INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL PARA LA REGULACIÓN Y USO ÉTICO DE LA INTELIGENCIA ARTIFICIAL EN LOS ESTADOS UNIDOS MEXICANOS.

Las suscritas **Ana Isabel González González** y **Mónica Elizabeth Sandoval Hernández** Diputadas Federales integrantes del Grupo Parlamentario del Partido Revolucionario Institucional en la LXVI Legislatura del Honorable Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II y 72 de la Constitución Política de los Estados Unidos Mexicanos; 55, fracción II, y 179 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos**,** somete a consideración de esta Honorable Asamblea la iniciativa **somete a consideración de esta soberanía la iniciativa con proyecto de decreto por el que se expide la Ley General para la Regulación y Uso Ético de la Inteligencia Artificial en los Estados Unidos Mexicanos, al tenor de lo siguiente:**

EXPOSICIÓN DE MOTIVOS

La Inteligencia Artificial (IA) se ha consolidado como uno de los vectores tecnológicos más disruptivos del siglo XXI, ejerciendo una influencia transversal en sectores estratégicos como la economía, la educación, la salud, la industria y los servicios financieros. A escala global, tanto organismos multilaterales como corporativos tecnológicos han documentado un ritmo de adopción acelerado. Se estima que aproximadamente una de cada seis personas a nivel mundial interactúa de manera regular con herramientas de inteligencia artificial generativa, un indicador que refleja una expansión transfronteriza sin precedentes.

Asimismo, el despliegue corporativo es notable: más del 70% de las unidades económicas internacionales han integrado sistemas de IA en sus cadenas operativas o procesos administrativos, priorizando la automatización de tareas, el análisis predictivo de datos y la optimización de los índices de productividad. En el contexto nacional, la penetración de la Inteligencia Artificial ha alcanzado niveles de adopción masiva que transforman la dinámica cotidiana de la población. De acuerdo con diagnósticos difundidos por la UNAM, se estima que el 66% de la población mexicana ya utiliza herramientas basadas en IA en su vida diaria.

En el ámbito de la salud, la Inteligencia Artificial (IA) ha revolucionado la gestión médica al permitir la sistematización integral de procedimientos administrativos, la optimización de protocolos diagnósticos y la mitigación de errores humanos. Asimismo, esta tecnología posee una participación activa en procesos clínicos de alta especialización y complejidad crítica, tales como la ejecución de intervenciones quirúrgicas de alta precisión mediante sistemas robóticos asistidos. De acuerdo con investigaciones de la Universidad Nacional Autónoma de México (UNAM), la integración de algoritmos de aprendizaje profundo en la lectura de imágenes médicas ha elevado la precisión diagnóstica en patologías complejas como el cáncer, mientras que el despliegue de plataformas robotizadas maximiza la seguridad del paciente y reduce los tiempos de recuperación postoperatoria[1]

La Inteligencia Artificial (IA) se ha convertido en una herramienta fundamental para fortalecer los sistemas de seguridad a nivel mundial y también en México. Durante los últimos años, su implementación ha crecido de manera constante debido al incremento de amenazas digitales, fraudes electrónicos y ataques cibernéticos que afectan tanto a gobiernos como a empresas privadas. Ante este panorama, diversas instituciones han recurrido a la construcción de sistemas de seguridad apoyados y reforzados mediante inteligencia artificial, capaces de analizar grandes volúmenes de información en tiempo real para detectar comportamientos sospechosos, prevenir riesgos y responder de manera más rápida y eficiente frente a posibles amenazas.

A nivel internacional, organismos gubernamentales, corporaciones tecnológicas y entidades financieras utilizan sistemas basados en IA para mejorar la vigilancia digital, proteger bases de datos y combatir delitos informáticos. En México, este fenómeno también ha mostrado un crecimiento importante, especialmente en el sector financiero y de ciberseguridad. Instituciones bancarias y empresas tecnológicas han comenzado a implementar sistemas de inteligencia artificial para prevenir fraudes electrónicos, detectar operaciones sospechosas y proteger la información personal de los usuarios, el periódico La Jornada reportó que Citibanamex ha declarado que logró reducir hasta en un 70% los intentos de fraude mediante herramientas basadas en inteligencia artificial. De acuerdo con directivos de la institución, estas tecnologías permiten detectar operaciones sospechosas y prevenir ataques cibernéticos de manera más eficiente[2]. Asimismo, dependencias gubernamentales y empresas privadas han incrementado el uso de tecnologías

automatizadas para monitorear amenazas digitales y reforzar sus sistemas de protección informática. Este avance responde principalmente al aumento de delitos cibernéticos y al crecimiento de las operaciones digitales en el país.

