PROYECTO DE LEY

LA CÁMARA DE REPRESENTANTES DE LA PROVINCIA

SANCIONA CON FUERZA DE

LEY

MARCO PARA LA CONTRATACIÓN, IMPLEMENTACIÓN Y USO RESPONSABLE DE SISTEMAS DE INTELIGENCIA ARTIFICIAL EN EL SECTOR PÚBLICO PROVINCIAL

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1.- Objeto.La presente ley tiene por objeto regular la contratación, implementación, uso, supervisión y evaluación de sistemas de inteligencia artificial en el Sector Público Provincial, a fin de asegurar un uso responsable, transparente, eficiente, interoperable, estratégico y centrado en las personas, promoviendo la innovación pública y la mejora de los servicios.

ARTÍCULO 2.- Ámbito de aplicación. Quedan comprendidos en la presente ley la Administración Pública Central, los organismos descentralizados y autárquicos, los entes públicos, las sociedades con participación estatal mayoritaria y toda otra entidad que utilice recursos públicos provinciales o trate datos bajo responsabilidad del Estado provincial, en los procesos alcanzados por la presente.

Los municipios podrán adherir a la presente ley conforme sus competencias y la normativa aplicable.

ARTÍCULO 3.- Definiciones. A los efectos de esta ley, se entiende por:

a) sistema de Inteligencia Artificial (Sistema de IA): sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere a partir de la información que recibe cómo generar resultados tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales, con diferentes niveles de autonomía y adaptabilidad;

b) proveedor: persona humana o jurídica que desarrolla, licencia, integra, implementa, opera, presta servicios vinculados o mantiene un sistema de IA para el Estado;

c) ciclo de vida: etapas de diseño o selección, adquisición/contratación, entrenamiento o configuración, pruebas, implementación, operación, monitoreo, actualización, retiro y archivo;

Cod_Veri:914642

d) trazabilidad: capacidad de reconstruir decisiones, datos, versiones, cambios y responsables del sistema;

e) auditabilidad: posibilidad técnica y jurídica de evaluar el sistema, sus datos, su desempeño y sus efectos, mediante auditorías internas y externas conforme corresponda;

f) interoperabilidad: capacidad de sistemas y componentes para intercambiar información y operar conjuntamente mediante estándares e interfaces definidas;

g) sesgo algorítmico: distorsión que puede generar resultados errados o discriminatorios por estereotipos, valores o patrones de exclusión presentes en datos o modelos; y

h) Evaluación de Impacto Algorítmico (EIA): proceso documentado para identificar, analizar, evaluar y mitigar riesgos y efectos del sistema de IA sobre derechos, servicios, seguridad, privacidad, equidad y desempeño, antes de su implementación y durante su operación. (Concepto compatible con evaluaciones de impacto ético y de datos).

ARTÍCULO 4.- Supletoriedad normativa. La presente ley se aplica sin perjuicio del cumplimiento de la normativa provincial vigente en materia de contrataciones, acceso a la información, registros y datos y demás normativa específica aplicable, y sin alterar las competencias legalmente asignadas a otros órganos, autoridades u organismos de control del Estado provincial.

CAPÍTULO II

PRINCIPIOS RECTORES

ARTÍCULO 5.- Principios. Los organismos alcanzados deberán observar, como mínimo, los siguientes principios:

a) transparencia y explicabilidad en grado proporcional al riesgo;

b) supervisión humana efectiva y responsabilidad institucional;

c) enfoque basado en riesgo durante todo el ciclo de vida;

d) protección de derechos y garantías de no discriminación;

e) calidad, seguridad y robustez técnica;

f) privacidad y protección de datos desde el diseño y por defecto;

g) innovación pública orientada a valor público, sin obstaculizar la mejora de servicios;

h) interoperabilidad y reutilización de componentes y soluciones tecnológicas;

i) rendición de cuentas y trazabilidad; y

j) proporcionalidad entre exigencias, costo, impacto y riesgo del sistema.

