artículo 60. La Secretaría tendrá las siguientes atribuciones:

- I. Formular, dirigir y evaluar la política de desarrollo científico, humanístico y tecnológico en materia de inteligencia artificial;
- II. Establecer lineamientos para el fomento de la investigación básica, aplicada y de frontera vinculada con sistemas de inteligencia artificial;
- III. Impulsar programas de formación, capacitación y profesionalización de talento especializado en inteligencia artificial;
- IV. Promover la articulación entre instituciones de educación superior, centros de investigación, laboratorios nacionales y el sector productivo;
- V. Coordinar la asignación de estímulos, financiamientos y apoyos a la investigación, desarrollo e innovación en inteligencia artificial;
- VI. Vincular la actividad científica y tecnológica con los objetivos de la Estrategia Nacional de Inteligencia Artificial;
- VII. Expedir disposiciones técnicas y criterios metodológicos para la evaluación de impactos científicos, tecnológicos y sociales de sistemas de inteligencia artificial;
- VIII. Las demás que le confieran esta Ley y otras disposiciones aplicables.

Artículo 61. La Secretaría integrará los resultados de investigaciones, prospectivas tecnológicas y estudios estratégicos para la planeación nacional en materia de inteligencia artificial, los cuales deberán incorporarse en los instrumentos de política pública correspondientes.

Artículo 62. La Secretaría deberá coordinarse con la Agencia de Transformación Digital y Telecomunicaciones para asegurar la implementación armónica de estándares, protocolos, metodologías y mejores prácticas aplicables al desarrollo y despliegue de tecnologías de inteligencia artificial.

Capítulo II. De la Agencia de Transformación Digital y Telecomunicaciones

Artículo 63. La Agencia de Transformación Digital y Telecomunicaciones será la autoridad técnica y operativa responsable de la transformación digital del sector público

federal, la adopción segura y ética de sistemas de inteligencia artificial y la supervisión del cumplimiento de las disposiciones previstas en esta Ley.

Artículo 64. La Agencia tendrá las siguientes atribuciones:

- I. Definir estándares, metodologías, especificaciones técnicas y lineamientos para el diseño, desarrollo, adquisición, implementación y mantenimiento de sistemas de inteligencia artificial en las dependencias y entidades de la Administración Pública Federal;
- II. Coordinar la transformación digital del sector público y promover el uso de inteligencia artificial para mejorar la eficiencia administrativa, la provisión de servicios y la interoperabilidad interinstitucional;
- III. Evaluar, auditar y verificar el cumplimiento de las obligaciones previstas en esta Ley aplicables al sector público federal;
- IV. Administrar la infraestructura tecnológica necesaria para la operación de sistemas que integren inteligencia artificial en los servicios públicos;
- V. Emitir lineamientos para la gestión de riesgos tecnológicos, ciberseguridad, gobernanza de datos e integridad algorítmica en sistemas públicos;
- VI. Coordinar la adopción de modelos de referencia, certificaciones técnicas y buenas prácticas internacionales en la materia;
- VII. Integrar información técnica para el Registro Nacional de Sistemas de Inteligencia Artificial;
- VIII. Las demás que establezcan esta Ley y otras disposiciones aplicables.

Artículo 65. La Agencia podrá emitir opiniones técnicas respecto del uso, adquisición o implementación de sistemas de inteligencia artificial en el ámbito técnico-operativo, por parte de dependencias y entidades de la Administración Pública Federal.

Artículo 66. La Agencia deberá coordinarse con la Secretaría de Ciencia, Humanidades, Tecnología e Innovación para garantizar la coherencia entre las políticas de investigación, desarrollo e innovación, y la transformación digital del sector público.

Capítulo III. De la Coordinación entre la Secretaría y la Agencia

Artículo 67. La Secretaría y la Agencia deberán coordinarse para garantizar la

coherencia entre la política científica, tecnológica y de innovación, y la implementación operativa de sistemas de inteligencia artificial en la Administración Pública Federal. La coordinación prevista en este Capítulo se realizará en el marco del Sistema Nacional de Inteligencia Artificial, bajo la conducción de la Autoridad Nacional en la materia y conforme a la legislación aplicable.

Artículo 68. Para tales efectos, ambas instituciones deberán:

- I. Celebrar acuerdos de coordinación, intercambio de información técnica y generación de bases de datos interoperables;
- II. Integrar grupos de trabajo especializados para la emisión de lineamientos conjuntos;
- III. Compartir metodologías para la evaluación de impacto, análisis de riesgo e identificación de sistemas de alto impacto;
- IV. Establecer mecanismos para la implementación de laboratorios de prueba, modelos *sandbox* y entornos de innovación regulada;
- V. Coordinar la representación técnica del Estado mexicano en foros, organismos y redes internacionales en materia de inteligencia artificial, cuando así proceda;
- VI. Armonizar la política científica y tecnológica con las necesidades operativas de la transformación digital del sector público.

Artículo 69. La Secretaría y la Agencia deberán asegurar que los sistemas de inteligencia artificial adoptados por el sector público cumplan con estándares de seguridad, transparencia, explicabilidad, protección de datos personales, ética y derechos humanos.

Artículo 70. Las discrepancias técnicas que surjan entre ambas instituciones se resolverán mediante los mecanismos de coordinación que defina el Reglamento de esta Ley, privilegiando el interés público, la seguridad tecnológica del Estado y la protección de los derechos humanos.

TÍTULO SEXTO

Educación, Capacitación y Cultura Digital en Inteligencia Artificial

Capítulo I. Alfabetización digital y ciudadanía digital

Artículo 71. El Estado garantizará el derecho a la alfabetización digital y el acceso equitativo a las competencias necesarias para comprender, utilizar y evaluar sistemas de inteligencia artificial, como parte del desarrollo pleno de la ciudadanía digital.

Artículo 72. La alfabetización digital comprenderá, de manera enunciativa mas no limitativa:

- I. Competencias básicas en el uso seguro y ético de tecnologías digitales;
- II. Comprensión general de los sistemas de inteligencia artificial y sus aplicaciones;
- III. Identificación de riesgos, sesgos y desinformación digital;
- IV. Conocimiento de los derechos humanos aplicables en entornos digitales;
- V. Protección de datos personales, privacidad y seguridad en línea.

Artículo 73. Las autoridades educativas federales y locales deberán incorporar contenidos transversales relacionados con inteligencia artificial y ciudadanía digital en los planes y programas de estudio de educación básica, media superior y superior.

Artículo 74. El Estado promoverá campañas nacionales de alfabetización digital dirigidas a niñas, niños, adolescentes, personas mayores, personas con discapacidad, pueblos y comunidades indígenas y demás grupos en situación de vulnerabilidad, para garantizar la inclusión digital y prevenir brechas tecnológicas.

Capítulo II. Formación docente y desarrollo de talento especializado

Artículo 75. Las instituciones de educación, centros de investigación y organismos públicos deberán implementar programas de formación, actualización y profesionalización docente en materia de inteligencia artificial, conforme a los lineamientos que emitan las autoridades educativas competentes.

Artículo 76. El Estado fomentará la creación de programas académicos, certificaciones, posgrados y especializaciones orientadas al desarrollo de talento científico, técnico y profesional en inteligencia artificial y tecnologías asociadas.

Artículo 77. Las instituciones educativas deberán promover la inclusión de contenidos

sobre ética algorítmica, derechos humanos, neuroderechos, ciberseguridad, gobernanza digital y sostenibilidad tecnológica en la formación del talento especializado.

Artículo 78. La Secretaría de Ciencia, Humanidades, Tecnología e Innovación y la Autoridad Nacional en Inteligencia Artificial promoverán la creación de redes académicas, laboratorios de innovación y alianzas nacionales e internacionales para la formación de talento y el intercambio científico.

Capítulo III. Programas de capacitación para los sectores público y privado

Artículo 79. Las dependencias y entidades de la Administración Pública Federal, así como los gobiernos estatales y municipales, deberán implementar programas permanentes de capacitación para servidoras y servidores públicos en el uso ético, seguro y responsable de sistemas de inteligencia artificial.

Artículo 80. Las capacitaciones del sector público incluirán, al menos:

- I. Uso y evaluación de sistemas de inteligencia artificial en procedimientos administrativos;
- II. Transparencia, explicabilidad y responsabilidad algorítmica;
- III. Protección de datos personales y ciberseguridad;
- IV. Prevención de sesgos y discriminación algorítmica;
- V. Gestión de riesgos tecnológicos y operación de sistemas de alto impacto.

Artículo 81. La Autoridad Nacional en Inteligencia Artificial podrá emitir estándares mínimos de capacitación, lineamientos para la evaluación de competencias y certificaciones aplicables a servidores públicos responsables de sistemas algorítmicos.

Artículo 82. El Estado fomentará programas de capacitación dirigidos al sector privado, especialmente micro, pequeñas y medianas empresas, con el fin de impulsar la adopción responsable y competitiva de soluciones basadas en inteligencia artificial.

Artículo 83. Las cámaras empresariales, organizaciones del sector productivo, instituciones académicas y organismos de la sociedad civil podrán celebrar convenios con la Autoridad Nacional en Inteligencia Artificial para desarrollar contenidos, certificaciones y modelos de capacitación conjunta.

TÍTULO SÉPTIMO

De la Perspectiva de Género, Inclusión y No Discriminación en la Inteligencia Artificial

Capítulo I. Disposiciones Generales

Artículo 84. Las políticas, normas, estrategias, sistemas y aplicaciones de inteligencia artificial que produzcan impactos significativos en derechos, oportunidades o condiciones de vida de las personas, desarrollados, implementados, utilizados o supervisados en el territorio nacional, deberán incorporar la perspectiva de género, el enfoque interseccional, la inclusión plena y la no discriminación, garantizando la igualdad sustantiva entre mujeres y hombres, así como la protección reforzada de los grupos en situación de vulnerabilidad.

Artículo 85. Para efectos de este Título, se entenderá por perspectiva de género la integración sistemática de medidas que permitan identificar, prevenir, corregir y eliminar desigualdades entre mujeres y hombres, así como los sesgos y estereotipos que pudieran reproducirse o amplificarse por medio de sistemas automatizados.

Artículo 86. El Estado, en el ámbito de sus atribuciones y respecto de las políticas públicas, proyectos tecnológicos, implementaciones de sistemas de inteligencia artificial y procesos de gobernanza algorítmica del sector público, garantizará que:

- I. Se evite la reproducción de estereotipos, sesgos, prejuicios o prácticas de discriminación directa o indirecta;
- II. Se promueva la representación equitativa de mujeres y de grupos históricamente discriminados en las distintas etapas del ciclo de vida de los sistemas de inteligencia artificial utilizados por las instituciones públicas;
- III. Se prevengan impactos desproporcionados o diferenciales basados en género, edad, origen étnico, discapacidad, orientación sexual, identidad de género, nivel socioeconómico, condición migratoria o cualquier otra categoría protegida; y
- IV. Se incorporen análisis y mediciones de impacto diferenciado con enfoque interseccional, cuando resulte aplicable.

