Deloitte.

El nuevo mapa regulatorio de la Inteligencia Artificial en Latinoamérica

Introducción

La Inteligencia Artificial (IA) representa uno de los principales motores de transformación tecnológica, económica, social y organizacional a nivel global. Su capacidad para procesar grandes volúmenes de información, automatizar decisiones complejas y generar nuevos modelos de negocio ha acelerado su adopción en prácticamente todos los sectores. No obstante, este mismo potencial ha puesto en evidencia riesgos significativos asociados con la seguridad, la privacidad, la discriminación algorítmica, la desinformación y la erosión de derechos fundamentales, lo que ha detonado un amplio debate sobre la necesidad de regular su desarrollo y su uso.

Latinoamérica atraviesa una fase decisiva de transición: el paso desde iniciativas estratégicas y marcos éticos no vinculantes hacia esquemas regulatorios más formales, con distintos niveles de madurez, alcance y capacidad sancionatoria. Aunque la región todavía presenta asimetrías importantes frente a jurisdicciones como la Unión Europea o Estados Unidos, comienza a consolidarse un patrón de convergencia normativa influenciado por estándares internacionales, organismos multilaterales y experiencias regulatorias más avanzadas.

Este proceso no implica únicamente la creación de nuevas leyes, sino también una redefinición más amplia de la relación entre innovación, confianza y supervisión. Sobre esta base, resulta fundamental analizar cómo se configura el marco regulatorio de la IA en Latinoamérica, cuáles son sus principales rasgos distintivos y qué implicaciones estratégicas plantea para las organizaciones que desarrollan, implementan o utilizan sistemas de Inteligencia Artificial en la región.

Actualización editorial

Posterior al cierre editorial de este documento, el Proyecto de Ley 043 de 2025 Senado / 324 de 2025 Cámara, que proponía establecer un marco regulatorio para la Inteligencia Artificial en Colombia, concluyó su trámite legislativo sin ser aprobado y fue archivado por el Congreso*. En consecuencia, las referencias contenidas en este estudio respecto de dicha iniciativa corresponden al estado del proceso legislativo vigente durante la etapa de investigación y elaboración del análisis. Este hecho no modifica las conclusiones centrales del documento, cuyo propósito es examinar las tendencias regulatorias que están configurando la gobernanza de la IA en Latinoamérica. De hecho, la evolución del caso colombiano refuerza uno de los principales hallazgos del estudio: la regulación regional es dinámica, heterogénea y sujeta a cambios derivados del debate legislativo y de la consolidación institucional en cada país.

*Congreso de la República de Colombia, "Ficha del proyecto de ley 043/2025S", 2026. https://www.camara.gov.co/inteligencia-artificial

El paralelismo histórico de la regulación tecnológica

La discusión actual sobre la regulación de la IA no es un fenómeno aislado ni completamente nuevo. Por el contrario, se inscribe en una secuencia histórica bien documentada: cada vez que una tecnología de uso transversal ha redefinido la forma de producir, organizar el trabajo o intercambiar valor, los marcos regulatorios han avanzado con cautela, generalmente después de que sus efectos —positivos y negativos— se hicieran visibles. Así ocurrió con la máquina de vapor durante la Revolución Industrial, con la electrificación de las economías a comienzos del siglo XX y, más recientemente, con la expansión de Internet y las tecnologías digitales.

En todos estos casos, el patrón fue similar. La innovación emergió más rápido que la capacidad institucional para comprenderla y gobernarla. Las primeras fases estuvieron marcadas por una regulación mínima o inexistente, impulsada tanto por la voluntad de no frenar el progreso como por la dificultad de anticipar impactos sistémicos. Solo cuando comenzaron a manifestarse externalidades claras —riesgos para la seguridad, concentraciones de poder económico, asimetrías de información o afectaciones a derechos fundamentales— los gobiernos adoptaron un papel más activo e intervinieron de forma decidida. Incluso entonces, la regulación no se dirigió a la tecnología en abstracto, sino a sus usos específicos: la seguridad industrial en el caso del vapor, la provisión del servicio público en la electricidad, o la protección de datos y de menores en el entorno digital.

Hoy, la IA reproduce esa misma lógica, aunque a una velocidad inédita. Su carácter de tecnología de propósito general —capaz de integrarse en sectores tan diversos como finanzas, salud, educación, manufactura o servicios públicos— hace inviable una definición regulatoria única y homogénea. Por ello, los marcos más recientes han optado por esquemas basados en principios y riesgos, diferenciando entre casos de uso de bajo impacto y aquellos con implicaciones más profundas en términos de seguridad, derechos o estabilidad económica. Se trata de una evolución que no representa una ruptura con la historia, sino una reiteración de ella: regular no para detener la innovación, sino para encauzarla y controlarla.

Para Latinoamérica, este paralelismo histórico es especialmente relevante. La región enfrenta el desafío de construir marcos regulatorios para la IA en un contexto de heterogeneidad institucional, brechas de capacidad gubernamental y distintos niveles de madurez digital. Sin embargo, también cuenta con una ventaja clave: no parte de cero. La experiencia acumulada en otras tecnologías transformadoras —y, más recientemente, en la regulación digital— ofrece lecciones claras sobre qué evitar y qué priorizar. En este contexto, el foco se desplaza hacia la forma en que la regulación puede habilitar una adopción responsable de la IA, fortalecer la confianza y, al mismo tiempo, preservar su capacidad de impulsar el desarrollo económico y social en Latinoamérica.