CAPÍTULO III

CLASIFICACIÓN DE SISTEMAS DE IA SEGÚN RIESGO

Cod_Veri:914642

ARTÍCULO 6.- Clasificación general. A los fines de esta ley, los sistemas de IA se clasifican en:

a) Riesgo bajo;

b) Riesgo medio;

c) Riesgo alto.

ARTÍCULO 7.- Criterios de clasificación. La clasificación deberá considerar, como mínimo:

a) el tipo de decisión o recomendación que produce el sistema;

b) la probabilidad y gravedad de impactos sobre derechos y libertades;

c) el tratamiento de datos personales o sensibles;

d) el ámbito de aplicación (salud, seguridad, asistencia social, educación, justicia administrativa, empleo público, fiscalización, infraestructura crítica u otros análogos);

e) el grado de autonomía y posibilidad de revertir o corregir resultados;

f) población potencialmente afectada, especialmente grupos en situación de vulnerabilidad.

ARTÍCULO 8.- Presunciones de riesgo alto. Se presumen de riesgo alto, salvo prueba fundada en contrario, los sistemas de IA cuyo resultado constituya base principal para decisiones o acciones con impacto legal o material significativo sobre derechos, acceso a servicios públicos críticos, salud y seguridad, seguridad pública, infraestructura crítica o activos estratégicos.

ARTÍCULO 9.- Determinación y registro de la clasificación. Cada organismo deberá documentar la clasificación del sistema de IA y registrarla conforme el Registro Provincial de Sistemas de IA creado por la presente, con justificación técnica y jurídica.

CAPÍTULO IV

RÉGIMEN DE CONTRATACIÓN PÚBLICA DE IA

ARTÍCULO 10.- Regla general. Toda contratación, adquisición, licenciamiento, desarrollo, integración, operación o mantenimiento de sistemas de IA deberá ajustarse al régimen provincial de contrataciones y a los requisitos adicionales de esta ley.

ARTÍCULO 11.- Requisitos mínimos en pliegos. Los pliegos y contratos deberán incluir, según corresponda al riesgo:

a) descripción funcional y técnica del sistema, datos y componentes;

b) requisitos de seguridad, robustez y pruebas;

c) requisitos de trazabilidad, versionado y registro de cambios;

d) obligaciones de mitigación y monitoreo de sesgos y desempeño;

e) condiciones sobre datos: calidad, procedencia, licencias**,** base jurídica del tratamiento, finalidad, restricciones de uso, minimización, conservación, anonimización, disociación o seudonimización cuando corresponda, y eliminación segura;

f) obligaciones de auditabilidad, acceso a información técnica suficiente y cooperación en auditorías;

g) régimen de incidentes y notificación (errores graves, brechas de seguridad, degradación, impactos no previstos);

h) derechos de uso, reutilización, modificación, mantenimiento, auditoría, portabilidad y continuidad operativa del Estado sobre entregables, documentación y configuraciones críticas, modelos ajustados, integraciones, APIs, bases de conocimiento, código fuente cuando corresponda y demás componentes críticos, conforme el régimen de propiedad intelectual aplicable;

i) condiciones de portabilidad y salida para evitar dependencias tecnológicas no justificadas, incluyendo documentación suficiente, transferencia de conocimiento y mecanismos de continuidad del servicio; y

j) prohibición de utilizar datos, documentos, consultas, resultados o interacciones del Estado provincial para entrenar, ajustar o mejorar modelos propios o de terceros, salvo autorización expresa, fundada y conforme la normativa aplicable.

ARTÍCULO 12.- Evaluación técnica y ética previa. Antes de adjudicar, el organismo contratante deberá realizar una evaluación proporcional al riesgo que considere, como mínimo: idoneidad técnica, seguridad, impacto en derechos, protección de datos, explicabilidad, gobernanza y factibilidad de auditoría, sin perjuicio de dictámenes que correspondan.