La Inteligencia Artificial, también se encuentra presente en el ámbito educativo, por ejemplo, una encuesta reciente de la Secretaría de Educación Pública (SEP) reveló que seis de cada diez universitarios mexicanos ya utilizan herramientas de inteligencia artificial generativa en sus actividades académicas, mientras que al menos cinco de cada diez docentes también emplean estas tecnologías para la elaboración de contenidos y apoyo pedagógico.[3] Asimismo, en el sector empresarial, estudios señalan que más de 495 mil empresas mexicanas adoptaron sistemas de inteligencia artificial durante el último año, elevando a aproximadamente 38% el número total de compañías que ya utilizan IA en sus operaciones diarias, principalmente para automatización, productividad y análisis de datos. como hemos observado y descrito en párrafos anteriores, datos oficiales e investigaciones revelan que, organismos financieros, instituciones gubernamentales y empresas de ciberseguridad han comenzado a implementar algoritmos inteligentes para detectar fraudes, monitorear amenazas digitales y fortalecer la protección de datos personales. Este panorama demuestra que la inteligencia artificial ya forma parte de casi todas las actividades humanas y productivas en el país, situación que evidencia no solo su importancia estratégica para el desarrollo nacional, sino también la necesidad urgente de construir marcos regulatorios y éticos que garanticen un uso seguro, transparente y respetuoso de los derechos humanos., pues su implementación ofrece grandes oportunidades para el país, pero también plantea riesgos relevantes.

A pesar de que la Inteligencia Artificial ya forma parte activa de diversas dinámicas humanas y sectores económicos en México, su adopción se ha dado al margen de un marco normativo especializado. La ausencia de reglas claras maximiza los riesgos operativos, éticos y legales en su utilización cotidiana. Por ello, resulta inaplazable que el Estado mexicano legisle en la materia para estructurar un marco de control que salvaguarde los derechos humanos de la ciudadanía frente al uso de estos sistemas automatizados. Más allá de frenar la innovación, la intervención estatal debe entenderse como un mecanismo indispensable para transformar una herramienta potencialmente riesgosa en un motor de desarrollo seguro, transparente y equitativo.

En este escenario de transición digital, resulta imperativo edificar un marco regulatorio y de protección ciudadana orientado a mitigar vulnerabilidades críticas como la discriminación algorítmica. De acuerdo con investigaciones de la Universidad Nacional Autónoma de México (UNAM), este fenómeno se define como la reproducción, automatización y amplificación de sesgos de género, raza, clase o condición socioeconómica mediante el diseño de sistemas de inteligencia artificial que asumen datos históricos prejuiciosos como verdades neutras, restringiendo de forma sistemática el acceso a derechos y oportunidades[4]. La recurrencia de este riesgo en el entorno global y nacional es alarmante: análisis especializados del Instituto de Investigaciones Jurídicas de la UNAM revelan que hasta un 40% de los algoritmos utilizados para el reclutamiento laboral, la evaluación de perfiles crediticios y el otorgamiento de servicios financieros en plataformas digitales presentan sesgos discriminatorios implícitos que marginan de manera desproporcionada a las mujeres y a los sectores de menores ingresos, lo que demuestra que la neutralidad tecnológica es una falacia si no existen auditorías de datos obligatorias y un control soberano por parte del Estado.[5]

Las violaciones a la privacidad, la falta de transparencia en decisiones automatizadas y los riesgos derivados del uso de inteligencia artificial en sistemas críticos representan actualmente algunos de los principales desafíos jurídicos y éticos asociados con el desarrollo tecnológico. Las violaciones a la privacidad ocurren cuando sistemas automatizados recopilan, almacenan o procesan datos personales sin consentimiento claro o sin mecanismos adecuados de protección, exponiendo información sensible de los usuarios.

Por otro lado, la falta de transparencia en decisiones automatizadas se refiere a la dificultad para comprender cómo funcionan los algoritmos que toman decisiones relevantes sobre personas, como la aprobación de créditos, procesos de selección laboral o evaluaciones gubernamentales, lo que puede generar discriminación, sesgos o afectaciones a derechos fundamentales. Asimismo, los riesgos en sistemas críticos como salud, justicia y seguridad pública son especialmente delicados, ya que errores algorítmicos o decisiones automatizadas incorrectas pueden afectar diagnósticos médicos, resoluciones judiciales, vigilancia ciudadana o acciones policiales. La UNESCO ha advertido que el crecimiento acelerado de la inteligencia artificial exige la creación de marcos éticos y regulatorios que protejan los derechos humanos, la transparencia y la seguridad de las personas frente al uso

indiscriminado de estas tecnologías.[6] Actualmente, México carece de una legislación integral en materia de inteligencia artificial, lo que evidencia la necesidad urgente de construir normas jurídicas especializadas que regulen su desarrollo, implementación y supervisión en beneficio de la sociedad.