La influencia de marcos globales en la regulación de la IA

La regulación de la Inteligencia Artificial ha entrado en una fase de mayor estructuración a nivel global, caracterizada por el tránsito desde principios éticos no vinculantes hacia marcos normativos y de gobernanza más [CL1.1]definidos, observándose diferencias significativas entre jurisdicciones. A nivel internacional, se observa una convergencia progresiva en torno a algunos ejes comunes: la necesidad de preservar el control humano, garantizar la transparencia y la explicabilidad, proteger la privacidad y los datos personales, mitigar sesgos y discriminación, y asegurar la rendición de cuentas a lo largo de todo el ciclo de vida de los sistemas de IA.

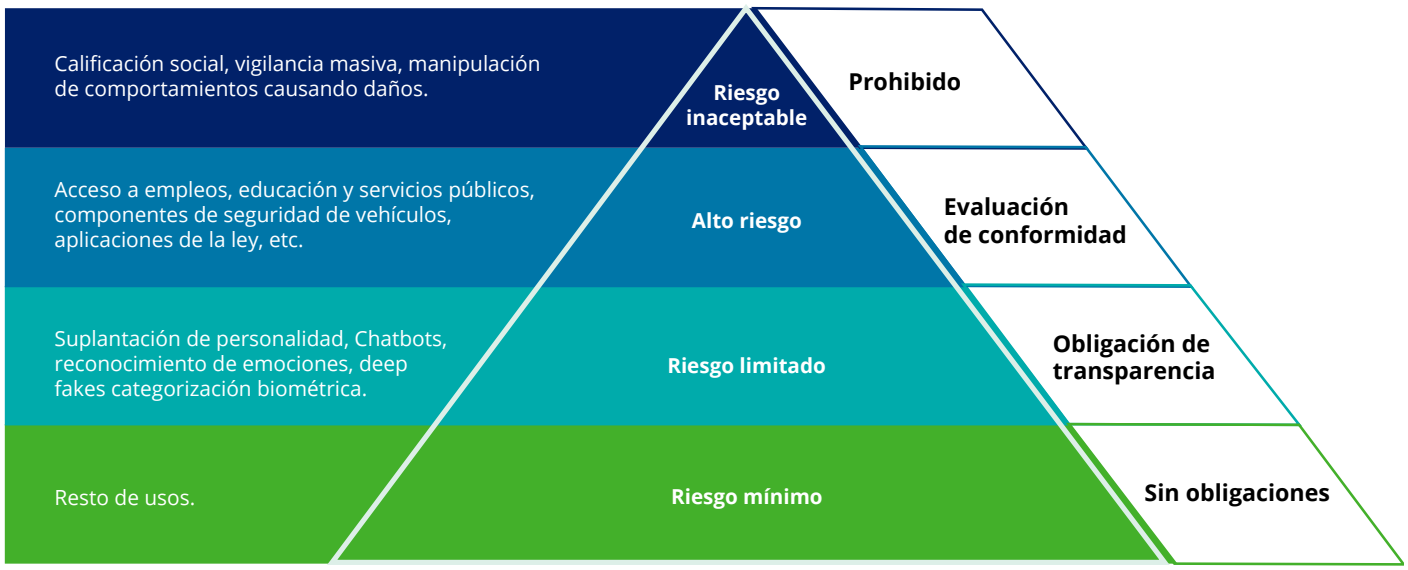
La Unión Europea (*UE*) ha marcado un hito en la gobernanza de la IA con la aprobación de la *Ley de Inteligencia Artificial de la Unión Europea* (AI Act), considerada el marco regulatorio más completo y avanzado hasta la fecha. No obstante, su implementación continúa desarrollándose de forma progresiva, con disposiciones que entrarán en vigor de manera escalonada y cuya aplicación práctica todavía está sujeta a criterios interpretativos, lineamientos técnicos y ajustes regulatorios posteriores. Aun así, la AI Act se ha consolidado como un referente global por su alcance extraterritorial y por ofrecer una arquitectura regulatoria replicable y adaptable a otros entornos institucionales y regulatorios, con distintos niveles de madurez, capacidades y marcos jurídicos[1].

El marco integral que esa ley establece está destinado a clasificar, supervisar y limitar los usos de la IA, con el objetivo de promover una tecnología confiable y centrada en las personas, protegiendo la seguridad, los derechos fundamentales, la democracia y el medio ambiente. La norma se aplica a actores dentro y fuera de la UE siempre y cuando los sistemas de IA, o los resultados que generan, se utilicen en territorio europeo. Además, introduce el concepto de "incidente grave" como un mecanismo clave para reforzar la supervisión frente a impactos críticos.

El riesgo es el eje que articula el enfoque regulatorio de la AI Act. A partir de esta lógica, la ley distingue cuatro niveles de impacto: inaceptable, alto, limitado y mínimo, que determinan el grado de intervención normativa aplicable a cada sistema de IA (gráfico 1). Este marco combina prohibiciones claras, exigencias de supervisión humana, gestión de riesgos y trazabilidad, con un régimen sancionador robusto que contempla multas de hasta 35 millones de euros o 7% de la facturación global anual, consolidando un modelo orientado a canalizar los beneficios de la IA y contener sus riesgos.

Gráfico 1. Niveles de riesgo

(Ley de Inteligencia Artificial de la Unión Europea)



En contraste con el modelo europeo, la gobernanza de la IA en Estados Unidos se caracteriza por una combinación de desregulación a nivel federal, mandatos de seguridad impulsados mediante órdenes ejecutivas y una fuerte dependencia de estándares técnicos y autorregulación sectorial. La evolución reciente del marco estadounidense —incluyendo las órdenes ejecutivas emitidas y revisadas durante 2025— refleja un esfuerzo por equilibrar liderazgo tecnológico, seguridad nacional y competitividad económica, lo que privilegia mecanismos flexibles frente a esquemas regulatorios centralizados[2].