ARTÍCULO 13.- Criterio de "valor público". En la evaluación de ofertas, además del precio, deberán ponderarse criterios de valor público, incluyendo calidad técnica, confiabilidad, equidad, transparencia, protección de datos, explicabilidad, supervisión humana, sostenibilidad e interoperabilidad.

ARTÍCULO 14.- Prioridad de interoperabilidad y reutilización. Los organismos deberán priorizar soluciones:

a) interoperables mediante estándares y APIs;

b) reutilizables como componentes; y
c) compatibles con arquitecturas de "Gobierno como plataforma", conforme la Autoridad de Aplicación determine.

ARTÍCULO 15.- Contratación de IA de propósito general y software con IA embebida.

Cuando se adquieran modelos o servicios de IA de propósito general, o software que incorpore funcionalidades de IA, las exigencias se aplicarán de modo adaptado y proporcional a las posibilidades reales de acceso a información del modelo subyacente, sin renunciar a obligaciones esenciales de seguridad, privacidad, transparencia y gestión de riesgos; debiendo el organismo contratante evaluar previamente la suficiencia de dichas garantías antes de su implementación.

ARTÍCULO 16. - Uso de herramientas de inteligencia artificial generativa. Los organismos alcanzados que utilicen herramientas de inteligencia artificial generativa deberán establecer reglas internas de uso responsable, proporcionales al riesgo, que contemplen como mínimo:
a) prohibición de ingresar datos personales sensibles, información confidencial, reservada, fiscal, sanitaria, judicial, de seguridad, protegida por secreto legal o sujeta a regímenes especiales, salvo autorización expresa, fundamento jurídico suficiente y medidas de seguridad adecuadas;
b) revisión humana previa de los resultados antes de su utilización en actos administrativos, comunicaciones oficiales o decisiones que produzcan efectos sobre personas;
c) identificación del uso de IA cuando el contenido generado o alterado sustancialmente sea difundido al público y pueda inducir a error sobre su origen;
d) registro razonable del uso en procesos de riesgo medio o alto, conforme establezca la reglamentación; y
e) prohibición de utilizar resultados generados por IA como fundamento único de decisiones administrativas con efectos jurídicos o materiales relevantes sobre las personas.

CAPÍTULO V

REGISTRO PROVINCIAL DE SISTEMAS DE IA

ARTÍCULO 17.- Creación. Créase el Registro Provincial de Sistemas de Inteligencia Artificial del Sector Público, de carácter obligatorio, digital y de acceso público, con excepciones fundadas por razones de seguridad, protección de datos o secreto comercial conforme reglamentación. En los casos de sistemas vinculados a

seguridad, infraestructura crítica o información sensible, la reglamentación deberá prever niveles diferenciados de acceso a la información y deberes de confidencialidad para los agentes y autoridades que intervengan en su administración, control o consulta.

ARTÍCULO 18.- Obligatoriedad. Todo organismo alcanzado deberá inscribir en el Registro:

a) sistemas de IA en operación;

b) sistemas en prueba piloto o sandbox; y

c) sistemas en proceso de contratación, una vez aprobado el expediente de inicio, en la forma que establezca la reglamentación.

ARTÍCULO 19.- Contenido mínimo público.

El Registro deberá publicar, como mínimo:

a) denominación del sistema y organismo responsable;

b) finalidad y servicio/función pública;

c) clasificación de riesgo y fundamento;

d) proveedor/es y modalidad de contratación;

e) categorías de datos utilizados (sin revelar datos personales ni información sensible);

f) existencia de EIA, auditorías y fecha de última revisión;

g) canales de consulta y reclamo ciudadano; y

h) fecha de alta, versión y estado (en prueba / activo / suspendido / retirado).

ARTÍCULO 20.- Actualización. La información deberá mantenerse actualizada durante el ciclo de vida del sistema.

CAPÍTULO VI

EVALUACIÓN DE IMPACTO ALGORÍTMICO (EIA)

ARTÍCULO 21.- Obligatoriedad. La EIA es obligatoria antes de implementar sistemas de riesgo medio y alto, y deberá actualizarse ante cambios sustanciales de datos, modelo, finalidad, población afectada o desempeño.