Capítulo II. Prevención y Mitigación de Sesgos Algorítmicos

Artículo 87. Los desarrolladores, proveedores e implementadores de sistemas de inteligencia artificial, así como los usuarios institucionales cuando resulte aplicable, deberán identificar, evaluar, prevenir y mitigar los sesgos algorítmicos relacionados con género, racialidad, clase social, edad, discapacidad y otras formas de desigualdad estructural, particularmente en los sistemas que produzcan impactos significativos sobre derechos u oportunidades de las personas.

Artículo 88. La Evaluación de Impacto Algorítmico prevista en esta Ley deberá considerar, de manera proporcional al nivel de riesgo y al impacto del sistema, entre otros aspectos:

- I. El análisis de posibles sesgos de género y de impacto interseccional;
- II. La revisión de las bases de datos utilizadas, atendiendo a criterios de representatividad y diversidad;
- III. La identificación y adopción de medidas razonables de mitigación frente a sesgos, discriminación algorítmica o decisiones automatizadas que afecten de manera desproporcionada a mujeres u otros grupos en situación de vulnerabilidad;
- IV. La definición de criterios o procedimientos de auditoría, cuando resulte aplicable;
y
- V. La validación técnica orientada a prevenir resultados discriminatorios o excluyentes.

Artículo 89. Quedará prohibido el desarrollo, implementación o uso de sistemas de inteligencia artificial que, de manera intencional o como resultado previsible de su diseño y sin medidas razonables de mitigación, generen daños graves a los derechos humanos de mujeres, niñas o grupos en situación de vulnerabilidad, en particular aquellos que:

- a) Produzcan contenidos o decisiones que impliquen violencia digital, explotación sexual, degradación o cosificación, en contravención de la legislación aplicable;
- b) Traten datos biométricos, neuronales o datos personales sensibles sin las

salvaguardas reforzadas previstas en esta Ley y en la normativa de protección de datos personales;

c) Generen decisiones automatizadas que restrinjan de manera injustificada o discriminatoria el acceso a oportunidades económicas, educativas, laborales o de participación pública.

Capítulo III. Violencia Digital, Deepfakes y Protección Reforzada de las Mujeres

Artículo 90. Los sistemas de inteligencia artificial que, por su diseño, finalidad o uso previsible, sean utilizados para producir, difundir, amplificar o automatizar contenidos que constituyan violencia digital contra las mujeres, en los términos de la legislación aplicable, serán considerados sistemas de alto riesgo y estarán sujetos a las obligaciones reforzadas previstas en esta Ley.

Artículo 91. Se considerarán prácticas prohibidas de violencia digital mediante inteligencia artificial aquellas que, de manera intencional o como resultado previsible de su diseño, operación o falta de salvaguardas razonables, tengan por objeto o efecto causar daño grave a mujeres o niñas, en particular:

I. La generación o difusión de deepfakes o contenidos sintéticos de carácter sexual o íntimo sin el consentimiento expreso de la persona afectada, o de cualquier contenido de esta naturaleza que involucre a niñas, niños o adolescentes, en cuyo caso el consentimiento será nulo e irrelevante;

II. La manipulación de imágenes, audios o videos con la finalidad de humillar, acosar, extorsionar o ejercer violencia contra una mujer;

III. La automatización deliberada de campañas de odio, difamación, desprestigio o agresiones basadas en género; y

IV. El diseño o uso de sistemas de inteligencia artificial destinados principalmente a facilitar el ciberacoso, hostigamiento o persecución digital.

Artículo 92. La Autoridad Nacional establecerá un Protocolo Nacional de Prevención y Atención de la Violencia Digital mediante Inteligencia Artificial, con enfoque de género y de derechos humanos, que incluirá, al menos:

- a) Mecanismos accesibles de denuncia inmediata;
- b) Procedimientos de trazabilidad y, en su caso, retiro oportuno de contenidos dañinos, conforme a la legislación aplicable y respetando el debido proceso;
- c) Esquemas de cooperación y coordinación con plataformas digitales y otros intermediarios tecnológicos; y
- d) Medidas de atención y reparación integral, en los términos previstos en la legislación correspondiente.

Capítulo IV. Participación de Mujeres y Grupos Subrepresentados en el Ecosistema de IA

Artículo 93. El Estado promoverá la participación activa, sustantiva y equilibrada de mujeres en:

- I. Equipos de investigación y desarrollo;
- II. Áreas de diseño, programación, ciencia de datos, ingeniería y seguridad informática;
- III. Comités, consejos consultivos y órganos rectores del Sistema Nacional de Inteligencia Artificial;
- IV. Procesos de gobernanza, estandarización y certificación tecnológica.

Artículo 94. Los programas de formación, becas, estancias científicas, financiamiento e incentivos implementados, administrados o financiados por el Estado, en el marco de esta Ley, deberán incorporar acciones afirmativas, con el objeto de fomentar la participación de mujeres y niñas en la ciencia, la tecnología y la inteligencia artificial.

Artículo 95. La Secretaría de Ciencia, Humanidades, Tecnología e Innovación promoverá:

- a) Redes de mujeres investigadoras en IA;
- b) Mentorías y liderazgo tecnológico femenino;
- c) Formación temprana de niñas en STEM;
- d) Programas de apoyo a emprendedoras de IA.

Capítulo V. Ciberseguridad con Enfoque de Género

Artículo 96. La política nacional de ciberseguridad deberá integrar un enfoque de género y tener por objeto:

- I. Reducir vulnerabilidades específicas que enfrentan mujeres y niñas en entornos digitales;
- II. Prevenir ciberataques, extorsión, espionaje y violencias digitales con impacto diferenciado;
- III. Fortalecer medidas de seguridad digital adaptadas a riesgos de género;
- IV. Promover campañas nacionales de educación en ciberseguridad con enfoque interseccional.

Artículo 97. Las dependencias del Estado deberán capacitar a su personal en:

- a) Violencia digital contra las mujeres;
- b) Ciberseguridad con perspectiva de género;
- c) Identificación de patrones algorítmicos discriminatorios;
- d) Atención sensible a víctimas.

Capítulo VI. Inclusión Digital de Grupos en Situación de Vulnerabilidad

Artículo 98. El Estado garantizará el acceso equitativo y seguro a tecnologías de inteligencia artificial para:

- I. Mujeres y niñas, particularmente en zonas rurales e indígenas;
- II. Personas con discapacidad;
- III. Personas mayores;
- IV. Comunidades indígenas;
- V. Personas LGBTIQ+;
- VI. Personas en situación de pobreza o exclusión digital.

Artículo 99. Los programas públicos deberán incorporar accesibilidad universal, diseño inclusivo y compatibilidad con tecnologías asistivas.

Capítulo VII. Obligaciones del Estado y del Sector Privado

Artículo 100. Las instituciones públicas y las entidades privadas que, en el ámbito de sus actividades y conforme a su grado de control, desarrollen, implementen o utilicen

sistemas de inteligencia artificial de impacto significativo, deberán:

- I. Incorporar, cuando resulte aplicable, la perspectiva de género en el diseño, desarrollo o despliegue de dichos sistemas;
- II. Adoptar medidas razonables para promover la igualdad de oportunidades y prevenir prácticas discriminatorias asociadas al uso de inteligencia artificial;
- III. Establecer mecanismos para la detección, documentación y reporte de incidentes de discriminación algorítmica a la autoridad competente;
- IV. Implementar acciones de mitigación, corrección o suspensión del uso de sistemas que presenten sesgos discriminatorios, en la medida de sus atribuciones y capacidades técnicas; y
- V. Garantizar niveles adecuados de transparencia respecto del funcionamiento general de los sistemas y del uso de datos, de conformidad con la legislación aplicable y con enfoque de género.

Capítulo VIII. Transversalidad, Monitoreo y Actualización

Artículo 101. La Autoridad Nacional en Inteligencia Artificial integrará un Observatorio Nacional de Igualdad Algorítmica, con funciones de análisis y seguimiento, que:

- a) Analizará los riesgos diferenciados que los sistemas de inteligencia artificial puedan generar para mujeres y otros grupos en situación de vulnerabilidad;
- b) Identificará y emitirá alertas técnicas sobre posibles sesgos algorítmicos;
- c) Publicará informes periódicos sobre desigualdad algorítmica y sus impactos sociales; y
- d) Formulará recomendaciones y emitirá alertas tempranas en casos de alto impacto, dirigidas a las autoridades competentes.

Artículo 102. La perspectiva de género será obligatoria en:

- I. El Glosario Reglamentario;
- II. La Estrategia Nacional de Inteligencia Artificial;

- III. La actualización normativa anual;
- IV. Certificaciones.

TÍTULO OCTAVO

Fomento al Desarrollo, Innovación y Capacidades Nacionales en Inteligencia Artificial

Capítulo I. Fomento a la investigación científica y tecnológica

Artículo 103. El Estado fomentará el desarrollo científico, humanístico y tecnológico en materia de inteligencia artificial, mediante programas, políticas, incentivos y mecanismos que impulsen la investigación básica, aplicada, experimental y de frontera.

Artículo 104. Las instituciones de educación superior, centros públicos de investigación y laboratorios nacionales deberán promover proyectos interdisciplinarios de investigación en inteligencia artificial, ciencia de datos, robótica inteligente, neurotecnologías, ciberseguridad y tecnologías emergentes asociadas.

Artículo 105. La Secretaría de Ciencia, Humanidades, Tecnología e Innovación, en coordinación con la Autoridad Nacional en Inteligencia Artificial, establecerá prioridades nacionales de investigación, líneas estratégicas de desarrollo tecnológico y agendas de innovación con perspectiva de derechos humanos, ética algorítmica, seguridad digital y sostenibilidad.

Artículo 106. El Estado promoverá la consolidación de redes nacionales e internacionales de colaboración científica, cooperación académica, movilidad estudiantil y participación en consorcios globales de investigación en inteligencia artificial.

Artículo 107. Las instituciones públicas deberán privilegiar proyectos que atiendan retos nacionales en salud, educación, empleo, seguridad, movilidad, medio ambiente, justicia y productividad, así como aquellos que reduzcan brechas tecnológicas regionales.

Capítulo II. Financiamiento e incentivos fiscales

Artículo 108. El Estado establecerá mecanismos de financiamiento público, mixto y

privado para impulsar proyectos de investigación, desarrollo tecnológico, innovación y emprendimiento en inteligencia artificial.

Artículo 109. El Presupuesto de Egresos de la Federación deberá prever recursos específicos para el desarrollo y fomento del uso de la inteligencia artificial, así como para la creación y fortalecimiento de infraestructura estratégica, capacidades de supercómputo, repositorios científicos y centros de excelencia.

Artículo 110. Se podrán otorgar estímulos fiscales, deducciones, créditos, fondos de garantía y apoyos concursables a proyectos que promuevan la innovación responsable, el desarrollo tecnológico nacional y la soberanía científica en inteligencia artificial.

Artículo 111. Los mecanismos de financiamiento deberán priorizar:

- I. Proyectos de alto impacto social;
- II. Innovación orientada a sectores estratégicos;
- III. Desarrollo de talento especializado;
- IV. Investigación con aplicación industrial;
- V. Soluciones que reduzcan desigualdades tecnológicas.

Capítulo III. Ecosistema emprendedor y startups de IA

Artículo 112. El Estado impulsará el desarrollo del ecosistema emprendedor en inteligencia artificial, mediante instrumentos de financiamiento, incubación, aceleración, infraestructura tecnológica y acompañamiento técnico.