El innegable y acelerado crecimiento de la inteligencia artificial en diversos sectores y en la vida misa de las y los mexicanos, ha generado la necesidad de construir una legislación especializada y una ley marco en materia de inteligencia artificial en México. La principal razón de esta necesidad radica en la obligación del Estado de proteger los derechos humanos frente a posibles riesgos derivados del uso indiscriminado de tecnologías automatizadas, particularmente en temas relacionados con privacidad, protección de datos personales, discriminación algorítmica y transparencia en la toma de decisiones automatizadas. Asimismo, la ausencia de regulación genera incertidumbre tanto para usuarios como para empresas e instituciones que desarrollan o implementan sistemas de inteligencia artificial, por lo que una legislación clara permitiría generar certeza jurídica respecto a los límites, responsabilidades y mecanismos de supervisión aplicables a estas tecnologías.

De igual forma, contar con un marco normativo moderno favorecería el impulso de la innovación y el desarrollo tecnológico, creando condiciones seguras para la inversión, la investigación y el crecimiento de empresas especializadas en inteligencia artificial. Finalmente, la creación de una ley marco permitiría al país alinearse con estándares y recomendaciones internacionales impulsadas por organismos como la UNESCO, la OCDE y la Unión Europea, los cuales han promovido principios éticos y regulatorios orientados a garantizar un uso responsable, transparente y centrado en la protección de los derechos fundamentales de las personas.

En este contexto, resulta indispensable establecer un marco normativo que regule el desarrollo, uso y supervisión de los sistemas de inteligencia artificial bajo un enfoque basado en riesgos, permitiendo identificar y controlar riesgos que puedan afectar derechos fundamentales, la seguridad o la privacidad de las personas. Una regulación integral no solo brindaría certeza jurídica y protección a los usuarios, sino que también fomentaría la innovación tecnológica responsable y el desarrollo de la

inteligencia artificial en México conforme a estándares éticos y de derechos humanos.

DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL PARA LA REGULACIÓN Y USO ÉTICO DE LA INTELIGENCIA ARTIFICIAL.

UNICO. Se expide la Ley General para la Regulación y Uso Ético de la Inteligencia Artificial, para quedar como sigue**:**

LEY GENERAL PARA LA REGULACIÓN Y USO ÉTICO DE LA INTELIGENCIA ARTIFICIAL

TÍTULO PRIMERO.
DISPOSICIONES GENERALES

Artículo 1. La presente Ley es de orden público e interés social y tiene por objeto regular el desarrollo, puesta a disposición, implementación, operación y supervisión de los sistemas de inteligencia artificial en el territorio nacional, con enfoque de derechos humanos, seguridad, transparencia e innovación responsable.

Artículo 2. Esta Ley es aplicable a:

I. Autoridades, dependencias y entidades de cualquier orden de gobierno que desarrollen, adquieran o utilicen sistemas de inteligencia artificial;
II. Personas físicas o morales que desarrollen, comercialicen, distribuyan, integren o utilicen sistemas de inteligencia artificial en México; y
III. Sistemas de inteligencia artificial cuyos resultados produzcan efectos en el territorio nacional.

Artículo 3. La interpretación de esta Ley se realizará conforme a la Constitución, los tratados internacionales en materia de derechos humanos y el principio pro persona.

Artículo 4. Toda actividad regulada por esta Ley deberá respetar, como mínimo, los derechos a la igualdad y no discriminación, privacidad, protección de datos

personales, libertad de expresión, acceso a la información, debido proceso, seguridad jurídica, trabajo digno y los derechos de niñas, niños y adolescentes.

Artículo 5. Son principios rectores de esta Ley: legalidad, transparencia, entendimiento razonable, responsabilidad, trazabilidad, seguridad y robustez, supervisión humana, prevención de daños, proporcionalidad, no discriminación y rendición de cuentas.

Artículo 6. Para efectos de esta Ley se entiende por:

I. **Agencia Nacional de Supervisión de la Inteligencia Artificial:** Nuevo organismo público autónomo encargado de supervisar, verificar y sancionar el uso de IA en México.
II. **Alfabetización en IA:** Programas de capacitación y educación para que personas, empresas y gobierno comprendan el funcionamiento y riesgos de la IA.
III. **Amenazas Digitales,** Riesgos o acciones maliciosas que afectan sistemas informáticos, redes, datos o servicios digitales.
IV. **Ataques Cibernéticos** Acciones dirigidas contra sistemas tecnológicos o redes digitales con el objetivo de dañar, alterar, bloquear o acceder ilícitamente a información.
V. **Auditorías algorítmicas:** Revisiones técnicas y organizacionales para verificar cumplimiento legal, funcionamiento y ausencia de riesgos indebidos
VI. **Contenido sintético:** Material generado o alterado mediante IA que puede aparentar ser auténtico o humano.
VII. **Corporaciones Tecnológicas** Empresas especializadas en el desarrollo, comercialización o implementación de tecnologías digitales, software e inteligencia artificial.
VIII. **Delitos Informáticos.** Conductas ilícitas cometidas mediante computadoras, redes o tecnologías digitales, como hackeo, robo de datos o fraude electrónico
IX. **Desplegador (usuario implementador):** quien utiliza un sistema de IA en una actividad profesional, comercial, laboral o pública;
X. **Discriminación algorítmica:** Reproducción y amplificación de sesgos de género, raza, clase o condición socioeconómica mediante algoritmos automatizados.