ARTÍCULO 22.- Contenido mínimo. La EIA deberá incluir, como mínimo:

a) descripción del sistema, finalidad, alcance y alternativas no algorítmicas consideradas;

b) clasificación de riesgo y justificación;

c) análisis de datos (base jurídica, finalidad, procedencia, calidad, representatividad, minimización, retención, seguridad, confidencialidad y medidas de anonimización, disociación o seudonimización cuando corresponda);

d) análisis de impactos sobre derechos, no discriminación, accesibilidad y debida diligencia;

e) medidas de supervisión humana y posibilidad de revisión/impugnación, sin perjuicio de los recursos administrativos, judiciales, acciones de hábeas data y mecanismos de acceso a la información pública que correspondan;

f) medidas de seguridad, robustez, pruebas y métricas;

g) plan de monitoreo continuo, auditorías e incidentes;

h) evaluación de transparencia y explicabilidad proporcional; y

i) decisión final de aprobación, condiciones y responsables.

ARTÍCULO 23.- Publicidad. Los resultados de la EIA serán públicos mediante el Registro, con versiones resumidas en lenguaje claro, preservando datos protegidos, seguridad y secreto comercial.

ARTÍCULO 24.- Condición de puesta en producción. Ningún sistema de riesgo medio o alto podrá entrar en operación sin EIA aprobada por la máxima autoridad del organismo. En los casos de riesgo alto, deberá contar, además, con dictamen previo, de carácter vinculante, emitido por la Autoridad de Aplicación, conforme el alcance y procedimiento que establezca la reglamentación, pudiendo dicha Autoridad determinar, de manera fundada, que el sistema no sea implementado o puesto en operación.

CAPÍTULO VII

SANDBOX REGULATORIO PROVINCIAL

ARTÍCULO 25.- Creación. Créase el Sandbox Regulatorio Provincial de IA, como entorno controlado para probar soluciones de IA en el Sector Público bajo reglas, límites, monitoreo y plazos definidos.

ARTÍCULO 26.- Finalidad. El Sandbox tendrá por finalidad:

a) validar soluciones con foco en valor público;

b) detectar riesgos tempranos y ajustar salvaguardas; y

c) promover innovación responsable y aprendizaje institucional.

ARTÍCULO 27.- Condiciones mínimas. El ingreso al Sandbox requerirá:

a) objetivo y alcance delimitado;
b) evaluación preliminar de riesgos;
c) medidas de protección de datos y seguridad;
d) supervisión humana; y
e) plazos, métricas y criterio de salida (aprobación, ajuste o descarte).

ARTÍCULO 28.- Publicidad. Los proyectos del Sandbox deberán informarse en el Registro con el nivel de detalle que establezca la reglamentación.

CAPÍTULO VIII

GOBIERNO COMO PLATAFORMA, REUTILIZACIÓN E INTEROPERABILIDAD

ARTÍCULO 29.- Reutilización obligatoria. Los organismos deberán reutilizar componentes, modelos, APIs, plantillas de evaluación, librerías y soluciones ya desarrolladas o adquiridas por el Estado Provincial, cuando sean técnicamente aptas y eficientes, salvo justificación fundada, debidamente documentada y sujeta a revisión conforme lo establezca la reglamentación.

ARTÍCULO 30.- Componentes comunes. La Autoridad de Aplicación promoverá el desarrollo y disponibilidad de componentes comunes, incluyendo:
a) servicios de identidad/autenticación cuando corresponda;
b) catálogos de datos y metadatos;
c) plantillas de EIA y cláusulas modelo; y
d) herramientas de monitoreo y auditoría proporcional.

ARTÍCULO 31.- Articulación con Silicon Misiones. La Autoridad de Aplicación articulará acciones de innovación pública, capacitación, prototipado y transferencia de conocimiento con Silicon Misiones conforme su marco legal vigente.