Artículo 113. La Autoridad Nacional en Inteligencia Artificial promoverá la creación de entornos de prueba, sandboxes regulatorios y laboratorios de innovación para facilitar el desarrollo seguro, controlado y ético de nuevas soluciones tecnológicas.

Artículo 114. Los emprendimientos de inteligencia artificial deberán orientarse por los principios de ética algorítmica, transparencia razonable, responsabilidad y protección de datos personales desde la etapa de diseño, sin perjuicio de la protección de secretos industriales y propiedad intelectual.

Artículo 115. El Estado fomentará la participación de emprendedores, pequeñas, medianas y grandes empresas, desarrolladores independientes y talento joven en programas de innovación, competencias tecnológicas y retos nacionales en materia de

inteligencia artificial.

Capítulo IV. Transferencia tecnológica y cooperación internacional

Artículo 116. La transferencia tecnológica en inteligencia artificial será una prioridad nacional y deberá promover la adopción de modelos, metodologías, innovaciones y buenas prácticas que fortalezcan la competitividad del país, respetando la soberanía tecnológica.

Artículo 117. Las instituciones públicas podrán celebrar acuerdos para el desarrollo conjunto de tecnologías, intercambio de conocimientos, licenciamiento, codesarrollo y copropiedad intelectual, sin perjuicio de la normatividad aplicable.

Artículo 118. La cooperación internacional deberá orientarse a:

- I. Impulsar la formación de talento;
- II. Facilitar la movilidad académica;
- III. Promover proyectos multilaterales de investigación;
- IV. Integrar a México en espacios de estandarización técnica global;
- V. Fortalecer la infraestructura científica y tecnológica del país.

Artículo 119. Los acuerdos de cooperación internacional deberán respetar la protección de datos personales, la seguridad nacional, los derechos humanos y los principios rectores establecidos en esta Ley.

Capítulo V. Fondo Nacional para el Desarrollo de la Inteligencia Artificial

Artículo 120. Se crea el Fondo Nacional para el Desarrollo de la Inteligencia Artificial, como instrumento financiero especializado destinado a apoyar la investigación, innovación y desarrollo tecnológico en materia de inteligencia artificial.

Artículo 121. El Fondo se integrará con:

- I. Recursos del Presupuesto de Egresos de la Federación;
- II. Aportaciones de dependencias y entidades públicas;
- III. Donaciones de organismos internacionales;
- IV. Aportaciones privadas nacionales y extranjeras;
- V. Ingresos derivados de proyectos tecnológicos y esquemas de innovación abierta.

Artículo 122. El Fondo priorizará proyectos que contribuyan al desarrollo científico nacional, la soberanía tecnológica, la protección de derechos humanos y la reducción de brechas digitales.

Artículo 123. El Reglamento establecerá los criterios para la operación, asignación de recursos, selección de proyectos, mecanismos de evaluación y transparencia del Fondo.

TÍTULO NOVENO

Evaluación, Clasificación y Gestión de Riesgos en Sistemas de Inteligencia Artificial

Capítulo I. Evaluación de Impacto Algorítmico

Artículo 124. Todo sistema de inteligencia artificial clasificado como de alto riesgo, así como aquel que pueda producir impactos significativos en los derechos humanos, la seguridad nacional, la salud pública, el medio ambiente, los procesos democráticos o los servicios esenciales, deberá someterse obligatoriamente a una Evaluación de Impacto Algorítmico previa a su implementación.

En ningún caso podrán implementarse ni mantenerse en operación sistemas de inteligencia artificial que produzcan efectos jurídicos o impactos significativos sobre derechos, cuando, por su diseño, complejidad, falta de documentación o contexto de uso resulte materialmente imposible explicar de manera razonable el proceso decisional.

Artículo 125. La Evaluación de Impacto Algorítmico deberá contener, al menos:

- I. Descripción técnica del sistema;
- II. Finalidad, contexto de uso y alcance funcional;
- III. Identificación de riesgos para derechos humanos, salvaguardas democráticas y seguridad pública;
- IV. Análisis de posibles sesgos, discriminación y afectaciones desproporcionadas;
- V. Evaluación de impacto en la privacidad y tratamiento de datos personales;
- VI. Medidas de mitigación, mecanismos de supervisión humana significativa y protocolos de intervención;
- VII. Mecanismos de trazabilidad, auditoría y registro de decisiones algorítmicas;

- VIII. Resultados de pruebas técnicas, validación y auditorías independientes, cuando resulte aplicable.

La evaluación de impacto algorítmico para los sistemas clasificados como de alto riesgo, sean públicos o privados, deberá realizarse con carácter previo a su puesta en operación o despliegue público, e incluir un análisis específico de las personas, comunidades, territorios y contextos que puedan verse afectados, así como de los impactos sociales, políticos, económicos, ambientales y culturales asociados.

Artículo 126. Las instituciones públicas y privadas que desarrollen, implementen o utilicen sistemas de inteligencia artificial clasificados como de alto riesgo, así como aquellos sistemas que puedan producir impactos significativos en los derechos humanos, deberán presentar la Evaluación de Impacto Algorítmico ante la autoridad competente con carácter previo a la puesta en operación del sistema. La actualización de dicha evaluación será obligatoria cuando exista una modificación sustancial del modelo, de los datos utilizados o de la finalidad del sistema.

Artículo 127. La Autoridad Nacional en Inteligencia Artificial establecerá metodologías unificadas, estándares técnicos y formatos oficiales para la elaboración y actualización de las Evaluaciones de Impacto Algorítmico.

Artículo 128. La autoridad podrá ordenar evaluaciones adicionales cuando exista riesgo inminente, denuncias fundadas, evidencia de fallas sistémicas o afectaciones a derechos humanos.

Capítulo II. Regulación de Sistemas de Inteligencia Artificial de Alto Riesgo

Artículo 129. Se consideran sistemas de inteligencia artificial de alto riesgo aquellos que, por su naturaleza, finalidad, contexto, probabilidad de uso o potencial de impacto, puedan generar daños significativos a derechos humanos, integridad física, salud, seguridad nacional, procesos democráticos, medio ambiente o servicios estratégicos.

Artículo 129 Bis.

La Autoridad Nacional establecerá, mediante disposiciones de carácter general, el procedimiento técnico-jurídico para la clasificación de los sistemas de inteligencia artificial conforme a niveles de riesgo, el cual deberá considerar, al menos:

- I. Evaluación ex ante previa a su despliegue;
- II. Evaluación periódica durante su operación;
- III. Posibilidad de reclasificación cuando cambien las condiciones de uso o impacto;
- IV. Criterios técnicos objetivos, verificables y documentables;
- V. Derecho de audiencia del desarrollador o proveedor.

Artículo 130. Los sistemas de alto riesgo estarán sujetos, de manera proporcional a su riesgo, a obligaciones reforzadas que incluirán, al menos:

- I. Gestión integral de riesgos durante todo el ciclo de vida del sistema;
- II. Pruebas técnicas y procesos de validación previos a su puesta en operación;
- III. Registro en el Registro Nacional de Sistemas de Inteligencia Artificial, en los términos que establezca esta Ley y su Reglamento;
- IV. Mecanismos de supervisión humana significativa;
- V. Requisitos de explicabilidad y trazabilidad verificables;
- VI. Auditorías periódicas, internas y, cuando resulte aplicable, externas; y
- VII. Salvaguardas técnicas y organizacionales adecuadas para prevenir, mitigar y responder a riesgos identificados.

Artículo 131. Los desarrolladores o proveedores de sistemas de inteligencia artificial clasificados como de alto riesgo deberán implementar medidas técnicas y organizacionales razonables, conforme a su grado de control, para asegurar que dichos sistemas:

- I. No operen fuera de los contextos de uso autorizados o previstos;
- II. No realicen conductas prohibidas conforme a esta Ley; y
- III. No generen decisiones automatizadas sin supervisión humana significativa cuando puedan afectarse derechos fundamentales.

Artículo 132. Los usuarios institucionales de sistemas de inteligencia artificial de alto riesgo deberán adoptar, en el ámbito de sus atribuciones, políticas de manejo ético, protocolos de ciberseguridad, mecanismos de revisión humana y registros de operación, de manera proporcional al nivel de riesgo y al impacto del sistema.

Artículo 133. El incumplimiento de las obligaciones previstas en este Capítulo será sancionado conforme al Título Décimo Cuarto de esta Ley.

Capítulo III. Certificación, Estándares y Auditorías

Artículo 134. La Autoridad Nacional en Inteligencia Artificial establecerá un Sistema Nacional de Certificación de Sistemas de Inteligencia Artificial, destinado a verificar, cuando resulte aplicable, el cumplimiento de estándares nacionales e internacionales en materia de seguridad, ética, transparencia y gobernanza.

Artículo 135. La certificación será obligatoria únicamente para:

- I. Los sistemas de inteligencia artificial clasificados como de alto riesgo, en los términos de esta Ley;
- II. Los sistemas de inteligencia artificial utilizados por autoridades públicas que, por su finalidad o contexto de uso, puedan afectar derechos fundamentales, servicios esenciales o procesos democráticos; y
- III. Los sistemas de inteligencia artificial generativa o de propósito general cuando, de manera sistemática, sean desplegados o adaptados para usos específicos que produzcan impactos significativos en derechos humanos, seguridad pública o procesos democráticos.

La determinación de que un sistema se constituya como de “alto riesgo” será emitida por la Autoridad Nacional mediante resolución debidamente fundada y motivada.

Artículo 136. La certificación de los sistemas de inteligencia artificial incluirá, de manera proporcional a su nivel de riesgo y contexto de uso, la verificación de:

- I. Conformidad técnica y funcionamiento seguro;
- II. Gestión integral de riesgos;
- III. Protección de datos personales y de la privacidad;
- IV. No discriminación y mitigación de sesgos;
- V. Transparencia y explicabilidad; y
- VI. Ciberseguridad y resiliencia.

Artículo 137. Las auditorías de los sistemas de inteligencia artificial sujetos a certificación serán proporcionales al nivel de riesgo, y podrán ser internas y, cuando resulte aplicable, externas, sin perjuicio de la protección de los derechos de propiedad intelectual, secretos industriales y confidencialidad comercial. Dichas auditorías deberán:

- I. Identificar desviaciones, vulnerabilidades y riesgos emergentes;
- II. Verificar el cumplimiento de estándares técnicos aplicables;
- III. Evaluar el desempeño y la eficacia del sistema en su contexto real de operación; y
- IV. Proponer medidas de mejora continua.

Artículo 138. Los desarrolladores o proveedores de sistemas de inteligencia artificial sujetos a certificación deberán conservar la evidencia técnica, los informes de auditoría y las bitácoras de funcionamiento durante los plazos y en los términos que establezca el Reglamento, a efecto de permitir su verificación por la autoridad competente.

Capítulo IV. Supervisión Continua y Actualización Normativa

Artículo 139. La Autoridad Nacional en Inteligencia Artificial ejercerá funciones de supervisión únicamente respecto de los sistemas de inteligencia artificial clasificados como de alto riesgo, de conformidad con esta Ley, de manera proporcional, justificada y basada en riesgo.