XI. **Distribuidor:** quien comercializa o facilita el acceso a un sistema de IA sin ser proveedor;

XII. **Entidades Financieras** Instituciones dedicadas a actividades bancarias, crediticias, aseguradoras o de manejo de recursos económicos.

XIII. **Evaluación de impacto:** análisis documentado de riesgos, mitigaciones y efectos;

XIV. **Fraudes Electrónicos** Actos ilícitos realizados mediante plataformas digitales o sistemas informáticos para engañar, robar información o recursos económicos

XV. **Incidente grave:** evento que cause o pueda causar daño significativo a personas, derechos o seguridad.

XVI. **Inteligencia Artificial (IA):** sistemas computacionales o híbridos que, a partir de datos, modelos o reglas, generan resultados como predicciones, recomendaciones, contenidos o decisiones;

XVII. **Inteligencia Artificial Generativa**: Tipo de inteligencia artificial capaz de crear contenidos nuevos como textos, imágenes, audios, videos o códigos a partir de datos y patrones aprendidos.

XVIII. **Organismos Gubernamentales,** Instituciones del Estado encargadas de ejercer funciones públicas, administrativas, regulatorias o de seguridad.

XIX. **Proveedor:** quien desarrolla, entrena, ajusta, ofrece o pone a disposición un sistema de IA;

XX. **Registro Nacional de Sistemas de IA de Alto Riesgo:** Base oficial administrada por la autoridad para registrar sistemas de IA considerados de alto riesgo.

XXI. **Sandboxes regulatorios:** Entornos controlados de prueba autorizados por la autoridad para experimentar con IA bajo supervisión y límites definido

XXII. **Sistema de alto riesgo:** el que puede afectar de manera significativa derechos o seguridad;

XXIII. **Sistema de IA:** aplicación, servicio, modelo, dispositivo o componente que utilice IA para producir resultados;

XXIV. **Sistemas Robóticos Asistidos.** Tecnologías que combinan robótica e inteligencia artificial para apoyar o ejecutar tareas especializadas con alta precisión, especialmente en medicina e industria.

XXV. **Suplantación dañosa:** Uso de IA para imitar identidades o atribuir expresiones falsas con intención de causar daño, fraude o violencia.

Artículo 7. En lo no previsto por esta Ley, se aplicarán supletoriamente las disposiciones administrativas y civiles federales aplicables y, en su caso, la normatividad en protección de datos personales, laboral, consumo, competencia económica y procedimiento administrativo, en tanto no se opongan a esta Ley.

Artículo 8. Cuando un sistema de IA se utilice en sectores regulados (salud, financiero, telecomunicaciones, transporte, educación u otros), deberá cumplirse esta Ley y la regulación sectorial correspondiente, aplicándose el estándar más protector para las personas.

TÍTULO SEGUNDO.
GOBERNANZA Y AUTORIDADES

Artículo 9. La autoridad rectora para la aplicación de esta Ley será la **Agencia Nacional de Supervisión de la Inteligencia Artificial**, en lo sucesivo la Agencia.

Artículo 10. La Agencia será un organismo público con autonomía técnica, con atribuciones para emitir lineamientos, supervisar, verificar y sancionar conforme a esta Ley.

Artículo 11. La Agencia coordinará su actuación con:

I. La autoridad garante en transparencia y protección de datos personales, o el organismo que en su caso la sustituya;
II. La autoridad laboral competente;
III. Las autoridades de protección de niñas, niños y adolescentes;
IV. Autoridades sectoriales cuando el sistema de IA opere en ámbitos regulados; y
V. Autoridades de seguridad pública y procuración de justicia cuando existan hechos posiblemente delictivos.

Artículo 12. La Agencia tendrá, entre otras, las facultades siguientes:

I. Emitir criterios técnicos y guías de cumplimiento;
II. Administrar el Registro Nacional de Sistemas de IA de Alto Riesgo;
III. Practicar verificaciones, requerir información y ordenar auditorías;
IV. Dictar medidas de seguridad y cautelares;

V. Conocer denuncias y tramitar procedimientos sancionadores;
VI. Acreditar y supervisar organismos evaluadores de conformidad; y
VII. Promover programas de alfabetización y buenas prácticas.