CAPÍTULO IX

GOBERNANZA INSTITUCIONAL Y RESPONSABLES

ARTÍCULO 32.- Autoridad de Aplicación. El Poder Ejecutivo designará Autoridad de Aplicación en el ámbito del organismo con competencia primaria en transformación digital/innovación pública, sin crear nuevas estructuras, pudiendo

asignar funciones a unidades existentes, y respetando las competencias legalmente asignadas a los organismos de control, asesoramiento jurídico, administración financiera, contratación pública, protección de datos personales y acceso a la información pública.

ARTÍCULO 33.- Funciones. Serán funciones mínimas de la Autoridad de Aplicación:

a) dictar normas complementarias y guías técnicas;

b) administrar el Registro y el Sandbox;

c) emitir estándares mínimos y cláusulas modelo para contratación de IA;

d) coordinar capacitaciones;

e) establecer criterios de interoperabilidad y reutilización;

f) definir lineamientos para auditorías y monitoreo; y

g) elaborar un informe anual público de situación.

ARTÍCULO 34.- Responsable de IA/Datos por organismo. Cada organismo designará un/a Responsable de IA y Datos (función asignada a personal existente), encargado/a de:

a) impulsar cumplimiento de esta ley;

b) coordinar EIA;

c) asegurar actualización del Registro;

d) gestionar incidentes y reportes;

e) actuar como punto de contacto interno y ciudadano.

ARTÍCULO 35.- Coordinación interinstitucional. La Autoridad de Aplicación coordinará con áreas de compras, legales, control interno y las que correspondan, incluyendo, cuando resulte pertinente y conforme sus competencias específicas, a Contaduría General, Fiscalía de Estado, Tribunal de Cuentas, órgano provincial competente en materia de protección de datos personales, áreas de ciberseguridad, acceso a la información pública y demás organismos con competencia específica**,** para integrar requisitos de IA en procedimientos vigentes, evitando duplicaciones.

CAPÍTULO X

CAPACITACIÓN Y DESARROLLO DE CAPACIDADES

ARTÍCULO 36.- Plan de capacitación. La Autoridad de Aplicación implementará un plan anual de capacitación para:

a) compras y contrataciones (cláusulas, evaluación de ofertas, valor público);

b) áreas usuarias (riesgos, supervisión humana, uso responsable);

c) equipos técnicos (seguridad, auditoría, monitoreo); y
d) formación en lenguaje claro para transparencia y rendición de cuentas.

ARTÍCULO 37.- Alfabetización interna. Los organismos deberán asegurar instancias mínimas de formación para quienes operen o decidan con apoyo de sistemas de IA, acorde al riesgo.

CAPÍTULO XI

TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y DERECHOS

ARTÍCULO 38.- Transparencia activa. La información obligatoria del Registro se considera parte de la transparencia activa, sin perjuicio del régimen de acceso a la información pública vigente.

ARTÍCULO 39.- Información al ciudadano. Cuando un sistema de IA de riesgo medio o alto intervenga en la atención, priorización, recomendación o decisión sobre una persona, el organismo deberá informar, en forma clara y accesible:
a) la intervención del sistema;
b) finalidad general;
c) existencia de supervisión humana;
d) vías de consulta, reclamo y revisión; y
e) autoridad u organismo responsable del sistema, cuando corresponda.
La información deberá brindarse sin revelar datos personales de terceros, información sensible, secretos protegidos, información de seguridad, secreto fiscal, comercial, industrial o cualquier otra información exceptuada por la normativa vigente.

ARTÍCULO 40.- Revisión humana. En sistemas de riesgo alto, toda decisión con efecto adverso relevante deberá contar con instancia de revisión humana efectiva conforme procedimientos aplicables. Excepcionalmente, la reglamentación podrá prever supuestos específicos y restrictivos, siempre que no se afecten derechos ni garantías esenciales de las personas involucradas. La revisión humana prevista en este artículo no sustituye ni limita los recursos administrativos, judiciales, acciones de hábeas data, acceso a la información pública u otras vías de impugnación o tutela de derechos previstas en la normativa vigente.