Más allá de estos modelos, otras jurisdicciones han comenzado a desarrollar enfoques regulatorios diferenciados. Japón, por ejemplo, ha privilegiado esquemas basados en principios, gobernanza corporativa y autorregulación guiada; Reino Unido ha optado por una supervisión distribuida a través de reguladores sectoriales existentes; mientras que Singapur y Canadá han impulsado modelos pragmáticos orientados a la gestión de riesgos y la innovación responsable. Estas experiencias evidencian que no existe un único modelo de regulación de la IA, sino trayectorias regulatorias diversas y adaptadas a las capacidades institucionales y prioridades económicas de cada jurisdicción[3, 4, 5, 6].

En un plano complementario, el estudio *AI for Good Impact Report 2025*, desarrollado por la Unión Internacional de Telecomunicaciones (*ITU*, por sus siglas en inglés) en colaboración con Deloitte, destaca el fortalecimiento de la gobernanza multilateral de la Inteligencia Artificial: las Naciones Unidas han creado mecanismos orientados a coordinar enfoques regulatorios, anticipar riesgos sistémicos y promover una IA alineada con los derechos humanos y el desarrollo sostenible[7]. De igual manera, el reporte pone de relieve instrumentos como el Pacto Digital Global, las recomendaciones de la OCDE, la Recomendación de la UNESCO sobre la Ética de la IA y el Convenio Marco del Consejo de Europa sobre IA configuran una base normativa internacional cada vez más coherente, aunque todavía fragmentada en su implementación[8].

Sobre este marco multilateral, la ONU advierte que, sin una gobernanza global efectiva, la IA puede profundizar desigualdades y concentrar beneficios en pocos actores. Para evitarlo, propone una arquitectura internacional de gobernanza basada en siete ejes[9]:

1. Un panel científico independiente para evaluar riesgos y tendencias.
2. Un diálogo político global para coordinar enfoques regulatorios.
3. La armonización de estándares técnicos.
4. El fortalecimiento de capacidades en países con menor desarrollo tecnológico.
5. Un fondo internacional para cerrar brechas de acceso.
6. Un marco global de datos que promueva usos responsables y representativos.
7. Una oficina de IA dentro de la ONU que coordine estos mecanismos.

Por su parte, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) establece un marco de referencia para una IA confiable, orientado a promover el bienestar, el crecimiento inclusivo, la sostenibilidad y el respeto por los derechos humanos y los valores democráticos. A partir de estos principios, la Recomendación del Consejo de la OCDE sobre Inteligencia Artificial formula cinco líneas de acción de política pública[10]:

1. Impulsar la inversión en investigación y desarrollo responsable.
2. Fomentar ecosistemas de IA inclusivos con infraestructura, datos y mecanismos de intercambio ético.
3. Construir marcos de gobernanza y regulación interoperables que habiliten la innovación y la escalabilidad.
4. Desarrollar capacidades humanas y gestionar de forma justa las transiciones laborales.
5. Fortalecer la cooperación internacional mediante la coordinación de políticas, estándares y buenas prácticas.

Antes de analizar el estado regulatorio de la IA en Latinoamérica, resulta importante distinguir entre los distintos tipos de instrumentos normativos que actualmente coexisten en la región. Por un lado, comienzan a surgir marcos regulatorios específicos de IA con efectos jurídicamente vinculantes; por otro, persisten proyectos legislativos en discusión, estrategias nacionales de IA, lineamientos éticos y esquemas de *soft law* sin capacidad sancionatoria directa. A ello se suma un conjunto amplio de regulaciones preexistentes —como normas de protección de datos, ciberseguridad, derechos del consumidor, competencia económica, antidiscriminación y responsabilidad civil— que resultan ya aplicables al desarrollo y uso de sistemas de Inteligencia Artificial.

Esta distinción es relevante porque evidencia que la IA no parte de un vacío normativo absoluto, sino de un ecosistema regulatorio fragmentado que actualmente atraviesa un proceso de reorganización, formalización y adaptación frente a nuevas capacidades tecnológicas.

Cómo evoluciona la regulación en Latinoamérica

Sobre la base internacional antes descrita, la regulación emergente de la Inteligencia Artificial en Latinoamérica muestra una clara convergencia hacia esquemas basados en riesgos, tomando como referencia la *AI Act* para clasificar los sistemas de IA en función de su impacto potencial sobre las personas, la sociedad y los derechos fundamentales.

Sin embargo, el nivel de desarrollo regulatorio aún es heterogéneo. Actualmente, Perú y El Salvador representan los casos más avanzados de institucionalización normativa en la región, al contar con legislación específica de IA ya aprobada y vigente. En ambos casos, el objetivo ha sido establecer capacidades iniciales de gobernanza, institucionalidad y coordinación pública para impulsar el desarrollo tecnológico bajo principios de uso responsable.

En contraste, países como Chile, Colombia, Brasil y México avanzan en discusiones legislativas y proyectos regulatorios que, aunque reflejan una tendencia regional clara hacia modelos basados en riesgos, todavía se encuentran sujetos a debate parlamentario, ajustes institucionales y definiciones sobre capacidades de supervisión y ejecución. Por ello, más que representar un inventario definitivo de regulación regional, estas iniciativas constituyen una fotografía representativa de las discusiones regulatorias actualmente en desarrollo en Latinoamérica.

En términos generales, los escasos marcos regulatorios latinoamericanos tienden a distinguir entre usos prohibidos por representar riesgos inaceptables, aplicaciones de alto riesgo sujetas a controles reforzados, usos de riesgo limitado con obligaciones de transparencia y aplicaciones de riesgo mínimo que permanecen mayormente sin regulación específica.