Artículo 140. La supervisión de los sistemas de inteligencia artificial de alto riesgo podrá comprender, cuando resulte necesario y conforme a los procedimientos previstos en esta Ley y su Reglamento:

- I. Monitoreo del funcionamiento del sistema, preferentemente mediante reportes, métricas o mecanismos indirectos, y de forma excepcional en tiempo real cuando sea técnicamente indispensable;
- II. Verificación del cumplimiento de las disposiciones normativas aplicables;
- III. Solicitud fundada y motivada de información técnica relevante;
- IV. Visitas de inspección previa orden debidamente fundada y motivada, en los términos de la legislación aplicable; y
- V. Evaluación de riesgos emergentes asociados al uso del sistema.

Artículo 141. La Autoridad Nacional en Inteligencia Artificial podrá ordenar, mediante resolución debidamente fundada y motivada, la suspensión temporal y, de manera excepcional, la suspensión definitiva del uso de sistemas de inteligencia artificial clasificados como de alto riesgo, cuando:

- I. Representen un riesgo grave e inminente para la integridad física, los derechos humanos o la seguridad pública;

- II. Incurran en un incumplimiento grave o reiterado de las obligaciones de certificación obligatoria previstas en esta Ley; o
- III. Se acrediten fallas técnicas sustanciales que comprometan la validez, confiabilidad o seguridad del sistema.

En todos los casos deberá garantizarse el derecho de audiencia y la aplicación de medidas proporcionales al nivel de riesgo identificado.

Artículo 142. El Estado promoverá la actualización periódica y técnica de los marcos metodológicos, estándares, lineamientos y herramientas aplicables a la inteligencia artificial, a través de:

- I. La revisión y, en su caso, actualización del Glosario Reglamentario;
- II. La adopción o referencia a estándares internacionales pertinentes;
- III. Mecanismos de cooperación técnica y científica nacional e internacional; y
- IV. Procesos de participación multisectorial para la mejora continua del marco técnico y normativo.

Artículo 143. La Autoridad Nacional en Inteligencia Artificial deberá presentar un informe anual de carácter público sobre las actividades de supervisión realizadas, los riesgos emergentes identificados, las certificaciones emitidas, las sanciones aplicadas y una evaluación general del estado del ecosistema de inteligencia artificial en el país.

TÍTULO DÉCIMO

De las Aplicaciones Prohibidas y de Alto Riesgo de la Inteligencia Artificial

Capítulo I. De las Aplicaciones Prohibidas de la Inteligencia Artificial

Artículo 144. Queda prohibido en el territorio nacional el desarrollo, comercialización, implementación, utilización o puesta en operación de sistemas de inteligencia artificial que, por su diseño, finalidad intrínseca y uso previsible, y previa determinación fundada y motivada de la Autoridad Nacional en Inteligencia Artificial, representen una amenaza grave, irreversible e incompatible con un Estado democrático de derecho para los derechos humanos, la dignidad humana, la autonomía individual, la integridad cognitiva, la seguridad nacional o la estabilidad democrática. La prohibición prevista en este artículo tendrá carácter excepcional y se aplicará únicamente cuando los riesgos identificados no puedan ser razonablemente mitigados mediante medidas técnicas, organizacionales o regulatorias.

Artículo 145. Para efectos de esta Ley, se consideran aplicaciones prohibidas de la inteligencia artificial, por constituir riesgos inaceptables y no razonablemente mitigables, entre otras, las siguientes:

- I. Sistemas de manipulación cognitiva o conductual dirigidos a influir, alterar o condicionar procesos mentales sin el consentimiento previo, libre, específico e informado de la persona, o en cualquier caso cuando

- involucren a niñas, niños o adolescentes, respecto de los cuales el consentimiento será nulo e irrelevante;
- II. Sistemas de puntuación social, utilizados por autoridades públicas o por particulares, que evalúen de manera integral el comportamiento, la reputación o las características personales de las personas y produzcan efectos discriminatorios, de exclusión o afectaciones significativas a sus derechos;
 - III. Sistemas de identificación biométrica masiva en tiempo real en espacios públicos, salvo cuando exista orden judicial, fundamento legal expreso y garantías equivalentes de necesidad, proporcionalidad y control democrático;
 - IV. Sistemas de vigilancia masiva que permitan el seguimiento, monitoreo o análisis conductual de personas o colectivos sin base legal suficiente, sin proporcionalidad y sin control judicial efectivo;
 - V. Sistemas de inteligencia artificial destinados al reconocimiento de emociones o estados mentales utilizados con fines laborales, educativos, migratorios, policiales o de selección de personal, cuando generen discriminación, afecten la autonomía individual o carezcan de base científica verificable;
 - VI. Sistemas de inteligencia artificial utilizados para la toma de decisiones letales autónomas, sin supervisión humana significativa y fuera de un marco normativo específico aplicable al uso legítimo de la fuerza;
 - VII. Sistemas que generen o difundan deepfakes o contenidos sintéticos engañosos con fines de fraude, extorsión, manipulación política, desinformación electoral, violencia de género, acoso, difamación o afectaciones graves a la seguridad pública;
 - VIII. Sistemas de inteligencia artificial diseñados para explotar deliberadamente las vulnerabilidades de grupos en situación de riesgo o discriminación estructural, como niñas, niños y adolescentes, personas mayores, personas con discapacidad, personas pertenecientes a la diversidad sexual y de género, o pueblos y comunidades indígenas; y
 - IX. Cualesquiera otros sistemas que, previa determinación fundada y motivada de la Autoridad Nacional en Inteligencia Artificial, y mediante lineamientos de carácter general, públicos y sujetos a control, representen riesgos inaceptables que no puedan ser razonablemente mitigados conforme a esta Ley.

Artículo 146. La autoridad competente podrá ordenar, mediante resolución debidamente fundada y motivada, el retiro del mercado, la suspensión temporal o definitiva de la operación, la desconexión técnica o la prohibición de uso de los sistemas de inteligencia artificial comprendidos en este Capítulo, cuando resulte estrictamente necesario para prevenir un riesgo grave e inminente y de manera proporcional al nivel de afectación identificado, garantizando en todo momento el derecho de audiencia y el debido proceso, sin perjuicio de las sanciones previstas en esta Ley.

Capítulo II. De los Sistemas de Alto Riesgo

Artículo 147. Se considerarán sistemas de inteligencia artificial de alto riesgo, cuando por su finalidad, contexto de uso o potencial de impacto puedan generar afectaciones significativas, entre otros, los siguientes:

- I. Sistemas utilizados en el ámbito de la salud, incluidos diagnósticos asistidos, terapias inteligentes y dispositivos médicos que incorporen inteligencia artificial;
- II. Sistemas empleados en procesos judiciales, de procuración de justicia o de seguridad pública;
- III. Sistemas destinados a la gestión u operación de infraestructura crítica, como energía, agua, transporte y telecomunicaciones;
- IV. Sistemas utilizados en procesos electorales o destinados a influir de manera significativa en la formación de la opinión pública, fuera de actividades legítimas de información, investigación o expresión;
- V. Sistemas destinados a evaluación educativa, acreditación o certificación automatizada;
- VI. Sistemas utilizados en relaciones laborales, incluidos evaluación de desempeño, selección de personal o procesos de terminación laboral automatizados;
- VII. Sistemas relacionados con la evaluación de crédito, scoring financiero o seguros;
- VIII. Sistemas utilizados para la gestión ambiental o la predicción de riesgos climáticos cuando sus resultados incidan en decisiones públicas o privadas de alto impacto; y
- IX. Sistemas que procesen datos biométricos, genéticos, neuronales o datos personales sensibles, cuando de ello se deriven impactos significativos en los derechos de las personas.

Artículo 148. La Autoridad Nacional en Inteligencia Artificial podrá actualizar el listado de sistemas de alto riesgo mediante disposiciones de carácter general, atendiendo a la evolución tecnológica, evidencia científica y estándares internacionales.

Capítulo III. Del Control, Mitigación y Gestión de Riesgos

Artículo 149. Todos los sistemas de inteligencia artificial de alto riesgo deberán contar con mecanismos de identificación, análisis, mitigación y monitoreo continuo de riesgos, en función de su naturaleza, diseño y nivel de impacto.

Artículo 150. Los sujetos regulados deberán implementar, en el ámbito de su organización y conforme a su tamaño, naturaleza y rol, un Sistema Integral de Gestión de Riesgos Algorítmicos, basado en los lineamientos generales que emita la Autoridad Nacional, el cual incluirá, al menos:

- I. Identificación temprana de riesgos técnicos, éticos, sociales, ambientales y de derechos humanos;
- II. Evaluación de impactos antes, durante y después de la operación del sistema;
- III. Protocolos de mitigación continua y medidas de corrección inmediata;
- IV. Procedimientos de auditoría interna y, cuando resulte aplicable, externa; y
- V. Mecanismos de reporte a la Autoridad Nacional sobre fallas críticas, incidentes relevantes o violaciones a esta Ley, en los términos que establezcan esta Ley y su Reglamento.

Artículo 151. Los sistemas de inteligencia artificial clasificados como de alto riesgo deberán incorporar, de manera proporcional a su naturaleza, finalidad y contexto de uso, además de las obligaciones previstas en esta Ley:

- I. Mecanismos técnicos de intervención, detención segura (“botón de apagado” o *stop override*) o limitación del funcionamiento del sistema, cuando resulte aplicable;
- II. Mecanismos de supervisión humana significativa, robusta y verificable;
- III. Evidencia documentada y trazable de las decisiones automatizadas o asistidas, en la medida necesaria para su revisión y auditoría; y
- IV. Evaluaciones periódicas del desempeño, la confiabilidad y la robustez técnica del sistema.

Artículo 152. La responsabilidad por el cumplimiento de las obligaciones previstas en

los Títulos Noveno y Décimo se determinará conforme al rol desempeñado por cada actor en el ciclo de vida del sistema de inteligencia artificial y a su grado de control efectivo sobre el diseño, desarrollo, implementación, operación o distribución del sistema. En ningún caso se impondrá responsabilidad objetiva por el solo hecho de participar en la cadena de valor, sin perjuicio de las responsabilidades civiles, administrativas o penales que correspondan por dolo, negligencia grave o incumplimiento de obligaciones específicas previstas en esta Ley.

TÍTULO DÉCIMO PRIMERO

Derechos y Obligaciones de Desarrolladores, Operadores, Proveedores y Usuarios

Capítulo I. Derechos de los usuarios frente a la IA

Artículo 153. Toda persona tendrá derecho a recibir información clara, accesible, verificable y oportuna sobre el uso de sistemas de inteligencia artificial cuando estos incidan de manera significativa en sus derechos, intereses legítimos o condiciones de acceso a bienes, servicios o decisiones públicas o privadas.

Artículo 154. Toda persona tendrá derecho a ser notificada de forma expresa cuando una decisión, recomendación, evaluación, clasificación o proceso que le afecte de manera directa haya sido asistido, total o parcialmente, por un sistema de inteligencia artificial, así como a conocer el grado de intervención humana en dicho proceso.

Artículo 155. Toda persona tendrá derecho a solicitar y obtener explicaciones claras, comprensibles y significativas, en lenguaje accesible, sobre la intervención de un sistema de inteligencia artificial en una decisión que le afecte de manera directa, sin que ello implique la revelación de secretos industriales, información confidencial o datos personales de terceros. Dichas explicaciones deberán incluir, al menos:

- I. Las razones principales que influyeron en la decisión, recomendación o resultado;
- II. La lógica general de funcionamiento del sistema o modelo utilizado;
- III. Las categorías de datos relevantes consideradas para la decisión;
- IV. Las medidas técnicas y organizativas adoptadas para prevenir, detectar y mitigar sesgos, errores o resultados discriminatorios.