ARTÍCULO 41.- Protección de datos y registros. El tratamiento de datos deberá respetar la normativa provincial aplicable sobre registros, archivos y habeas data, y las reglas de privacidad y seguridad del Estado, así como la Ley Nacional 25.326

de Protección de Datos Personales, la Ley XII Nº 10 de la Provincia de Misiones y los regímenes especiales aplicables en materia de secreto fiscal, sanitario, estadístico, judicial, administrativo, de seguridad, niñez, adolescencia y demás información legalmente protegida.

En particular, deberá asegurarse la licitud del tratamiento, finalidad determinada, minimización, calidad de datos, seguridad, confidencialidad, conservación limitada, trazabilidad de accesos y, cuando corresponda, anonimización, disociación o seudonimización de datos.

ARTÍCULO 42.- Uso de datos para entrenamiento, ajuste o validación de modelos. El uso de datos bajo responsabilidad del Estado provincial para entrenamiento, ajuste, prueba o validación de modelos de IA sólo podrá realizarse cuando exista base jurídica suficiente, finalidad compatible, evaluación de riesgos y medidas adecuadas de seguridad y protección de datos.

Los datos personales o sensibles no podrán ser utilizados para tales fines salvo autorización legal, consentimiento válido cuando corresponda, o aplicación de técnicas de anonimización o disociación que impidan identificar a las personas.

Los contratos con proveedores deberán prohibir el uso de datos, documentos, consultas, resultados o interacciones del Estado provincial para entrenar modelos propios o de terceros, salvo autorización expresa y fundada del organismo competente.

CAPÍTULO XII

MONITOREO, AUDITORÍA Y GESTIÓN DE INCIDENTES

ARTÍCULO 43.- Monitoreo continuo. Los sistemas de riesgo medio y alto deberán contar con monitoreo de desempeño y riesgos, con métricas y umbrales de alerta.

ARTÍCULO 44.- Auditorías. La Autoridad de Aplicación establecerá criterios para auditorías proporcionales. Para riesgo alto, podrá requerir auditorías periódicas y auditorías externas cuando la criticidad lo justifique, las que deberán ser realizadas por equipos o personas con independencia suficiente respecto del proveedor y del equipo responsable de implementación del sistema.

Las auditorías deberán respetar la normativa vigente sobre acceso a la información pública, protección de datos personales, confidencialidad, secreto comercial, seguridad pública, infraestructura crítica y demás restricciones legales aplicables.

ARTÍCULO 45.- Incidentes. Los organismos deberán registrar incidentes relevantes (seguridad, privacidad, sesgos graves, errores sistemáticos, impactos no previstos), con obligación de reportarlos a la autoridad de aplicación en un máximo de 48 horas hábiles. Luego, deberán adoptar medidas correctivas y preventivas, conforme protocolo reglamentario, sin perjuicio de las comunicaciones que correspondan a otros organismos competentes cuando el incidente involucre datos personales, seguridad de la información, infraestructura crítica, secreto fiscal, sanitario, judicial u otra materia especialmente protegida.

ARTÍCULO 46.- Suspensión preventiva. Ante riesgo grave o daño probable, el organismo deberá disponer la suspensión preventiva del sistema y comunicarlo a la Autoridad de Aplicación, dejando constancia en el Registro con el detalle permitido.

CAPÍTULO XIII

RESPONSABILIDADES Y SANCIONES

ARTÍCULO 47.- Responsabilidad. El uso de sistemas de IA no exime responsabilidad administrativa, civil o penal que corresponda a funcionarios, agentes u operadores, ni al proveedor en el marco contractual.

ARTÍCULO 48.- Incumplimientos. Constituyen incumplimientos, según gravedad:

a) operar sistemas de riesgo medio/alto sin EIA;

b) omitir inscripción o falsear información del Registro;

c) impedir auditorías previstas contractualmente;

d) no gestionar incidentes o no aplicar suspensión preventiva cuando corresponda; y

e) contratar sin incorporar requisitos mínimos de pliegos y contrato.