Para las organizaciones, el enfoque basado en niveles de riesgo y clasificación de usos desplaza el foco hacia la identificación de la naturaleza y clasificación de los sistemas de IA que utilizan —por ejemplo, si se trata de modelos generativos, sistemas de automatización de decisiones o aplicaciones catalogadas como de alto riesgo—, así como de su finalidad, los datos que los sustentan y el nivel de impacto asociado sobre personas, operaciones o derechos fundamentales. La gestión del riesgo de los sistemas de IA se convierte así en un componente central del cumplimiento normativo y del gobierno corporativo.

Para dimensionar este tránsito en la región, la siguiente línea de tiempo resume la evolución de las principales iniciativas de gobernanza de IA en Latinoamérica, desde estrategias nacionales y marcos éticos hasta proyectos legislativos y normas con efectos vinculantes. Su objetivo es ofrecer una lectura cronológica del ritmo y la secuencia de adopción (más que un inventario por país); el detalle comparativo de instrumentos, estatus y autoridades se presenta en una tabla posterior.

Evolución de marcos de IA relevantes en Latinoamérica

(*Línea de tiempo regional de iniciativas de Ley y leyes aprobadas*)

A partir de esa evolución, y en paralelo al paso desde iniciativas estratégicas hacia instrumentos más formales, los marcos regulatorios latinoamericanos comparten un énfasis creciente en la gobernanza de la IA a lo largo de todo su ciclo de vida. Esto incluye obligaciones relacionadas con la calidad y la trazabilidad de los datos, la transparencia de los sistemas, la explicabilidad de las decisiones automatizadas y la existencia de mecanismos efectivos de supervisión humana.

La protección de datos personales aparece como un eje transversal. En muchos casos, las obligaciones asociadas al uso de IA se articulan directamente con los regímenes de protección de datos ya existentes, lo que refuerza la exigencia de privacidad desde el diseño, minimización de datos y control sobre inferencias sensibles. En Colombia, por ejemplo, se exige evaluar la representatividad y calidad de los datos como parte de los estudios de impacto; en Perú, la privacidad se eleva a principio rector del uso de IA; y en Chile, la autoridad de protección de datos asume un rol central en la fiscalización de sistemas de alto riesgo.

Asimismo, la prevención de sesgos y discriminación representa ya una preocupación regulatoria explícita. Los proyectos normativos analizados reconocen que, en contextos de alta desigualdad estructural, la IA puede amplificar exclusiones existentes, particularmente en sectores como finanzas, empleo, educación y acceso a servicios públicos.

En paralelo, la discusión regulatoria en Latinoamérica comienza a incorporar una dimensión adicional: el papel gubernamental no solo como regulador de la IA, sino también como usuario intensivo de esta tecnología. Diversos gobiernos de la región evalúan o implementan sistemas de IA para automatizar trámites, fortalecer la seguridad pública, optimizar servicios ciudadanos, priorizar recursos o mejorar capacidades de fiscalización y supervisión. Si bien este proceso puede generar ganancias importantes en eficiencia operativa y capacidad institucional, también incrementa la preocupación sobre vigilancia, privacidad, sesgos algorítmicos y automatización de decisiones con impacto sobre derechos fundamentales.

Para el sector privado, esta evolución tiene implicaciones directas. A medida que las instituciones públicas adopten IA en ámbitos sensibles —como contratación pública, supervisión regulatoria, servicios financieros, salud o seguridad—, aumentarán las exigencias relacionadas con trazabilidad, calidad de datos, transparencia algorítmica y mecanismos de explicabilidad para las empresas que desarrollen, implementen o provean estas tecnologías. En consecuencia, el uso gubernamental de IA podría convertirse en un acelerador indirecto de estándares regulatorios y de cumplimiento para el ecosistema empresarial.

Tabla comparativa. Marcos regulatorios y proyectos nacionales recientes en Latinoamérica
(Lectura por país)

País	Marco reciente	Tipo	Estado	Autoridad u órgano previsto
Argentina	Responsabilidad algorítmica y promoción de la robótica, algoritmos verdes e inteligencia artificial en la República Argentina[11].	Proyecto de ley.	Presentado (marzo 2024).	Consejo Asesor de IA y mecanismos de certificación/registro de riesgos, según el proyecto.
Brasil	PL 2338/2023 (y sustitución consolidada CTIA)[12].	Proyecto de ley.	Aprobado por el Senado y remitido a la Cámara de Diputados (marzo 2025).	Sistema Nacional de Regulación y Gobernanza de IA (SIA), con autoridad competente y autoridades sectoriales.[13]
Colombia	Proyecto de Ley 043-2025 Senado / 324-2025 Cámara (texto propuesto para primer debate)[14].	Proyecto de ley.	En trámite con ponencia positiva (diciembre 2025) y fe de erratas (febrero 2026).	Autoridad nacional liderada por MinCiencias y coordinación institucional; inspección y vigilancia conforme competencias (incl. SIC para datos/ consumo/competencia).
Costa Rica	Estrategia Nacional de Inteligencia Artificial (documento oficial)[15].	Estrategia nacional.	Documento de política pública (sin fuerza sancionatoria directa).	Liderazgo institucional desde el Ejecutivo/ sector digital (según el documento).
Chile	Boletín 16821-19 (refundido con 15869-19)[16].	Proyecto de ley.	Segundo trámite constitucional (mayo 2024).	Fiscalización a cargo de la Agencia de Protección de Datos Personales según la propuesta.
El Salvador	Ley de Fomento a la Inteligencia Artificial y Tecnologías Similares (Decreto 234)[17].	Ley nacional.	Vigente.	Agencia Nacional de Inteligencia Artificial (ANIA).
México	Ley Nacional de Inteligencia Artificial[18].	Iniciativa / proyecto.	Presentada (febrero 2026).	Autoridad propuesta: creación de la Agencia Reguladora del Desarrollo, Uso y Aplicación de la IA (como autoridad central con facultades normativas, de supervisión y sanción).
Perú	Ley 31814 (julio 2023) y Decreto Supremo 115-2025-PCM (septiembre 2025)[19].	Ley + reglamento[20].	Vigentes.	Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno y Transformación Digital.
Uruguay	Estrategia Nacional de IA 2024-2030 (enfoque de desarrollo y uso responsable)[21].	Estrategia nacional.	Documento de política pública vigente como hoja de ruta nacional.	Gobernanza desde la institucionalidad digital del Estado (según la estrategia).