Artículo 156. Toda persona tendrá derecho a impugnar decisiones automatizadas o semiautomatizadas que afecten sus derechos, intereses legítimos o condiciones de acceso a bienes, servicios o beneficios, así como a solicitar una revisión humana significativa por parte del responsable del sistema de inteligencia artificial. La revisión humana deberá ser realizada por una persona competente, imparcial y con facultades para confirmar, modificar o revocar la decisión, y no podrá consistir en una validación meramente formal o automática del resultado generado por el sistema.

Artículo 157. Toda persona tendrá derecho a la protección de sus datos personales, incluidos aquellos datos inferidos, derivados o generados mediante el uso de sistemas de inteligencia artificial, así como a ejercer los derechos de acceso, rectificación, oposición, supresión y portabilidad, conforme a la legislación aplicable en materia de protección de datos personales.

Artículo 158. Toda persona tendrá derecho a ser protegida contra prácticas discriminatorias, sesgos algorítmicos injustificados, vigilancia masiva no autorizada y cualquier uso de sistemas de inteligencia artificial que vulnere la dignidad humana, la integridad personal o los derechos fundamentales.

Artículo 159. Toda persona tendrá derecho a solicitar ante la autoridad competente la suspensión, total o parcial, del uso de un sistema de inteligencia artificial cuando existan indicios razonables de que su operación genera o puede generar daños o riesgos significativos para los derechos humanos, la seguridad, la salud, el medio ambiente o el orden democrático. La solicitud de suspensión no tendrá efectos automáticos y deberá ser resuelta conforme a los procedimientos y plazos establecidos por la legislación aplicable, sin perjuicio de las facultades preventivas, correctivas o sancionadoras de la autoridad competente.

Capítulo II. Obligaciones de proveedores y desarrolladores

Artículo 160. Las personas físicas o morales que desarrollen, implementen, comercialicen, operen o administren sistemas de inteligencia artificial serán responsables, en el ámbito de sus competencias y grado de control, de asegurar que el diseño, funcionamiento y uso de dichos sistemas cumplan con los principios previstos en esta Ley, así como con los estándares técnicos, normativos y de buenas prácticas aplicables, nacionales o internacionales, reconocidos por la autoridad competente.

Artículo 160 Bis. La existencia de sistemas de inteligencia artificial, incluidos aquellos con altos niveles de autonomía, no exime ni atenúa la responsabilidad humana, institucional o jurídica de las personas físicas o morales a las que hace mención el artículo anterior.

Artículo 161. Los proveedores y desarrolladores de sistemas de inteligencia artificial estarán obligados, en el ámbito de sus respectivas funciones, competencias y grado de control sobre el sistema, a:

- I. Realizar evaluaciones de impacto algorítmico cuando diseñen, entrenen o implementen sistemas clasificados como de alto riesgo;
- II. Incorporar medidas de seguridad desde el diseño y por defecto, cuando tengan control sobre la arquitectura, configuración o despliegue del sistema;
- III. Documentar el ciclo de vida del sistema en las fases bajo su responsabilidad, y conservar la trazabilidad técnica correspondiente;
- IV. Implementar medidas razonables y proporcionales para la prevención, detección y mitigación de sesgos o prácticas discriminatorias;
- V. Facilitar mecanismos de supervisión humana significativa, cuando el sistema sea utilizado para apoyar o adoptar decisiones que afecten derechos.

Artículo 162. Los desarrolladores, proveedores, integradores u operadores de sistemas de inteligencia artificial deberán proporcionar a las autoridades competentes, a solicitud fundada y motivada, la información técnica, documental o funcional necesaria y proporcional para la verificación, auditoría, certificación, supervisión o revisión de dichos sistemas, considerando el nivel de riesgo del sistema y el grado de control del sujeto obligado. La información requerida no se entregará de manera automática, ni podrá exceder lo estrictamente necesario para el cumplimiento de las funciones de la autoridad, y no implicará la revelación de secretos industriales, información confidencial ni datos personales de terceros, salvo en los casos y bajo las salvaguardas previstas por la ley.

Artículo 163. Toda persona responsable de sistemas de inteligencia artificial deberá implementar, en el ámbito de su grado de control, mecanismos de transparencia razonables y técnicamente viables que permitan a las personas identificar cuando un contenido, interacción o decisión haya sido generada o asistida, total o parcialmente, mediante inteligencia artificial. En particular, las personas tendrán derecho a ser informadas de manera clara y accesible cuando interactúen con un sistema de inteligencia artificial o *bot*, salvo en los casos expresamente previstos por la ley.

Artículo 164. Los desarrolladores y proveedores de sistemas de inteligencia artificial de propósito general o generativa (GPAI), incluidos los modelos fundacionales, deberán implementar, en el ámbito de sus respectivas funciones y grado de control, medidas técnicas y organizativas adecuadas para prevenir, detectar y mitigar:

- I. La manipulación informativa;
- II. La desinformación automatizada;
- III. La generación de contenidos ilícitos;
- IV. La suplantación de identidad o el fraude digital.

Artículo 165. Cuando un sistema de inteligencia artificial sea utilizado para fines gubernamentales o de interés público, los desarrolladores, proveedores u operadores, en el ámbito de sus respectivas funciones y grado de control, deberán garantizar su compatibilidad con estándares reforzados de transparencia, supervisión pública y rendición de cuentas, incluyendo mecanismos de auditoría técnica, funcional o documental, cuando así lo determine la autoridad competente. La auditoría no implicará necesariamente la revelación del código fuente, salvo en los casos, condiciones y con las salvaguardas que establezca la legislación aplicable.

Capítulo III. Responsabilidad civil, administrativa y penal

Artículo 166. La responsabilidad por los daños derivados del uso, operación, implementación o falla de sistemas de inteligencia artificial será objetiva, en el ámbito del grado de control y beneficio obtenido, cuando se trate de:

- I. Sistemas clasificados como de alto riesgo conforme a esta Ley;
- II. Sistemas utilizados por autoridades públicas o en el ejercicio de funciones de interés público;

- III. Sistemas que, por su naturaleza o forma de uso, puedan causar daños significativos a la vida, integridad personal, salud, patrimonio, derechos digitales o la estabilidad social.

Artículo 167. Los desarrolladores, proveedores, operadores y usuarios que intervengan de manera relevante en el ciclo de vida de un sistema de inteligencia artificial podrán ser solidariamente responsables, en el ámbito de su grado de control e intervención, cuando:

- I. Exista incumplimiento de las obligaciones de seguridad, transparencia o mitigación de riesgos previstas en esta Ley;
- II. Se actúe con dolo, negligencia grave o abuso en el diseño, implementación, operación o uso del sistema;
- III. Se omita informar vulnerabilidades relevantes, fallas críticas o riesgos conocidos, o se manipule deliberadamente el sistema de inteligencia artificial.

Artículo 168. La responsabilidad administrativa se determinará conforme a lo previsto en esta Ley, su Reglamento y la legislación aplicable en materia de responsabilidades de servidores públicos, entidades paraestatales y particulares vinculados con el sector público.

Artículo 169. Las conductas dolosas o gravemente negligentes, realizadas mediante el uso de sistemas de inteligencia artificial, que generen daños graves a la integridad de las personas, afecten infraestructura crítica, vulneren datos personales sensibles, manipulen procesos democráticos o pongan en riesgo la seguridad nacional, serán sancionadas conforme al Código Penal Federal y demás disposiciones aplicables.

Artículo 170. La autoridad competente deberá establecer criterios técnicos, públicos y verificables para determinar la causalidad, el nexo funcional y la atribución de responsabilidad cuando una decisión automatizada o asistida por sistemas de inteligencia artificial haya contribuido de manera significativa o determinante a la producción de un daño.

TÍTULO DÉCIMO SEGUNDO

Transparencia, Rendición de Cuentas y Datos Abiertos

Capítulo I. Registro Nacional de Sistemas de IA

Artículo 171. Se crea el Registro Nacional de Sistemas de Inteligencia Artificial, como un instrumento administrativo de carácter público, gratuito, en línea, de fácil acceso y uso simplificado, administrado por la Autoridad Nacional en Inteligencia Artificial, con el objeto de contar con un padrón básico de referencia y contacto de los sistemas y plataformas de inteligencia artificial que operen en el territorio nacional. El Registro tendrá una finalidad informativa, estadística y de coordinación, y no constituirá por sí mismo un mecanismo de autorización, certificación, evaluación de riesgos ni supervisión sancionatoria.

Artículo 172. El Registro Nacional de Sistemas de Inteligencia Artificial deberá contener información general y mínima, suficiente para identificar y contactar a los responsables del sistema, que incluirá, al menos:

- I. Identificación y datos de contacto del desarrollador, proveedor, operador o responsable del sistema en México, según corresponda;
- II. Denominación comercial o técnica del sistema o plataforma de inteligencia artificial;
- III. Descripción general de su finalidad y ámbito de aplicación;
- IV. Sector o sectores en los que se utiliza el sistema;
- V. Modalidad de operación del sistema (por ejemplo, uso público, privado, institucional o mixto); y
- VI. Medio de contacto designado para efectos de coordinación con la Autoridad Nacional.

La información solicitada deberá ser proporcionada de manera declarativa, sin requerimientos técnicos complejos ni entrega de documentación sensible.

Artículo 173. Los desarrolladores, proveedores u operadores de sistemas o plataformas de inteligencia artificial que ofrezcan, desplieguen o utilicen dichos sistemas en el territorio nacional deberán realizar su inscripción en el Registro Nacional de Sistemas de Inteligencia Artificial de manera sencilla y previa o posterior a su puesta en operación, conforme a los lineamientos que emita la Autoridad Nacional. La inscripción en el Registro no generará obligaciones adicionales a las previstas expresamente en esta Ley.

Artículo 174. Las actualizaciones al Registro deberán realizarse únicamente cuando exista un cambio relevante en la información de identificación o contacto, o cuando se modifique de manera general la finalidad o el ámbito de aplicación del sistema. La Autoridad Nacional procurará que los procesos de actualización sean ágiles, digitales y no onerosos.

Artículo 175. El Registro tendrá carácter público, sin perjuicio de que se reserve o clasifique, en su caso, la información protegida por la legislación aplicable en materia de datos personales, seguridad nacional, secretos industriales o derechos de propiedad intelectual. En ningún caso el Registro podrá requerir la divulgación de código fuente, modelos propietarios, bases de datos, algoritmos específicos ni información estratégica.

Capítulo II. Publicidad de algoritmos y decisiones automatizadas

Artículo 176. Las instituciones públicas que utilicen sistemas de inteligencia artificial en procedimientos administrativos, servicios públicos, funciones sustantivas o decisiones

que produzcan efectos jurídicos o afecten derechos, deberán publicar información general, clara y accesible sobre el funcionamiento del sistema, conforme a los principios de transparencia razonable. La obligación de publicidad no implicará la divulgación de código fuente, modelos propietarios ni información cuya revelación esté expresamente prohibida por la ley en materia de seguridad nacional, datos personales o derechos de propiedad intelectual.