Artículo 13. La Agencia contará con un Consejo Consultivo con participación plural (academia, sector productivo, sociedad civil y especialistas) con funciones de opinión no vinculante, priorizando la protección de derechos.

Artículo 14. La Agencia publicará de forma accesible: criterios, guías, estadísticas de incidentes, sanciones firmes y un informe anual, preservando datos personales y secretos industriales.

TÍTULO TERCERO.
CLASIFICACIÓN DE RIESGOS Y PRÁCTICAS PROHIBIDAS

Artículo 15. Clasificación por niveles de riesgo.
Los sistemas de IA se clasifican en:
I. Riesgo mínimo;
II. Riesgo limitado;
III. Alto riesgo; y
IV. Riesgo prohibido.

Artículo 16. Se consideran de riesgo mínimo los sistemas cuyo uso no impacte significativamente derechos o seguridad; se sujetarán a buenas prácticas y transparencia general.

Artículo 17. Riesgo limitado. Se consideran de riesgo limitado los sistemas que interactúan con personas o generan contenido susceptible de confusión; deberán cumplir obligaciones de aviso e identificación de IA.

Artículo 18. Alto riesgo. Se consideran de alto riesgo, entre otros, los sistemas de IA usados en:

I. Salud, diagnóstico o triage;
II. Educación con efectos de evaluación o acceso;
III. Empleo (reclutamiento, evaluación, permanencia o despido);

IV. Seguridad pública, vigilancia focalizada o análisis predictivo;
V. Justicia (apoyo a decisiones jurisdiccionales o ministeriales);
VI. Servicios esenciales (crédito, seguros, vivienda, servicios públicos); y
VII. Identidad, biometría o verificación de personas.

Artículo 19. Para clasificar un sistema como de alto riesgo se considerarán: impacto a derechos, probabilidad y severidad de daños, población afectada, irreversibilidad, opacidad, dependencia del sistema y dificultad de corrección.

Artículo 20. Se prohíben los sistemas de IA destinados a:

I. Manipular conductas aprovechando vulnerabilidades de manera que cause daños relevantes;
II. Implementar vigilancia masiva indiscriminada sin base legal y control judicial cuando corresponda;
III. Realizar “puntuación social” generalizada con efectos adversos sobre derechos; y
IV. Cualquier uso cuyo propósito directo sea vulnerar derechos humanos.

Artículo 21. Todo proveedor y desplegador deberá clasificar el sistema que opere y conservar evidencia documental. La Agencia podrá reclasificar cuando existan elementos que lo justifiquen.

Artículo 22. Cambios sustanciales. Si un sistema de IA sufre cambios sustanciales (datos, modelo, finalidad, contexto o población), deberá reevaluarse su riesgo y, en su caso, repetirse la evaluación de impacto y la conformidad.

TÍTULO CUARTO.
OBLIGACIONES SEGÚN EL ROL EN LA CADENA DE VALOR

Capítulo I. Obligaciones comunes

Artículo 23. Quienes desarrollen o utilicen IA deberán actuar con diligencia razonable para prevenir daños previsibles.

Artículo 24. Todo sistema de IA deberá adoptar medidas razonables de seguridad, control de accesos y protección contra manipulación, fugas y fallas.

Artículo 25. Se deberán prevenir sesgos y resultados discriminatorios, con pruebas y ajustes razonables, especialmente cuando el sistema afecte derechos o acceso a oportunidades.

Capítulo II. Proveedores

Artículo 26. El proveedor deberá generar y conservar documentación mínima: finalidad, limitaciones, datos utilizados de forma general, métricas relevantes, riesgos conocidos y controles implementados.

Artículo 27. Los proveedores de sistemas de alto riesgo deberán establecer un esquema documentado de gestión de riesgos durante todo el ciclo de vida.

Artículo 28. Deberán aplicarse criterios de calidad, pertinencia y minimización en los datos, y medidas para reducir sesgos y errores.

Artículo 29. Los sistemas de alto riesgo deberán permitir rastrear resultados relevantes y conservar registros técnicos necesarios para auditoría y rendición de cuentas.

Artículo 30. El proveedor deberá proporcionar instrucciones claras al desplegador: finalidad, condiciones de uso, limitaciones, riesgos y medidas de supervisión humana.

Capítulo III. Desplegadores
(usuarios implementadores)

Artículo 31. El desplegador deberá usar el sistema de IA conforme a su finalidad declarada y a las instrucciones del proveedor.

Artículo 32. En sistemas de alto riesgo, el desplegador garantizará supervisión humana efectiva, con capacidad real de intervención, corrección y suspensión.

Artículo 33. Antes de usar un sistema de alto riesgo, el desplegador deberá realizar una evaluación de impacto proporcional, incluyendo impactos a derechos humanos cuando proceda.