ARTÍCULO 49.- Sanciones administrativas. Sin perjuicio del régimen disciplinario aplicable, podrán imponerse, por la autoridad competente y conforme el procedimiento que corresponda**:** apercibimiento, suspensión de puesta en producción, obligación de remediación, y demás medidas correctivas que establezca la reglamentación.

En contratación, podrán aplicarse sanciones y penalidades contractuales, incluida rescisión por incumplimiento grave, conforme el régimen de contrataciones y las cláusulas contractuales aplicables.

CAPÍTULO XIV

IMPLEMENTACIÓN PROGRESIVA Y DISPOSICIONES TRANSITORIAS

ARTÍCULO 50.- Reglamentación. El Poder Ejecutivo reglamentará la presente ley dentro de los ciento ochenta (180) días desde su publicación.

ARTÍCULO 51.- Implementación por etapas. Establécese una implementación progresiva:

a) etapa I (0–6 meses desde reglamentación): puesta en marcha del Registro; designación de responsables de IA/Datos; guía mínima de clasificación de riesgo; plantillas base de pliegos y EIA;

b) etapa II (6–18 meses): obligatoriedad plena de EIA para nuevos sistemas de riesgo medio/alto; funcionamiento del Sandbox; primeros componentes comunes y lineamientos de interoperabilidad; y

c) etapa III (18–36 meses): auditorías periódicas para sistemas de riesgo alto; consolidación de reutilización obligatoria y evaluación anual.

ARTÍCULO 52.- Regularización de sistemas existentes. Los sistemas de IA ya operativos deberán:

a) inscribirse en el Registro dentro de los noventa (90) días de habilitado;

b) realizar EIA dentro de los doce (12) meses si son de riesgo medio o alto; y

c) adecuar contratos vigentes en la medida legalmente posible (renovaciones, adendas o nuevos procesos).

ARTÍCULO 53.- Financiamiento. Autorizase al Poder Ejecutivo a realizar adecuaciones presupuestarias necesarias para el cumplimiento de la presente, priorizando reutilización de capacidades existentes y cooperación con instituciones públicas y académicas, sin crear estructuras nuevas.

ARTÍCULO 54.- Revisión periódica. La Autoridad de Aplicación deberá elaborar, cada año, un informe de revisión normativa y técnica sobre la implementación de la presente ley, considerando la evolución tecnológica, los estándares nacionales e internacionales, los resultados de auditorías, incidentes registrados, funcionamiento del Registro, experiencia del Sandbox y recomendaciones de mejora. Dicho informe será público, sin perjuicio de las excepciones legales aplicables.

ARTÍCULO 55.- Comuníquese al Poder Ejecutivo.

Cod_Veri:914642

FUNDAMENTOS

El presente proyecto establece el marco rector para el despliegue de la Inteligencia Artificial en la gestión pública provincial, consolidando a Misiones como epicentro de una vanguardia tecnológica con sentido humano.

La Inteligencia Artificial constituye el nuevo lenguaje de la eficacia y la modernización. Sin embargo, su carácter disruptivo y su capacidad de influencia exigen, de manera impostergable, una arquitectura de seguridad robusta que garantice transparencia, equidad y, fundamentalmente, soberanía digital en el siglo XXI. Ante este escenario, esta iniciativa adopta un modelo de gobernanza basado en la inteligencia preventiva, estableciendo una hoja de ruta donde la trazabilidad algorítmica, la auditabilidad técnica y, por, sobre todo, la supervisión humana efectiva, son el eje central de todo el ciclo de vida de los sistemas.

Resulta fundamental reconocer que la incorporación de la inteligencia artificial en el sector público es una realidad ineludible, toda vez que los servidores públicos, quienes elaboran políticas y brindan servicios al ciudadano, ya hacen uso de estas herramientas en su cotidianidad. Por ello, este proceso debe ser ordenado, seguro y ético, garantizando la transparencia, la seguridad de los datos y la mitigación de sesgos, para que la tecnología provea soluciones rápidas, eficientes, integrales e inclusivas que no dejen a nadie afuera.