Artículo 177. La información pública a que se refiere el artículo anterior comprenderá, de manera proporcional a la naturaleza y nivel de impacto del sistema, al menos:

- I. La finalidad y los objetivos del sistema;
- II. Una descripción de la lógica general de funcionamiento del modelo, en términos comprensibles para el público no especializado;
- III. Los tipos y categorías generales de datos empleados;
- IV. Los principales factores o variables consideradas en la toma de decisiones;
- V. Las medidas implementadas para prevenir sesgos, discriminación o afectaciones desproporcionadas;
- VI. La existencia de evaluaciones, revisiones o auditorías realizadas; y
- VII. Los mecanismos de supervisión humana, así como las vías administrativas o jurisdiccionales de revisión e impugnación disponibles.

Artículo 178. Cuando un sistema de inteligencia artificial forme parte de procesos administrativos del sector público que involucren derechos sociales, económicos, políticos, educativos, de salud o de acceso a la justicia, la autoridad competente deberá poner a disposición del público, de manera proporcional y razonable, versiones explicables, descripciones funcionales o representaciones generales del sistema, que permitan evaluar su integridad, confiabilidad y adecuación al fin público, sin implicar la divulgación de código fuente, modelos propietarios ni información protegida por la ley.

Artículo 179. La Autoridad Nacional solo de manera excepcional y mediante resolución debidamente fundada y motivada, cuando no existan medios alternativos menos intrusivos, podrá requerir el acceso limitado y proporcional a código fuente, modelos, pesos, documentación técnica o bitácoras de sistemas de inteligencia artificial, exclusivamente cuando:

- I. Existan indicios claros, verificables y documentados de afectaciones graves a derechos humanos;
- II. Se investiguen incidentes críticos que hayan producido o puedan producir daños significativos; o
- III. Sea estrictamente necesario para la verificación del cumplimiento de medidas correctivas previamente ordenadas respecto de sistemas utilizados por autoridades públicas.

En todos los casos, el requerimiento deberá especificar el alcance, finalidad y temporalidad del acceso, y limitarse únicamente a la información indispensable para el fin perseguido.

Artículo 180. El acceso a elementos protegidos por derechos de propiedad intelectual o secretos industriales solo podrá concederse a la Autoridad Nacional, bajo protocolos estrictos de confidencialidad, seguridad de la información y uso limitado, sin transferencia de titularidad ni divulgación a terceros. Dicho acceso solo procederá como medida de última ratio, cuando resulte indispensable para prevenir o remediar un riesgo grave e inminente a derechos humanos o a la seguridad nacional, y siempre que la medida sea proporcional y temporal, conforme a lo previsto en esta Ley y su Reglamento.

Capítulo III. Acceso ciudadano a información y mecanismos de rendición de cuentas

Artículo 181. El Estado garantizará el derecho de toda persona a acceder a información verificable, oportuna y comprensible relativa al uso de sistemas de inteligencia artificial por parte de autoridades públicas o de entidades que ejerzan funciones de interés público, en el ámbito de sus competencias.

Artículo 182. La Autoridad Nacional deberá habilitar mecanismos razonables y accesibles de participación ciudadana, que podrán incluir, entre otros:

- I. Plataformas de consulta pública sobre políticas, lineamientos y usos relevantes de la inteligencia artificial en el sector público;
- II. Observatorios ciudadanos o instancias de seguimiento con participación multisectorial;

- III. Reportes accesibles sobre el uso de sistemas de inteligencia artificial por parte de autoridades públicas;
- IV. Herramientas informativas para facilitar la identificación o verificación de contenidos generados o asistidos por inteligencia artificial, cuando resulte técnica y jurídicamente viable; y
- V. Procedimientos para solicitar intervención humana o revisión administrativa en los casos de decisiones automatizadas que produzcan efectos jurídicos o afecten derechos.

Artículo 183. Toda persona tendrá derecho a solicitar la revisión de decisiones automatizadas o semiautomatizadas que produzcan efectos jurídicos o impactos significativos sobre sus derechos o intereses, cuando dichas decisiones sean adoptadas por autoridades públicas o por entidades que ejerzan funciones de interés público. En estos casos, las autoridades deberán proporcionar información suficiente y comprensible para conocer las razones generales de la decisión, y ofrecer un mecanismo de revisión humana significativa, conforme a los procedimientos previstos en esta Ley y demás disposiciones aplicables.

Artículo 184. La Autoridad Nacional publicará anualmente un Informe de Transparencia en Inteligencia Artificial, que tendrá por objeto informar a la sociedad sobre el estado general del ecosistema de inteligencia artificial en el país y el ejercicio de las atribuciones previstas en esta Ley. Dicho informe deberá incluir, al menos:

- I. Información agregada y actualizada del Registro Nacional de Sistemas de Inteligencia Artificial;
- II. Resultados generales de auditorías, certificaciones o evaluaciones realizadas, en términos estadísticos y no individualizados, salvo disposición legal en contrario;
- III. Incidentes relevantes, fallas críticas y medidas generales adoptadas;
- IV. Casos identificados de aplicaciones prohibidas, en forma anonimizada o agregada;
- V. Recomendaciones, criterios y medidas correctivas emitidas por la Autoridad Nacional;
- VI. Identificación de riesgos emergentes y tendencias relevantes; y
- VII. Información estadística de interés público en la materia.

Artículo 185. Las autoridades públicas deberán contar con mecanismos razonables y

proporcionales de rendición de cuentas respecto del uso de sistemas de inteligencia artificial, que podrán incluir, según corresponda:

- I. Auditorías internas y, cuando resulte aplicable, externas;
- II. Paneles o instancias de asesoría técnica y experta;
- III. Esquemas de monitoreo y evaluación pública basados en información agregada y no sensible; y
- IV. Mecanismos de participación multisectorial en la evaluación de políticas y usos relevantes de la inteligencia artificial.

Artículo 186. Los mecanismos de transparencia y rendición de cuentas establecidos en este Título serán obligatorios para las instituciones públicas. Tratándose de particulares, dichos mecanismos serán exigibles únicamente en la medida en que utilicen sistemas de inteligencia artificial en actividades de interés público, servicios esenciales o sectores regulados, de forma proporcional a su rol, nivel de impacto y conforme a lo expresamente previsto en esta Ley, sin generar obligaciones adicionales distintas a las aquí establecidas.

TÍTULO DÉCIMO TERCERO

Procedimientos Administrativos en Materia de Inteligencia Artificial

Capítulo I. Sistema Nacional de Certificación en Inteligencia Artificial

Artículo 187. Se crea el Sistema Nacional de Certificación en Inteligencia Artificial, como un mecanismo técnico, voluntario y no punitivo, orientado a promover la adopción de buenas prácticas, el cumplimiento de estándares de calidad, seguridad, ética y gobernanza, así como a fortalecer la confianza de usuarios, consumidores y autoridades en el uso de sistemas de inteligencia artificial. La certificación tendrá carácter de distintivo público de calidad y cumplimiento, y no constituirá, por sí misma, un requisito de autorización general para la operación de sistemas de inteligencia artificial.

Artículo 188. La certificación de sistemas de inteligencia artificial será:

- I. Obligatoria, únicamente para los sistemas clasificados como de alto riesgo, en los términos previstos por esta Ley; y
- II. Voluntaria, para los demás sistemas de inteligencia artificial, como instrumento de mejora continua, diferenciación reputacional y fortalecimiento de la confianza pública.

Artículo 189. La certificación voluntaria permitirá a desarrolladores, proveedores y operadores:

- I. Acreditar el cumplimiento de estándares técnicos y mejores prácticas en materia de inteligencia artificial;
- II. Demostrar compromiso con principios de ética, transparencia, seguridad y protección de derechos;
- III. Facilitar la confianza de usuarios, consumidores, inversionistas y autoridades; y
- IV. Mantener procesos de actualización periódica conforme a la evolución tecnológica y regulatoria.

Artículo 190. La Autoridad Nacional en Inteligencia Artificial emitirá, mediante lineamientos de carácter general, los criterios, niveles, modalidades y vigencia de las certificaciones, asegurando que:

- I. Sean proporcionales al nivel de riesgo y contexto de uso del sistema;
- II. Se basen en estándares internacionales y mejores prácticas reconocidas;
- III. No impliquen la divulgación de información protegida por derechos de propiedad intelectual, secretos industriales o datos personales; y
- IV. No generen obligaciones o sanciones distintas a las expresamente previstas en esta Ley.

Capítulo II. Auditorías y Supervisión Proporcional

Artículo 191. La Autoridad Nacional en Inteligencia Artificial podrá realizar auditorías técnicas, operativas o documentales, exclusivamente respecto de:

- I. Sistemas de inteligencia artificial clasificados como de alto riesgo; o
- II. Sistemas utilizados por autoridades públicas cuando produzcan efectos jurídicos o impactos significativos sobre derechos o servicios esenciales.

Las auditorías deberán ser excepcionales, proporcionales y debidamente fundadas y motivadas.

Artículo 192. Las auditorías solo podrán realizarse cuando:

- I. Formen parte de un procedimiento de certificación obligatoria o voluntaria, exclusivamente para efectos de verificación técnica del cumplimiento de los criterios de certificación solicitada;
- II. Se deriven de incidentes críticos, denuncias fundadas o riesgos graves debidamente documentados; o
- III. Tengan por objeto verificar el cumplimiento de medidas correctivas previamente ordenadas.

Artículo 193. Tratándose de sistemas de inteligencia artificial que no estén clasificados como de alto riesgo, la certificación voluntaria se basará en mecanismos proporcionales, declarativos y no intrusivos, orientados a acreditar buenas prácticas y procesos de gobernanza, sin implicar auditorías técnicas profundas ni acceso a información protegida, ni generar facultades adicionales de supervisión o sanción. Tratándose de sistemas de alto riesgo, la certificación podrá incluir auditorías técnicas y verificaciones reforzadas, conforme a lo previsto en esta Ley.

Artículo 194. El acceso a información técnica, documentación o registros deberá limitarse estrictamente a lo necesario para el fin de la auditoría, sin implicar la divulgación de código fuente, modelos propietarios o secretos industriales, salvo en los casos excepcionales previstos expresamente en esta Ley.

Artículo 195. La obstrucción deliberada de una auditoría legalmente ordenada o la alteración dolosa de información relevante será considerada infracción, en los términos previstos por esta Ley.

Artículo 196. Como parte de los procedimientos de auditoría previstos en este Capítulo, la Autoridad Nacional en Inteligencia Artificial podrá ordenar visitas de verificación, únicamente mediante resolución fundada y motivada, cuando resulten indispensables para constatar el funcionamiento real de sistemas de alto riesgo o de uso público sensible.

Artículo 197. Como resultado de las auditorías, la Autoridad Nacional podrá emitir:

- I. Recomendaciones no vinculantes;
- II. Medidas correctivas proporcionales; y
- III. En su caso, las medidas previstas en los artículos relativos a suspensión o retiro del sistema, conforme al procedimiento y garantías establecidos en esta Ley.

Capítulo III. Estándares técnicos

Artículo 198. La implementación de las obligaciones previstas en esta Ley se apoyará en estándares técnicos sectoriales, de carácter especializado, flexible y actualizado, que tendrán por objeto establecer criterios operativos y buenas prácticas para el desarrollo, despliegue y uso de sistemas de inteligencia artificial en sectores específicos. Dichos estándares se definirán en el Reglamento de esta Ley, y deberán:

- I. Atender a las particularidades de cada sector, incluyendo, entre otros, los ámbitos de salud, educación, seguridad, justicia, finanzas, medio ambiente e infraestructura crítica;
- II. Ser proporcionales al nivel de riesgo, impacto y contexto de uso de los sistemas de inteligencia artificial;
- III. Basarse en estándares internacionales, evidencia científica y mejores prácticas reconocidas; y
- IV. Respetar los principios, derechos y garantías establecidos en esta Ley, sin crear obligaciones adicionales ni sanciones no previstas expresamente.

La adopción de estándares técnicos sectoriales no implicará la divulgación de información protegida por derechos de propiedad intelectual, secretos industriales o datos personales, ni podrá utilizarse como requisito de autorización previa, salvo en los casos expresamente previstos por la Ley.

Artículo 199. Los estándares técnicos sectoriales a que se refiere esta Ley serán obligatorios únicamente para los sistemas de inteligencia artificial clasificados como de alto riesgo, así como para aquellos utilizados por autoridades públicas cuando produzcan efectos jurídicos o impactos significativos sobre derechos o servicios esenciales. Tratándose de sistemas de inteligencia artificial de riesgo medio o bajo, los estándares técnicos tendrán carácter referencial o de buenas prácticas, sin perjuicio de las obligaciones expresamente previstas en esta Ley. En todos los casos, los estándares técnicos deberán aplicarse de manera proporcional al contexto, finalidad y nivel de

riesgo del sistema, y no podrán utilizarse para imponer requisitos técnicos, autorizaciones previas o sanciones no previstas expresamente en esta Ley.

Capítulo IV. Procedimientos de queja, reparación y atención a usuarios afectados

Artículo 200. Toda persona podrá presentar quejas ante la Autoridad Nacional cuando considere que un sistema de inteligencia artificial ha vulnerado sus derechos, generado daños, actuado de manera sesgada, discriminatoria o riesgosa, o incumple las disposiciones de esta Ley.

Artículo 201. Las quejas podrán presentarse mediante medios digitales, escritos, plataformas públicas, ventanillas especializadas o cualquier mecanismo que determine la Autoridad Nacional.

Artículo 202. Recibida la queja, la Autoridad Nacional iniciará un procedimiento para:

- I. Admitir o desechar la queja y justificar ante la persona promovente el curso de acción;
- II. Solicitar información técnica al desarrollador, proveedor o usuario institucional;
- III. Requerir evaluaciones de impacto adicionales;
- IV. Emitir medidas provisionales de protección;
- V. Ordenar auditorías o verificaciones urgentes.

Artículo 203. Durante la tramitación del procedimiento, la Autoridad Nacional podrá ordenar medidas cautelares cuando exista:

- I. Riesgo para derechos fundamentales;
- II. Daño potencial grave;
- III. Evidencia de discriminación, sesgo, opacidad o fallas críticas.

Artículo 204. La resolución deberá contener, en su caso, órdenes de:

- I. Corrección técnica;
- II. Ajuste de parámetros o modelos;
- III. Reparación de daños;
- IV. Suspensión temporal;
- V. Suspensión definitiva;

VI. Multas o sanciones conforme a lo dispuesto en esta Ley.

Artículo 205. En casos que involucren a instituciones públicas, la Autoridad Nacional deberá garantizar la revisión humana significativa de la decisión impugnada y asegurar la reparación integral del daño cuando corresponda.

Artículo 206. Ninguna queja podrá implicar represalias, discriminación o afectación contra la persona promovente. Las autoridades deberán garantizar canales seguros y confidenciales para la presentación de denuncias.

Artículo 207. La Autoridad Nacional publicará lineamientos para la atención de incidentes algorítmicos, fallas críticas, sesgos discriminatorios y riesgos emergentes, garantizando la protección de los usuarios afectados.

TÍTULO DÉCIMO CUARTO

Infracciones, Responsabilidades y Sanciones

Capítulo I. Clasificación de infracciones

Artículo 208. Las infracciones derivadas del incumplimiento de esta Ley se clasificarán en leves, graves y gravísimas, atendiendo a la gravedad del daño o riesgo generado, la intencionalidad de la conducta, el grado de negligencia y el impacto efectivo o potencial sobre derechos humanos, seguridad pública, integridad cognitiva, privacidad, infraestructura crítica o estabilidad democrática.

Artículo 209. Constituyen infracciones leves:

- I. Omitir actualizaciones no sustantivas en registros técnicos, siempre que no afecten la operación segura del sistema;
- II. Retrasar de manera injustificada la entrega de información no esencial requerida por la autoridad;
- III. Incumplir lineamientos administrativos de carácter general de naturaleza procedimental, que no comprometan derechos fundamentales ni la integridad del sistema.

Artículo 210. Constituyen infracciones graves:

- I. Omitir la realización de evaluaciones de impacto algorítmico cuando sean obligatorias;
- II. Negarse de manera injustificada a proporcionar información técnica estrictamente indispensable, requerida conforme a los procedimientos previstos en esta Ley, para auditorías o supervisión;
- III. Implementar sistemas de inteligencia artificial sin cumplir con los requisitos de certificación o registro, únicamente en los casos en que estos sean exigidos expresamente por esta Ley;
- IV. Manipular, alterar o destruir documentación técnica, registros algorítmicos o bitácoras de funcionamiento;
- V. Omitir de manera relevante o reiterada las medidas de mitigación de riesgos, transparencia o supervisión humana significativa expresamente exigidas por esta Ley;
- VI. Utilizar sistemas de alto riesgo fuera de los contextos autorizados; Incumplir medidas cautelares, preventivas o correctivas dictadas por la Autoridad Nacional.

Artículo 211. Constituyen infracciones gravísimas:

- I. Desarrollar o utilizar aplicaciones expresamente prohibidas en esta Ley;
- II. Implementar sistemas que, por acción u omisión dolosa o con negligencia grave, generen daños graves o irreversibles a la vida, integridad física o cognitiva, salud, privacidad, derechos humanos, seguridad nacional o infraestructura crítica;

- III. Emplear inteligencia artificial para manipulación cognitiva, política, electoral o social con fines ilícitos o contrarios a los principios democráticos, de manera deliberada. No se considerarán comprendidas en este supuesto las actividades de comunicación política, publicidad o difusión de ideas realizadas de conformidad con la ley y los principios democráticos;
- IV. Operar, desplegar o poner en funcionamiento, por parte de autoridades públicas o de particulares, sistemas autónomos letales o sistemas de inteligencia artificial capaces de causar daño grave a la integridad de las personas, cuando se realice sin supervisión humana significativa o fuera de los supuestos expresamente previstos en la ley aplicable;
- V. Utilizar inteligencia artificial para vigilancia masiva sin base legal suficiente o sin garantías adecuadas;
- VI. Proveer sistemas principalmente diseñados para el fraude, la extorsión, la desinformación o la suplantación de identidad;
- VII. Introducir deliberadamente vulnerabilidades, puertas traseras, malware o funciones ocultas en sistemas de inteligencia artificial.

Capítulo II. Procedimiento sancionador

Artículo 212. El procedimiento sancionador se iniciará de oficio, por denuncia ciudadana, informe técnico, auditoría, reporte de incidente algorítmico o cualquier otro medio objetivo y verificable que haga presumir la existencia de infracciones.

Artículo 213. Al iniciarse el procedimiento, la Autoridad Nacional deberá:

- I. Notificar al presunto infractor;
- II. Definir la conducta imputada;
- III. Solicitar la información técnica necesaria;
- IV. Determinar si existen riesgos inminentes que ameriten medidas provisionales.

Artículo 214. Durante el procedimiento, la Autoridad Nacional podrá imponer medidas cautelares, inmediatas o urgentes, cuando:

- I. Exista riesgo grave para derechos fundamentales;
- II. El sistema pueda causar daños irreversibles;
- III. Se detecten fallas críticas, sesgos severos o resultados impredecibles;
- IV. El proveedor o usuario institucional obstaculice la supervisión.

Las medidas cautelares deberán ser proporcionales, temporales y estrictamente necesarias, y no tendrán carácter sancionatorio.

Artículo 215. Concluida la investigación, la Autoridad Nacional emitirá resolución fundada y motivada que podrá contener:

- I. Determinación de inexistencia de infracción;
- II. Determinación de infracción leve, grave o gravísima;
- III. Medidas correctivas obligatorias;
- IV. Suspensión temporal del sistema;
- V. Suspensión definitiva o retiro del mercado;
- VI. Imposición de sanciones o multas;
- VII. Orden de reparación integral del daño.

Artículo 216. La resolución en ningún caso sustituirá responsabilidades civiles, administrativas o penales derivadas de los hechos.

Capítulo III. Medidas de reparación y sanciones aplicables

Artículo 217. Las sanciones podrán consistir en:

- I. Amonestación pública o privada;
- II. Multas proporcionales al daño, riesgo o beneficio obtenido;
- III. Suspensión temporal del sistema, servicio o modelo;
- IV. Suspensión definitiva o retiro del mercado;
- V. Inhabilitación para desarrollar o comercializar sistemas de inteligencia artificial;
- VI. Cancelación de certificaciones, registros o autorizaciones;
- VII. Clausura temporal o definitiva de plataformas o servicios, únicamente cuando la infracción sea gravísima y no existan medidas menos restrictivas eficaces.

Artículo 218. Las multas podrán determinarse considerando:

- I. La gravedad del daño o riesgo generado;
- II. La reincidencia;
- III. La intencionalidad o negligencia grave;
- IV. La naturaleza del sistema;

- V. El beneficio económico obtenido u ocasionado por la conducta sancionada;
- VI. El impacto social, ambiental, cognitivo o democrático.

Artículo 219. La reparación integral del daño podrá comprender:

- I. Correcciones técnicas obligatorias;
- II. Eliminación de datos obtenidos ilícitamente;
- III. Ajustes del sistema para garantizar no discriminación y corrección de sesgos;
- IV. Compensación económica a las personas afectadas;
- V. Garantías de no repetición;
- VI. Publicación de la resolución para fines de transparencia.

Artículo 220. La inhabilitación, suspensión o retiro del sistema se aplicará cuando:

- I. El sistema incurra en conductas prohibidas;
- II. Genere daños irreversibles;
- III. Existen vulnerabilidades no mitigables;
- IV. El proveedor haya actuado con dolo, ocultamiento o fraude.

Artículo 221. Cuando los hechos constituyan delitos, la Autoridad Nacional dará vista inmediata a la Fiscalía General de la República y demás autoridades competentes.

Artículo 222. La reincidencia en infracciones graves o gravísimas será considerada circunstancia agravante y podrá duplicar las sanciones aplicables.

Artículo 223. Las personas físicas o morales sancionadas podrán interponer los medios de impugnación previstos en la legislación aplicable; sin embargo, dichos recursos no suspenderán medidas cautelares dictadas para proteger derechos fundamentales o evitar daños inmediatos.

TRANSITORIOS

PRIMERO. La presente Ley entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO. El Ejecutivo Federal, por conducto de la Autoridad Nacional en Inteligencia Artificial, la Secretaría de Ciencia, Humanidades, Tecnología e

Innovación y de la Agencia de Transformación Digital y Telecomunicaciones, expedirá el Reglamento de la presente Ley dentro de un plazo máximo de ciento ochenta días naturales, contados a partir de su entrada en vigor.

El Reglamento deberá desarrollar, al menos, lo relativo a:

- a) La metodología para la clasificación de los sistemas de inteligencia artificial conforme a un enfoque basado en riesgos;
- b) Los procedimientos para la realización de evaluaciones de impacto algorítmico;
- c) Los protocolos de registro, certificación y supervisión de sistemas de inteligencia artificial;
- d) Los mecanismos de auditoría algorítmica;
- e) Los criterios para garantizar la supervisión humana significativa en los sistemas de alto riesgo.
- f) Los estándares técnicos generales y sectoriales aplicables al desarrollo, despliegue, uso y supervisión de los sistemas de inteligencia artificial.

TERCERO. Los Poderes de la Unión, las entidades federativas, los municipios y los organismos constitucionalmente autónomos deberán adecuar su normativa, reglamentos, lineamientos y disposiciones administrativas a lo previsto en la presente Ley, dentro de un plazo no mayor a 365 días naturales, contados a partir de su entrada en vigor.

CUARTO. Dentro de los noventa días naturales siguientes a la entrada en vigor de la presente Ley, deberá instalarse e iniciar funciones la Autoridad Nacional en Inteligencia Artificial, en los términos previstos en el artículo correspondiente de este ordenamiento, como la instancia responsable de la coordinación, articulación y seguimiento de la política pública nacional en materia de inteligencia artificial, conforme a las atribuciones que le confiere esta Ley.

La Autoridad Nacional ejercerá sus funciones bajo los principios de coordinación interinstitucional, eficiencia administrativa, aprovechamiento de capacidades institucionales existentes y racionalidad presupuestaria, en los términos que

establezca el Reglamento.

QUINTO. Dentro del mismo plazo previsto en el artículo transitorio anterior, la Autoridad Nacional en Inteligencia Artificial deberá integrar e instalar el Consejo Consultivo Nacional al que se refiere esta Ley, como un órgano de apoyo, consulta y emisión de recomendaciones no vinculantes, con la participación de la Federación, las entidades federativas, los municipios, la academia, el sector privado y la sociedad civil.

SEXTO. El Ejecutivo Federal aprobará y publicará la Estrategia Nacional de Inteligencia Artificial dentro de un plazo no mayor a ciento ochenta días naturales, contados a partir de la entrada en vigor de la presente Ley, como instrumento rector de planeación, coordinación, articulación y evaluación de la política pública en la materia. La conducción, seguimiento y evaluación de la Estrategia corresponderán a la Autoridad Nacional en Inteligencia Artificial, en los términos previstos en este ordenamiento y su Reglamento.

SÉPTIMO. Los sistemas de inteligencia artificial que se encuentren en operación con anterioridad a la entrada en vigor de la presente Ley deberán, en su caso, ser identificados, registrados y clasificados conforme a su nivel de riesgo, y sujetarse proporcional y progresivamente a los mecanismos de evaluación, auditoría o supervisión que resulten aplicables, de conformidad con lo previsto en esta Ley y su Reglamento, dentro de un plazo máximo de dos años.

OCTAVO. La implementación de la presente Ley se llevará a cabo preferentemente mediante el uso, fortalecimiento y coordinación de las entidades, órganos e instancias existentes, evitando la creación de estructuras administrativas innecesarias o duplicadas, conforme a los principios de eficiencia, austeridad y racionalidad del gasto público.

NOVENO. Los derechos adquiridos conforme a las leyes vigentes en materia de propiedad intelectual, propiedad industrial, derechos de autor, protección de datos personales, neuroderechos o cualquier otra materia relacionada no se verán afectados de manera retroactiva por la entrada en vigor de la presente Ley.

DÉCIMO. En lo no previsto por la presente Ley, se estará a lo dispuesto en los tratados internacionales en materia de derechos humanos de los que el Estado mexicano sea parte, así como a los principios de interpretación pro persona, no regresividad, igualdad sustantiva, perspectiva de género e inclusión digital.

ANEXOS

Glosario Reglamentario en Materia de Inteligencia Artificial

Artículo 1. Para efectos de interpretación, aplicación y ejecución de este Reglamento, se entenderá por:

A. Aprendizaje automático (*machine learning*): Subcampo de la inteligencia artificial que utiliza algoritmos y modelos estadísticos para entrenar sistemas capaces de identificar patrones en los datos y generar predicciones o decisiones, sin necesidad de programación explícita para cada tarea específica.

B. Aprendizaje profundo (*deep learning*): Técnica avanzada de aprendizaje automático que utiliza redes neuronales artificiales con múltiples capas para aprender representaciones jerárquicas y extraer características complejas de grandes volúmenes de datos, aplicable en reconocimiento de voz, procesamiento de imágenes, texto y otros datos no estructurados.

C. Deepfake: Contenido sintético o manipulado digitalmente, generado mediante modelos de inteligencia artificial, que altera o sustituye de manera hiperrealista rostros, voces, imágenes o secuencias de video, con la finalidad de imitar, falsear o distorsionar información, identidades o hechos, ya sea con fines lícitos o ilícitos.

D. Explicabilidad reforzada: Conjunto de métodos, técnicas y mecanismos destinados a permitir que los usuarios, auditores o autoridades comprendan, interpreten y evalúen las decisiones o resultados generados por sistemas complejos de inteligencia artificial, garantizando su transparencia, trazabilidad y rendición de cuentas, con el fin de preservar la confianza pública y la protección de derechos.

E. Gemelo digital: Representación virtual dinámica e interactiva de una persona, objeto, proceso, sistema o infraestructura real, actualizada continuamente mediante datos provenientes de su operación o actividad, utilizada para simular escenarios, optimizar desempeño, prevenir fallos o apoyar la toma de decisiones.

F. Gobernanza algorítmica: Conjunto de normas, mecanismos, procesos y estructuras institucionales destinados a supervisar, coordinar y controlar el desarrollo, implementación y uso de los sistemas de inteligencia artificial, garantizando la transparencia, la inclusión, la participación social y la rendición de cuentas en su funcionamiento e impacto.

G. IA de propósito general (*General Purpose AI – GPAI*): Modelos o sistemas de inteligencia artificial diseñados para realizar múltiples funciones o tareas en diversos contextos, más allá de un uso o aplicación específica, incluidos los modelos generativos de lenguaje, imagen, audio y video, susceptibles de ser adaptados o integrados en distintos sectores o productos.

H. IA explicable (*Explainable AI – XAI*): Principio técnico y normativo que exige que los sistemas de inteligencia artificial sean comprensibles, auditables y transparentes para los usuarios, auditores y autoridades competentes, a fin de garantizar la trazabilidad, la rendición de cuentas y la confianza pública en sus resultados.

I. Neurotecnología: Conjunto de técnicas, dispositivos, sistemas o aplicaciones que registran, estimulan, interpretan o modifican la actividad neuronal, cerebral o cognitiva mediante interfaz directa con el sistema nervioso o el procesamiento de señales cerebrales, con fines médicos, científicos, educativos, militares o de consumo, y que pueden incidir en la conducta, las emociones o los procesos mentales de las personas.

J. Rendición de cuentas algorítmica: Responsabilidad verificable y continua atribuible a los desarrolladores, proveedores y usuarios de sistemas de inteligencia artificial para documentar, explicar, justificar y responder por las decisiones automatizadas, sus fundamentos, efectos y consecuencias, a fin de garantizar la transparencia, la supervisión y la protección de los derechos de las personas.

K. Soberanía tecnológica: Capacidad y facultad del Estado mexicano para desarrollar, adaptar, regular y controlar tecnologías críticas, incluidas la inteligencia artificial, los datos estratégicos, el hardware, el software y la infraestructura digital, garantizando la independencia estratégica, la protección de los intereses nacionales y el desarrollo autónomo frente a actores externos públicos o privados.

L. Tecnología de caja negra: Sistema o modelo de inteligencia artificial cuyos procesos internos de decisión o aprendizaje no son comprensibles ni verificables por los usuarios, auditores o autoridades competentes, lo que impide o limita la evaluación de su lógica, sesgos, errores o riesgos, y afecta la transparencia y la rendición de cuentas.

M. Tecnologías emergentes: Innovaciones científicas o tecnológicas en

desarrollo acelerado o en proceso de adopción reciente, con alto potencial transformador en los sistemas sociales, económicos, culturales o políticos, que incluyen —entre otras— la inteligencia artificial avanzada, la robótica, la biotecnología, el blockchain, la nanotecnología y la computación cuántica.

N. Trazabilidad algorítmica: Capacidad verificable y continua de rastrear, registrar y documentar todas las fases de diseño, entrenamiento, implementación, operación y resultados de un sistema de inteligencia artificial, con el propósito de garantizar su control, revisión, auditoría y corrección, en caso de errores, fallos o afectaciones a derechos o bienes jurídicos.

ARTÍCULO TRANSITORIO

ÚNICO. La Autoridad Nacional en Inteligencia Artificial, en el ámbito de sus atribuciones, queda facultada para emitir y actualizar periódicamente el presente Glosario Reglamentario mediante disposiciones administrativas de carácter general, con el propósito de incorporar términos emergentes, innovaciones tecnológicas y estándares internacionales en evolución, asegurando su compatibilidad con los principios rectores de esta Ley y su Reglamento.

NOTA DE TRANSPARENCIA Y BUENAS PRÁCTICAS EDITORIALES:

En aras de la creciente utilización de sistemas de inteligencia artificial generativa en la elaboración de documentos legislativos y públicos en diversas naciones, y como parte de una política de transparencia institucional de la Comisión de Análisis, Seguimiento y Evaluación sobre la Aplicación y Desarrollo de la Inteligencia Artificial en México del Senado de la República, alineada con dichas prácticas internacionales, se hace constar que en la preparación de este documento se emplearon herramientas digitales —incluidos sistemas de inteligencia artificial generativa— exclusivamente para tareas auxiliares de revisión formal del texto, tales como redacción, ortografía y corrección gramatical, siempre bajo supervisión humana permanente. En ningún caso dichas herramientas intervinieron en el contenido sustantivo, en las políticas públicas propuestas, en los criterios jurídicos ni en la orientación legislativa del documento.

Los que suscriben

Senadores integrantes de la Comisión de Análisis, Seguimiento y Evaluación sobre la aplicación y desarrollo de la Inteligencia Artificial en México.

Sen. Rolando Rodrigo Zapata
Bello
Presidente

Sen. Juanita Guerra Mena
Secretaria

Sen. Miguel Pavel Jarero
Velázquez
Secretario

Sen. Araceli Saucedo Reyes
Integrante

Sen. Agustín Dorantes Lámbarri
Integrante

Sen. Yeidekol Polevnsky
Gurwitz
Integrante

Sen, Luis Donaldo Colosio Riojas
Integrante

Sen Karina Isabel Ruíz Ruíz
Integrante

Sen. Luis Alfonso Silva Romo
Integrante

Sen. Reyna Celeste Ascencio
Ortega
Integrante

Dado en el Salón de Sesiones en el mes de marzo de 2026.