Artículo 34. Cuando el sistema de IA influya de manera relevante en decisiones sobre personas, el desplegador deberá conservar evidencia sobre el uso del sistema y los criterios de revisión humana.

Capítulo IV. Distribuidores e integradores

Artículo 35. El distribuidor deberá informar al adquirente sobre obligaciones de esta Ley cuando el sistema sea de riesgo limitado o alto.

Artículo 36. Quien integre múltiples componentes de IA para una finalidad de alto riesgo asumirá obligaciones como proveedor respecto del sistema integrado.

TÍTULO QUINTO.
REGISTRO NACIONAL, EVALUACIÓN DE IMPACTO Y CONFORMIDAD

Capítulo I. Registro Nacional

Artículo 37. Se crea el Registro Nacional, a cargo de la Agencia, para sistemas de alto riesgo operando en México.

Artículo 38. Todo sistema de alto riesgo deberá inscribirse antes de su operación, salvo excepciones justificadas por interés público urgente, conforme a lineamientos de la Agencia.

Artículo 39. La inscripción contendrá, al menos: responsable, finalidad, sector, medidas de mitigación, evaluación de impacto, esquema de supervisión humana y contacto para quejas.

Artículo 40. El Registro tendrá una versión pública con información esencial y una versión reservada con detalles técnicos, protegiendo datos personales y secretos industriales.

Capítulo II. Evaluación de impacto

Artículo 41. Los sistemas de alto riesgo deberán contar con evaluación de impacto previa, que identifique riesgos y medidas de mitigación.

Artículo 42. Cuando el sistema sea usado por autoridades o incida en derechos fundamentales, la evaluación deberá incluir un apartado específico de impacto en derechos humanos y grupos vulnerables.

Artículo 43. La evaluación de impacto se actualizará cuando existan cambios sustanciales o incidentes graves.

Capítulo III. Conformidad y certificación

Artículo 44. Los sistemas de alto riesgo deberán demostrar conformidad con los requisitos aplicables antes de su operación.

Artículo 45. La conformidad podrá demostrarse mediante:

I. Autoevaluación documentada bajo lineamientos de la Agencia; y/o
II. Evaluación por terceros acreditados cuando la Agencia lo determine por nivel de riesgo o sensibilidad.

Artículo 46. La Agencia acreditará organismos evaluadores conforme a criterios técnicos y de independencia.

Artículo 47. Acreditada la conformidad, el responsable emitirá una declaración documentada y la conservará para verificación.

Artículo 48. La conformidad tendrá vigencia conforme a lineamientos; deberá renovarse si hay cambios sustanciales o al concluir su periodo.

TÍTULO SEXTO.
SUPERVISIÓN, MONITOREO Y REPORTE DE INCIDENTES

Artículo 49. Los responsables de sistemas de alto riesgo deberán monitorear su desempeño, sesgos y fallas de manera continua y documentada.

Artículo 50. Todo incidente grave deberá reportarse a la Agencia en términos de lineamientos, incluyendo medidas tomadas para contener el daño.

Artículo 51. La Agencia podrá ordenar auditorías técnicas y organizacionales cuando existan indicios de incumplimiento o riesgo relevante.

Artículo 52. La Agencia podrá realizar visitas de verificación, requerir información y entrevistar al personal responsable, respetando la legalidad y el debido proceso.

Artículo 53. Proveedores, desplegadores y distribuidores deberán cooperar con la Agencia, aportando información necesaria para supervisión.

TÍTULO SÉPTIMO.
MEDIDAS DE SEGURIDAD Y CAUTELARES

Artículo 54. Ante riesgo inminente o daño en curso, la Agencia podrá ordenar:

I. Suspensión temporal del sistema;
II. Limitación de funcionalidades;
III. Corrección obligatoria;
IV. Retiro o deshabilitación; o
V. Avisos obligatorios a personas usuarias.

Artículo 55. Las medidas cautelares se dictarán de forma fundada, proporcional y temporal, y podrán revisarse a solicitud del interesado.

Artículo 56. Cuando proceda, la Agencia podrá exigir un plan de corrección con plazos, responsables y verificaciones.

TÍTULO OCTAVO.
DERECHOS DE LAS PERSONAS Y MECANISMOS DE REPARACIÓN

Artículo 57. Toda persona tiene derecho a ser informada de manera clara cuando interactúe con un sistema de IA, salvo excepciones legales.

Artículo 58. Cuando una decisión que afecte significativamente a una persona esté influida por IA, la persona podrá solicitar una explicación razonable sobre los factores principales considerados.

Artículo 59. En ámbitos de alto riesgo, la persona podrá solicitar revisión humana efectiva de la decisión, salvo imposibilidad legal debidamente fundada.