El desafío de gestionar riesgos en entornos impulsados por IA

Un rasgo común en Latinoamérica es que la gobernanza de la Inteligencia Artificial se apoya en capacidades limitadas de *enforcement*. Por ahora, en la mayoría de los países no existen autoridades especializadas en supervisión del uso de la IA; en su lugar, el control recae en instituciones preexistentes —como agencias de transformación digital, ministerios sectoriales o autoridades de protección de datos. Este enfoque favorece una implementación gradual, pero también incrementa el riesgo de fragmentación institucional y vacíos regulatorios.

Ese diseño institucional está estrechamente vinculado a desafíos estructurales de la región, como las brechas digitales, la desigualdad socioeconómica, la debilidad institucional y la dependencia tecnológica. En este contexto, la preocupación regulatoria se concentra en ámbitos donde la IA puede amplificar exclusiones persistentes, como los sesgos algorítmicos, el uso indebido de datos personales, la vigilancia, la desinformación y la automatización de decisiones en servicios públicos. Como respuesta, los marcos emergentes priorizan principios transversales —transparencia algorítmica, supervisión humana, evaluación previa de impactos— y buscan alinearse con estándares internacionales promovidos por la UNESCO y la OCDE.

Pese a estas convergencias, el grado de desarrollo de los regímenes sancionatorios introduce diferencias relevantes entre países. Mientras algunas jurisdicciones avanzan hacia esquemas con multas significativas, suspensión de actividades o bloqueo de sistemas, otras continúan privilegiando enfoques basados en principios, gobernanza y certificación, apoyándose en marcos administrativos o sectoriales existentes. En conjunto, el panorama latinoamericano muestra una homogeneidad creciente en los principios y obligaciones sustantivas, pero una heterogeneidad marcada en la operatividad del *enforcement*, particularmente en la capacidad técnica de auditoría y supervisión de sistemas complejos de IA. Esta brecha refuerza la necesidad de que las organizaciones desarrollen modelos sólidos de gobernanza interna, más allá del cumplimiento mínimo exigido por la norma.

Para las organizaciones, los riesgos asociados con la IA ya no se limitan a escenarios hipotéticos de regulación futura. Incluso en ausencia de legislación específica en varios países, las empresas enfrentan riesgos legales y regulatorios inmediatos derivados de normas existentes en materia de privacidad, protección al consumidor, propiedad intelectual, ciberseguridad, competencia económica y responsabilidad civil.

A ello se suman riesgos de cumplimiento futuro vinculados con la aceleración regulatoria observada en distintos mercados; riesgos operativos y de gobernanza relacionados con errores algorítmicos, falta de supervisión humana o dependencia excesiva de terceros; así como riesgos reputacionales derivados de sesgos, desinformación, uso indebido de datos o decisiones automatizadas percibidas como injustas.

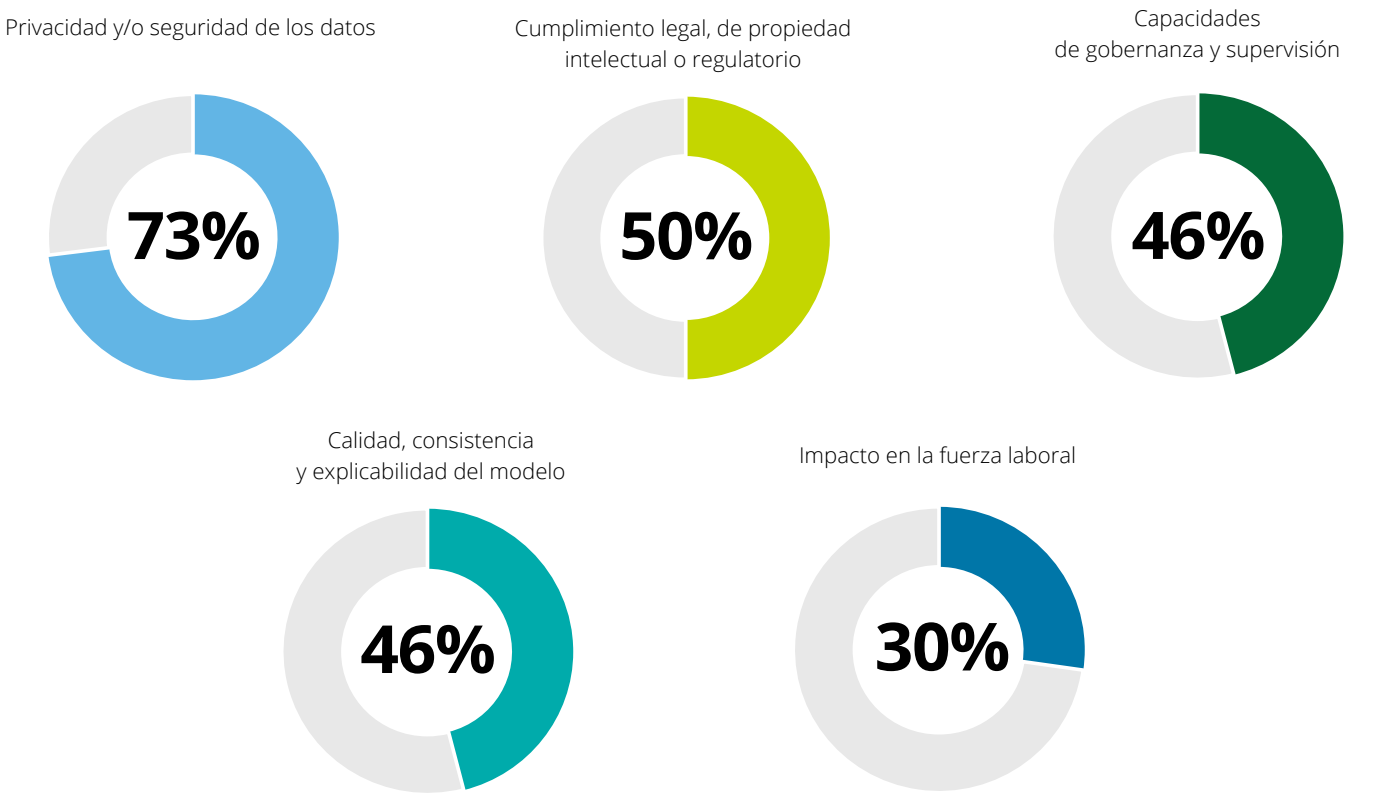
En este entorno, la exposición regulatoria comienza a depender no solo del tipo de tecnología utilizada, sino también del contexto de uso, la criticidad del proceso automatizado y el impacto potencial sobre personas, operaciones o derechos fundamentales.

Como se ha señalado previamente, el enfoque basado en riesgos se consolida también en el contexto latinoamericano. En este escenario, el énfasis regulatorio comienza a concentrarse en los sistemas clasificados como de alto riesgo, desplazando el foco desde la mera adopción de políticas internas hacia la capacidad de demostrar cumplimiento verificable a lo largo de todo el ciclo de vida de la IA: desde el diseño y entrenamiento, hasta el despliegue, monitoreo continuo y eventual retiro de los sistemas.

Cada vez es más patente que los reguladores exigirán evidencia auditable sobre cómo funcionan los modelos, qué datos utilizan, quién supervisa sus resultados y qué mecanismos existen para corregir errores o impugnar decisiones automatizadas. Esto implica desarrollar inventarios de sistemas, clasificaciones de riesgo, registros de cambios, documentación técnica, mecanismos de supervisión humana y procesos claros de reclamación.

Deloitte llevó a cabo una encuesta a nivel global en la que participaron poco más de tres mil líderes empresariales con el objetivo de conocer cómo las organizaciones han adoptado IA en sus operaciones cotidianas. Entre los hallazgos que destaca el estudio, se señala que los riesgos de IA que más preocupan a las empresas están relacionados con la gobernanza. La privacidad y seguridad de los datos encabeza la lista con 73% y, en segundo lugar, 50% identifica como preocupación central los riesgos legales, de propiedad intelectual y de cumplimiento regulatorio (Gráfico 2)[22].

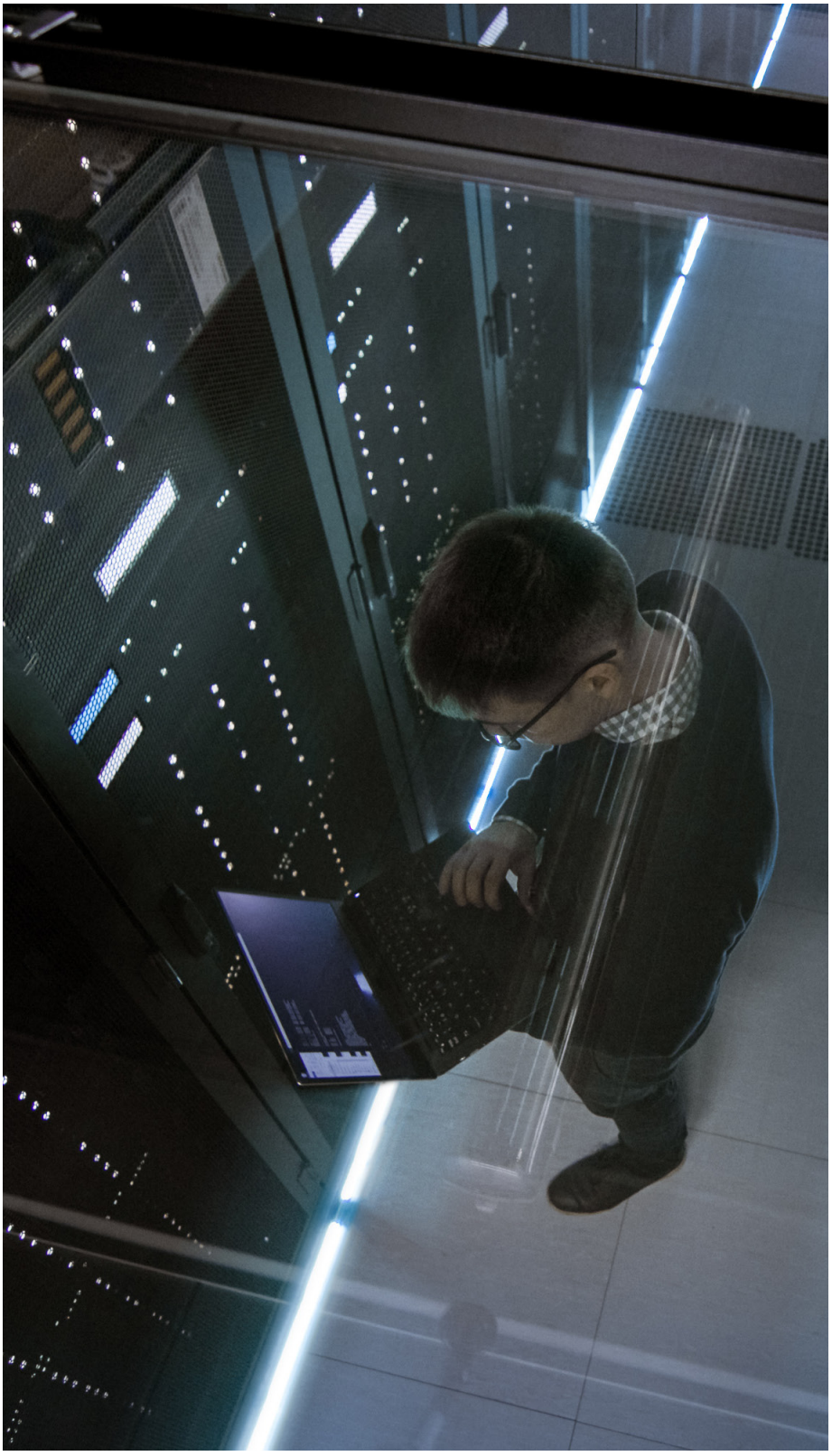
Gráfico 2. Los riesgos más preocupantes de la IA
(Porcentajes a nivel global)