Si bien la realidad cotidiana demanda soluciones inmediatas para los múltiples desafíos que atraviesan la vida de los misioneros, nuestra responsabilidad como legisladores exige, al mismo tiempo, una mirada estratégica que se anticipe a los escenarios venideros. No podemos permitir que el despliegue de nuevas tecnologías ocurra de manera desordenada o improvisada; es nuestra función indelegable regular su integración en la gestión, estableciendo requisitos claros que aseguren un uso correcto y

responsable. La tecnología, por sí misma, no garantiza el bienestar. Es el diseño institucional, la regulación responsable y el control riguroso lo que permite que estas herramientas actúen como verdaderos vehículos de transformación. Esta ley se erige sobre la convicción de que debemos liderar el despliegue tecnológico, dictando las normas que aseguren que la automatización nunca sustituya el criterio, la responsabilidad y la empatía que demanda el servicio al ciudadano.

Este marco normativo promueve un ecosistema ágil, capaz de integrar evaluaciones de impacto algorítmico (EIA) obligatorias, criterios de interoperabilidad conforme a estándares globales y la implementación de un sandbox regulatorio para el desarrollo de soluciones en entornos controlados. La prioridad absoluta reside en el valor público y en la integridad de los datos de cada misionero, garantizando sistemas robustos, explicables y sujetos a un control permanente que evite sesgos y arbitrariedades.

La presente iniciativa se encuentra alineada con los principales estándares internacionales en materia de gobernanza de la inteligencia artificial. En particular, recepta los principios establecidos en la Recomendación sobre la Ética de la Inteligencia Artificial, aprobada por la UNESCO en el año 2021, que promueve un desarrollo y utilización de la inteligencia artificial centrados en las personas, respetuosos de los derechos humanos, la diversidad y la inclusión. Asimismo, toma como referencia los Principios sobre Inteligencia Artificial de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), adoptados en 2019, que impulsan sistemas confiables, transparentes, seguros y sujetos a supervisión humana. Del mismo modo, incorpora criterios compatibles con el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, basado en un enfoque regulatorio según el nivel de riesgo de los sistemas de inteligencia artificial, así como con la Carta Iberoamericana de Innovación en la Gestión Pública, que promueve la utilización responsable de tecnologías digitales para fortalecer las capacidades institucionales, mejorar la prestación de los servicios públicos y generar mayor valor público.

La implementación de esta normativa reafirma que el futuro no ocurre por azar, sino que se construye con diseño, método y una visión política clara. Misiones lidera una vez más, no solo integrando tecnología de punta, sino definiendo las reglas de juego necesarias para un progreso que es, ante todo, inteligente, inclusivo, audaz y, por sobre todas las cosas, responsable. Al establecer este blindaje ético y técnico, la Provincia garantiza que el camino hacia la digitalización total sea siempre un proceso transparente y al servicio del bienestar de toda la comunidad.

Desde el punto de vista económico y presupuestario, la iniciativa ha sido concebida procurando una implementación gradual y financieramente sostenible. En tal sentido, prevé una aplicación progresiva de las obligaciones que establece, prioriza la reutilización de capacidades institucionales, recursos humanos y soluciones tecnológicas ya existentes en el ámbito de la Administración Pública Provincial, promueve la

cooperación con instituciones públicas y académicas y dispone que la Autoridad de Aplicación sea ejercida por organismos existentes, evitando la creación de nuevas estructuras administrativas. Asimismo, la implementación por etapas y la posibilidad de realizar las adecuaciones presupuestarias necesarias permitirán instrumentar la presente ley de manera ordenada, eficiente y compatible con las disponibilidades financieras de la Provincia.

Por las razones expuestas, es que solicito a mis pares el acompañamiento para la aprobación del presente proyecto de ley.

Cod_Veri:914642