Artículo 60. Las personas podrán presentar quejas ante el responsable y/o ante la Agencia. Los responsables deberán habilitar canales accesibles.

Artículo 61. Cuando se acrediten afectaciones, podrán imponerse medidas de corrección, compensación, rectificación, disculpa pública cuando corresponda, y otras previstas por el marco aplicable.

TÍTULO NOVENO.
USOS EN ENTORNOS SOCIALES, LABORALES Y PROTECCIÓN DE MENORES

Capítulo I. Entornos sociales y contenido sintético

Artículo 62. Quien difunda contenido generado o alterado por IA con potencial de confusión deberá identificarlo de manera clara, conforme a lineamientos.

Artículo 63. Se prohíbe usar IA para suplantar identidad o atribuir expresiones falsas con finalidad de causar daño, fraude o violencia.

Artículo 64. Los usos de IA que afecten deliberación pública deberán prevenir desinformación sistemática y manipulación indebida, conforme a la legislación aplicable.

Capítulo II. Ámbito laboral

Artículo 65. Cuando se use IA en reclutamiento, evaluación, supervisión o decisiones laborales, el empleador deberá informar de forma clara a las personas trabajadoras.

Artículo 66. Se prohíbe el uso de IA para decisiones laborales con efectos discriminatorios o sin posibilidad de revisión humana.

Artículo 67. En sistemas de alto riesgo en el trabajo, deberá existir evaluación de impacto, incluyendo riesgos de sesgo, privacidad y efectos en dignidad y condiciones laborales.

Capítulo III. Niñas, niños y adolescentes

Artículo 68. En cualquier sistema de IA accesible a niñas, niños o adolescentes prevalecerá el interés superior de la niñez.

Artículo 69. Los datos personales de menores tendrán protección reforzada. Queda prohibido usarlos para perfiles de riesgo o publicidad dirigida en términos contrarios al marco aplicable.

Artículo 70. Los sistemas accesibles a menores deberán incorporar medidas de seguridad, controles parentales cuando proceda, lenguaje claro y mitigación de riesgos de dependencia, manipulación o daño.

Artículo 71. Se prohíbe emplear IA para:

I. Explotación, abuso o violencia contra menores;
II. Generación o difusión de contenido sexual o degradante de menores; y
III. Cualquier práctica que ponga en riesgo su integridad.

TÍTULO DÉCIMO.
INNOVACIÓN, ALFABETIZACIÓN Y ESPACIOS DE PRUEBA

Artículo 72. El Estado promoverá investigación, desarrollo e innovación en IA con enfoque ético y beneficios sociales.

Artículo 73. La Agencia podrá autorizar entornos controlados de prueba (sandboxes) con salvaguardas, duración definida y evaluación de riesgos.

Artículo 74. La Agencia promoverá programas de alfabetización y capacitación para sector público, privado, educativo y social, priorizando seguridad y derechos.

Artículo 75. Contratación pública. Las adquisiciones gubernamentales de IA deberán exigir evaluación de impacto, transparencia y cláusulas de auditoría y seguridad conforme a lineamientos.

TÍTULO DÉCIMO PRIMERO.
INFRACCIONES, SANCIONES Y
PROCEDIMIENTO ADMINISTRATIVO SANCIONADOR

Capítulo I. Infracciones

Artículo 76. Las infracciones a esta Ley se clasifican en leves, graves y muy graves, conforme al riesgo, daño causado, intencionalidad, reincidencia y cooperación.

Artículo 77. Son infracciones leves, entre otras: incumplir avisos de interacción con IA o fallas menores de documentación sin daño acreditado.

Artículo 78. Son graves, entre otras: operar un sistema de alto riesgo sin evaluación de impacto, sin registro o sin supervisión humana efectiva.

Artículo 79. Son muy graves, entre otras: operar prácticas prohibidas, ocultar incidentes graves, impedir auditorías o causar daños significativos por negligencia o dolo.

Capítulo II. Sanciones

Artículo 80. Las sanciones podrán consistir en:

I. Amonestación;
II. Multa;

III. Suspensión temporal;
IV. Clausura o retiro;
V. Inhabilitación para operar sistemas de alto riesgo por un periodo;
VI. Publicación de sanción firme; y
VII. Medidas de reparación y corrección.

Artículo 81. Se considerarán: gravedad del daño, número de personas afectadas, beneficio obtenido, reincidencia, cooperación, medidas de mitigación y capacidad económica.

Artículo 82. La acción para sancionar prescribirá conforme a plazos que determine el reglamento, atendiendo a la gravedad de la infracción, sin perjuicio de responsabilidades civiles o penales.

Capítulo III. Procedimiento administrativo sancionador

Artículo 83. El procedimiento iniciará de oficio o por denuncia. La Agencia emitirá acuerdo de inicio con hechos, norma presuntamente infringida y requerimientos.