En conjunto, estos hallazgos sugieren que los riesgos de la IA no son exclusivamente tecnológicos. También abarcan dimensiones legales, operativas, reputacionales y humanas. Por ello, las organizaciones que aspiren a escalar el uso de IA de manera sostenible deberán fortalecer sus capacidades de gobernanza, ciberseguridad, cumplimiento y supervisión antes de acelerar su adopción.

Desde esta perspectiva de riesgo ampliado, la ciberseguridad adquiere un papel central en la gobernanza de la Inteligencia Artificial, pues amenazas como *data poisoning*, *prompt injection*, robo o extracción de modelos, así como la dependencia excesiva de terceros, obligan a integrar la IA dentro de los marcos tradicionales de gestión de riesgos de ciberseguridad. Esta convergencia entre ciberseguridad e IA ha incrementado de forma significativa los riesgos financieros y operativos para las organizaciones: a nivel global, la actividad delictiva digital genera pérdidas comparables a las de grandes sectores económicos, no solo por fraude o robo de información, sino también por costos de recuperación, sanciones regulatorias y daños reputacionales. En Latinoamérica, aunque el impacto económico agregado sea menor, el crecimiento sostenido y la mayor sofisticación de los ataques convierten a la región en un objetivo cada vez más relevante, especialmente en sectores críticos y en entornos institucionales en proceso de consolidación.

A ello se suma el creciente riesgo asociado con desinformación, contenido sintético y *deepfakes*. Las nuevas iniciativas regulatorias comienzan a incorporar obligaciones de etiquetado y divulgación para contenidos generados artificialmente, particularmente por los riesgos de fraude, suplantación de identidad, manipulación de procesos democráticos y erosión de la confianza pública.



Implicaciones estratégicas para las organizaciones

En este entorno regulatorio en progreso, el marco normativo de la IA adquiere una dimensión claramente estratégica, más allá del cumplimiento estrictamente legal. Las empresas que operan en múltiples países de Latinoamérica enfrentan un mosaico normativo en evolución, con distintos niveles de exigencia, autoridades competentes y mecanismos de sanción. Intentar gestionar este escenario de forma fragmentada, país por país, incrementa los costos y la complejidad del cumplimiento.

A ello se suma un desafío estructural: las brechas en capacidades digitales e infraestructura tecnológica existentes en Latinoamérica. La disponibilidad desigual de conectividad, capacidad de cómputo, centros de datos, talento especializado y ecosistemas de datos limita la velocidad de adopción de IA entre países, industrias y organizaciones. Mientras algunos mercados avanzan hacia implementaciones más sofisticadas apoyadas en infraestructura digital madura, otros enfrentan restricciones operativas y regulatorias que dificultan escalar iniciativas de IA de manera consistente.

Estas diferencias podrían profundizar asimetrías competitivas dentro de la región, particularmente en sectores intensivos en datos y automatización. Asimismo, la creciente discusión sobre soberanía tecnológica y localización de infraestructura podría incrementar la presión sobre las empresas para adaptar arquitecturas, almacenamiento y procesamiento de datos a requisitos regulatorios locales, elevando la complejidad operativa y los costos de cumplimiento multinacional.

Ante este contexto de capacidades desiguales y creciente fragmentación regulatoria, la tendencia sugiere que la estrategia más eficaz es construir un núcleo regional de gobernanza de IA, alineado con estándares internacionales y marcos de gestión de riesgos ampliamente aceptados —como la norma *ISO/IEC 42001*, que establece un sistema estructurado para la gestión y supervisión de la Inteligencia Artificial—[23], que luego pueda adaptarse a las particularidades regulatorias locales.

En este sentido, la gobernanza de la IA se perfila como un diferenciador competitivo: las organizaciones que invierten de forma temprana en control, trazabilidad y supervisión cuentan con mayores capacidades para escalar el uso de la tecnología con confianza y resiliencia.

Conclusión

La regulación de la Inteligencia Artificial en Latinoamérica ya no es un escenario hipotético, sino una realidad en proceso de consolidación. Aunque los avances presentan ritmos desiguales, el patrón es claro: un enfoque basado en riesgos, un mayor énfasis en la protección de derechos fundamentales, una integración progresiva con la gobernanza de datos y un fortalecimiento paulatino de los regímenes sancionatorios. Este movimiento responde tanto a la presión internacional como a la necesidad interna de asegurar que la adopción de la IA genere valor sin profundizar brechas sociales ni erosionar la confianza pública.

No obstante, el mayor desafío no es la ausencia total de regulación, sino la coordinación regional y la coherencia normativa. Existe un consenso creciente sobre la conveniencia de armonizar marcos regulatorios, evitar una proliferación desordenada de leyes nacionales y construir capacidades institucionales que permitan una implementación efectiva. En este sentido, Latinoamérica parece avanzar hacia un modelo de gobernanza de la IA pragmático y adaptativo, que busca aprender de las experiencias europeas sin replicarlas de forma automática y que equilibra la necesidad de protección con el objetivo de no frenar la adopción tecnológica en economías con procesos de transformación digital.

Para las organizaciones, el desafío no radica únicamente en cumplir con nuevas obligaciones normativas, sino mucho más en integrar la IA de manera responsable y controlada dentro de su modelo de negocio y de gobierno corporativo. En este escenario, el desempeño sostenible no lo marcará la intensidad de adopción regulatoria, sino la solidez con la que las compañías e instituciones adoptan desde la convicción un marco de IA segura, responsable y ética.

Referencias

1. Unión Europea, "Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de IA)", 2024. https://artificialintelligenceact.eu/es/chapter/1/
2. United States Government, *"Removing Barriers to American Leadership in Artificial Intelligence"*, 2025. https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence
3. Regulations. AI, *"Japan - AI Regulatory Framework"*, 2026. https://regulations.ai/regulations/japan-summary
4. Secretary of State for Science, Innovation and Technology, "*A pro-innovation approach to AI regulation*", 2023. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#executive-summary
5. Infocomm Media Development Authority, *"Model AI Governance Framework for Agentic AI"*, 2026. https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf
6. AI Govenance, *"Canada's AI Governance Landscape"*, 2025. https://aigovernance.ca/canada
7. AI for Good & Deloitte, *"AI for Good Impact Report 2025 – 2nd Edition"*, 2025. https://aiforgood.itu.int/newsroom/publications-and-reports/#pubid-49585
8. UNESCO. "Recomendación sobre la ética de la inteligencia artificial (SHS/BIO/PI/2021/1)", 2022. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa
9. United Nations, *"Governing AI for Humanity: Final Report"*, 2024. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf
10. Organisation for Economic Co-operation and Development, *"Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)"*, 2019. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
11. Diputados Argentina, "Proyecto de Ley: responsabilidad algorítmica y promoción de la robótica, algoritmos verdes e inteligencia artificial en la república argentina", 2024. https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/0805-D-2024.pdf
12. Senado Federal, "*Projeto de Lei n° 2338*", 2023. https://www25.senado.leg.br/web/atividade/materias/-/materia/157233
13. Senado Federal, *Parecer (SF) Nº 1*, 2024. https://legis.senado.leg.br/sdleg-getter/documento?disposition=inline&dm=9858756&ts=1764601035552&ts=1764601035552

Referencias

14. Congreso de la república de Colombia, Informe de ponencia positiva para primer debate al proyecto de ley número 43 de 2025 senado, 324 de 2025 cámara, 2025. https://normograma.com/legibus/legibus/gacetas/2025/GC_2348_2025.pdf

15. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, "Estrategia Nacional de Inteligencia Artificial 2024-2027", 2024. https://www.camtic.org/wp-content/uploads/2024/04/Estrategia-Nacional-de-Inteligencia-Artificial-Version-21.03.24-Para-consulta-pu%CC%81blica.pdf

16. Cámara de Diputadas y Diputados de Chile. (2024). Proyecto de ley que regula los sistemas de inteligencia artificial (Boletín 16821 19). https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmID=17429&prmBOLETIN=16821-19

17. Asamblea Legislativa, Ley de fomento a inteligencia artificial y tecnologías, 2025. https://www.asamblea.gob.sv/leyes-y-decretos/view/6137

18. Senado de la República, "Proyecto de decreto por el que se expide la Ley Nacional de Inteligencia Artificial", 2026. https://www.senado.gob.mx/66/gaceta_del_senado/documento/156513

19. Perú, Congreso de la República, "Ley N.° 31814: Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país", 2023. https://cdn.www.gob.pe/uploads/document/file/5038703/ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-fav-ley-n-31814.pdf

20. Gobierno de Perú, "Conoce el Reglamento de la Ley de inteligencia artificial en el Perú", 2026. https://www.gob.pe/110224-conoce-el-reglamento-de-la-ley-de-inteligencia-artificial-en-el-peru

21. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, "Estrategia Nacional de Inteligencia Artificial 2024 – 2030", 2024. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-inteligencia-artificial-2024-2030

22. Deloitte, *"State of AI in the Enterprise. The untapped edge"*, 2026. https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/consulting/2026/state-of-ai-2026.pdf

23. ISO/IEC 42001:2023, *"Information technology —Artificial intelligence— Management system"*, 2023. https://www.iso.org/es/norma/42001

Contacto

Carlos Labanda
Socio Líder de *Artificial Intelligence & Data*
Deloitte Spanish Latin America
fgarciacruz@deloittemx.com

Andrea Bernales Zapata
Socia *Cyber*
Deloitte Spanish Latin America
abernales@deloittemx.com

José Luis Jerez
Socio de Impuestos y Servicios Legales
Deloitte Spanish Latin America
jjerez@deloitte.com

Brenda García Flores
Socia Líder de Política Pública para S-LATAM
Deloitte México
bgarciaflores@deloittemx.com

Leticia Stephanie Enríquez
Abogada en Servicios Legales de Tecnología | Impuestos y Servicios Legales
Deloitte México
leenriquez@deloittemx.com

Centro de contacto
+52 55 5080 6633
centrodecontacto@deloittemx.com

Deloitte.