Artículo 84. La persona presunta infractora será notificada y tendrá derecho a: conocer el expediente, ofrecer pruebas y formular alegatos.

Artículo 85. Se admitirán pruebas técnicas, documentales, periciales y otras pertinentes. La Agencia podrá requerir pruebas adicionales o dictámenes.

Artículo 86. La Agencia podrá dictar medidas cautelares conforme al Título Séptimo cuando exista riesgo inminente o continuidad del daño.

Artículo 87. La Agencia emitirá resolución fundada y motivada, determinando existencia o no de infracción, sanción, medidas correctivas y plazos de cumplimiento.

Artículo 88. La resolución podrá ejecutarse conforme a reglas administrativas aplicables. El cumplimiento será verificable y, en su caso, sujeto a nuevas medidas.

Artículo 89. Si la Agencia advierte posibles delitos o violaciones a otras leyes, dará vista a las autoridades competentes.

TÍTULO DÉCIMO SEGUNDO.
MEDIOS DE IMPUGNACIÓN

Artículo 90. Contra actos y resoluciones de la Agencia procederá el recurso de revisión, conforme a plazos y formalidades que establezca el reglamento.

Artículo 91. La interposición del recurso no suspende automáticamente el acto impugnado, salvo que se conceda suspensión cuando no se afecte el interés público y se eviten daños irreparables.

Artículo 92. La autoridad competente resolverá confirmando, modificando o revocando el acto impugnado, debidamente fundado y motivado.

ARTÍCULOS TRANSITORIOS

Primero. El presente Decreto entrará en vigor a los ciento ochenta días naturales siguientes al de su publicación en el Diario Oficial de la Federación.

Segundo. El Ejecutivo Federal deberá expedir el reglamento de la presente Ley dentro de los ciento veinte días naturales siguientes a la publicación del presente Decreto.

Tercero. La **Agencia Nacional de Supervisión de la Inteligencia Artificial** deberá quedar constituida y en operación dentro de los ciento ochenta días naturales siguientes a la entrada en vigor de la presente Ley.

Cuarto. Las dependencias y entidades de la Administración Pública, en el ámbito de sus competencias, deberán realizar las adecuaciones administrativas y presupuestarias necesarias para cumplir con esta Ley dentro de los ciento ochenta días naturales siguientes a su entrada en vigor.

Quinto. Los sistemas de inteligencia artificial considerados de alto riesgo que se encuentren operando a la entrada en vigor de esta Ley deberán inscribirse en el Registro Nacional y completar su evaluación de impacto en un plazo no mayor a trescientos sesenta días naturales, conforme a los lineamientos que emita la Agencia.

Sexto. En tanto se emiten lineamientos, criterios y formatos previstos en esta Ley, los sujetos obligados deberán adoptar medidas razonables de documentación, supervisión humana, gestión de riesgos y atención de incidentes, sin perjuicio de las obligaciones previstas en otros ordenamientos aplicables.

Palacio Legislativo de San Lázaro
08 de junio de 2026.

Ana Isabel González González

Mónica Elizabeth Sandoval Hernández

Notas:

1. Melba Pría, “La inteligencia artificial en la medicina del siglo XXI”, *Gaceta UNAM*, 15 de enero de 2026, sección Academia, https://www.gaceta.unam.mx/la-inteligencia-artificial-en-la-medicina/.

2. Gutierres Julio. La Jornada. “Fraudes se redujeron 70% con inteligencia artificial: Citibanamex”. *La Jornada*, 4 de marzo de 2024. https://www.jornada.com.mx/noticia/2024/03/04/economia/fraudes-se-redujeron-70-con-inteligencia-artificial-citibanamex-9093?utm_source=chatgpt.com

3. Infobae México, “6 de cada 10 universitarios en México ya usan inteligencia artificial generativa, revela encuesta de la SEP”, *Infobae*, 29 de abril de 2026, https://www.infobae.com/mexico/2026/04/29/6-de-cada-10-universitarios-en-mexico-ya-usan-inteligencia-artificial-generativa-revela-encuesta-de-la-sep/.

4. Ciro Murayama y María Elena Estavillo, “Sesgos de género y exclusión en la era del algoritmo”, *Revista de la Universidad de México*, n.° 912 (febrero de 2025): 42-45, https://www.revistadelauniversidad.mx/articulos/sesgos-y-algoritmos.

5. Instituto de Investigaciones Jurídicas, *Inteligencia Artificial y Derechos Humanos: Diagnóstico sobre sesgos de automatización en México* (Ciudad de México: UNAM, IIJ, 2025), p. 78-82.

6. UNESCO. *Recomendación sobre la Ética de la Inteligencia Artificial*. París: UNESCO, 2021. Consultado el 18 de mayo de 2026. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics.