NYCE
A QIMA COMPANY

Perspectivas sobre el estado de la Inteligencia Artificial en Latinoamérica: Oportunidades, Riesgos y el Papel de la ISO/IEC 42001

Estudio cualitativo de Análisis Documental

ESR Empresa Socialmente Responsable

EMPRESAS EXCEPCIONALES

NYCE®
A QIMA COMPANY

Desde hace más de 30 años, en NYCE hemos acompañado la transformación tecnológica en México y América Latina, brindando confianza a través de servicios de evaluación de la conformidad. En 2012 ampliamos nuestro alcance hacia la certificación de sistemas de gestión, y hoy contamos acreditación para certificar organizaciones en más de 25 estándares, incluyendo ISO 9001 (calidad), ISO/IEC 27001 (seguridad de la información), ISO 20000–1 (servicios de TI), ISO 14001 (medio ambiente) y el estándar de Protección de Datos Personales, en el cual fuimos el primer organismo acreditado en México. Miembros de la red IQNET, que agrupa a los certificadores más relevantes del mundo, y participamos activamente en las comisiones de trabajo de la Organización Internacional de Normalización (ISO), contribuyendo con nuestra experiencia técnica en el desarrollo de normas que tienen impacto global. Hoy, frente al avance acelerado de la inteligencia artificial, asumimos un nuevo compromiso: impulsar su adopción ética y segura. Por ello, nos enorgullece ser el primer organismo latinoamericano acreditado para certificar sistemas de gestión de IA bajo la norma ISO/IEC 42001, consolidando nuestro rol como puente entre innovación y responsabilidad en esta nueva era digital.

Autores

Dr. José Luis Hernández Chávez
Fundador y CEO - White Box Project

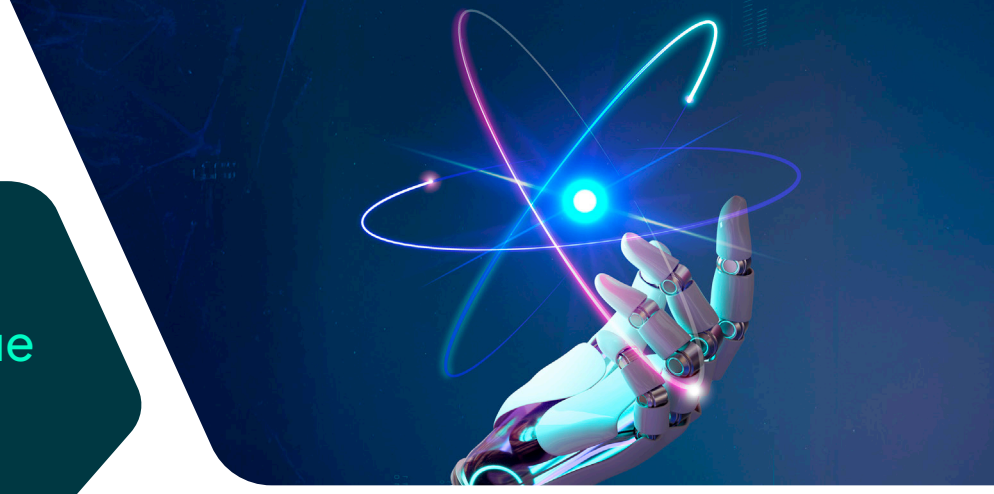
Conferencista internacional experto en compliance y prevención de riesgos derivados del uso de inteligencia artificial. Su labor impulsa la implementación ética y responsable de la IA desde la docencia, la investigación y la formación de líderes en cumplimiento normativo.

Dra. Ariana Bucio
Directora Operativa - BP Grus

Ingeniera, doctora y estratega tecnológica, Ha sido una figura clave en el desarrollo de marcos de referencia internacionales como ITIL® 4 y SDI, donde ha contribuido como autora, traductora y embajadora. Ha impulsado una visión en la que la tecnología es eficaz solo si es humana, ética y adaptable a los contextos reales de cada organización.

Ing. Camila Andrea Escobar Fernández
Gerente - ES Gestión Empresarial

Especialista en sistemas de gestión y evaluación de la conformidad, con sólida experiencia en normas ISO y en la implementación de marcos que garantizan calidad, trazabilidad y confianza. Su visión integral aporta un enfoque riguroso y estratégico a la adopción responsable de tecnologías como la inteligencia artificial.

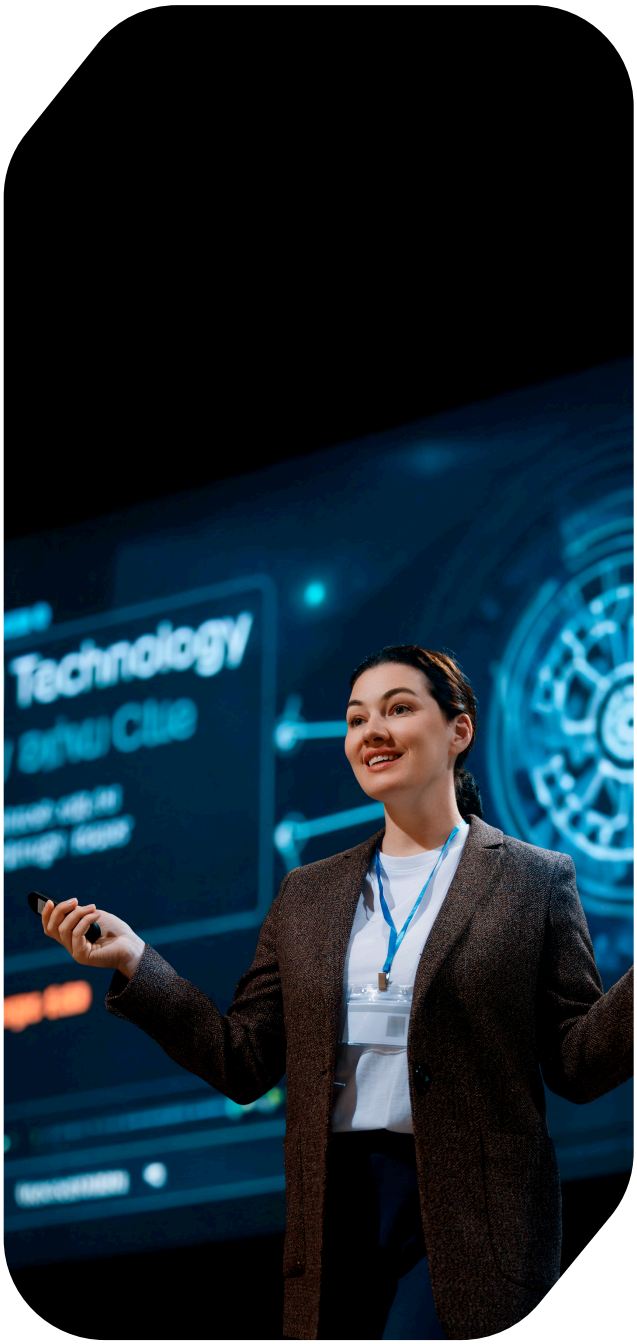


Metodología y enfoque

Este estudio se desarrolló a través de un análisis documental exhaustivo, realizado por un equipo multidisciplinario de especialistas con amplia experiencia en implementación y certificación de sistemas de gestión, tecnologías emergentes, políticas públicas y gestión de riesgos. La revisión comprendió literatura académica, marcos normativos internacionales, informes técnicos de organismos multilaterales, estrategias nacionales de IA, casos de uso empresarial y documentos regulatorios vigentes y en desarrollo en América Latina.

El objetivo principal fue construir una perspectiva integral del ecosistema de inteligencia artificial (IA) en la región, que no solo describiera el estado actual de adopción tecnológica, sino que permitiera identificar con claridad las condiciones habilitadoras, los riesgos emergentes, y las oportunidades para una implementación ética, responsable y sostenible.

A diferencia de otros estudios centrados únicamente en el impacto económico o el potencial de la IA en términos de productividad o atractivo tecnológico, este análisis adopta un enfoque transversal y diferenciador, poniendo especial énfasis en su manejo responsable, su regulación y, sobre todo, su certificación para un impacto estratégico. Esto es clave para una adopción segura y confiable en nuestra región.



El enfoque de certificación aporta un valor adicional al estudio, al evidenciar que no basta con implementar tecnología: se requiere contar con mecanismos verificables y auditables que aseguren el cumplimiento de principios éticos, requisitos técnicos y normativas regulatorias emergentes. Esto resulta especialmente relevante en contextos donde la confianza del usuario, la protección de datos personales, la no discriminación algorítmica y la trazabilidad de decisiones automatizadas son factores críticos.

Esta perspectiva normativa y de certificación diferenciada representa una contribución clave al debate regional, ya que permite vincular el desarrollo tecnológico con la generación de confianza pública, la competitividad empresarial y el fortalecimiento institucional, tres condiciones indispensables para que la IA contribuya efectivamente al desarrollo sostenible de América Latina.

Índice

Introducción

La Inteligencia Artificial (IA) se ha consolidado como una de las fuerzas más disruptivas del siglo XXI, transformando la manera en que gobiernos, empresas y sociedades interactúan, toman decisiones y generan valor. En este contexto global, América Latina enfrenta una paradoja: un enorme potencial en términos de datos, talento y creatividad, pero también desafíos estructurales que limitan una adopción sólida y equitativa de esta tecnología.

Este estudio ofrece un panorama integral sobre el estado actual de la IA en la región y propone líneas de acción para una implementación responsable, sostenible y estratégica. La reflexión se estructura en cuatro capítulos interconectados:

El primer capítulo examina la urgente necesidad de contar con marcos regulatorios y esquemas de corregulación que permitan alinear la innovación con principios éticos y de seguridad. Se destaca el papel de referentes internacionales, como la norma ISO/IEC 42001, para guiar a gobiernos y organizaciones en la construcción de entornos confiables para el desarrollo de sistemas de IA.

En el segundo capítulo, se analiza el panorama regional de la IA, evidenciando tanto los avances como las brechas en infraestructura, capacitación y políticas públicas. A pesar de la creciente actividad en algunos países, la falta de estrategias coordinadas sigue siendo un obstáculo para el aprovechamiento pleno de las oportunidades que ofrece esta tecnología.

El tercer capítulo se enfoca en la transformación del sector empresarial. Aquí se abordan los beneficios de la IA en términos de eficiencia, automatización y competitividad, pero también los riesgos asociados a su uso sin una adecuada gestión ética. La adopción de la IA debe ir acompañada de principios que garanticen no solo resultados económicos, sino también impactos sociales positivos.

Finalmente, el cuarto capítulo profundiza en la norma ISO/IEC 42001, dedicada a sistemas de gestión de IA, explorando su valor como herramienta estratégica para mitigar riesgos, generar confianza y facilitar el cumplimiento de marcos internacionales. Se contrastan sus alcances con otros esquemas relevantes, como el GDPR, el AI Risk Management Framework del NIST y el Reglamento Europeo de IA, subrayando su aplicabilidad en el contexto latinoamericano.

En un momento clave para la región, este artículo invita a tomadores de decisiones, empresas, responsables de políticas públicas y comunidad académica a reflexionar sobre el papel que jugará América Latina en la gobernanza de la IA. No se trata solo de incorporar tecnología, sino de hacerlo con visión ética, técnica y social, asegurando que sus beneficios alcancen a todos.

NYCE
A QIMA COMPANY

Capítulo 1: Inteligencia Artificial y la necesidad de regulación en América Latina.

La inteligencia artificial está transformando nuestro mundo a un ritmo vertiginoso, pero en América Latina enfrentamos un desafío clave: cómo aprovechar esta tecnología sin perder de vista la ética, la seguridad y los derechos fundamentales. Este capítulo invita a reflexionar sobre la importancia de construir un marco regulatorio que no solo controle, sino que también impulse un desarrollo responsable y confiable de la IA en nuestra región, abriendo el camino hacia un futuro más justo y tecnológico.

Perspectiva clave del capítulo

1. La IA avanza más rápido que las leyes, tener marcos para gobernarla es un imperativo ético y estratégico, no solo una cuestión tecnológica o jurídica.

2. En América Latina, regular no siempre significa prohibir: corregulación puede ser la fórmula para innovar con responsabilidad.

3. Las normas técnicas como ISO/IEC 42001 ya ofrecen soluciones concretas mientras la legislación se pone al día.

4. Sin reglas claras, la confianza en la IA se debilita, y con ella, su potencial para transformar industrias y gobiernos.

5. Certificar cómo usamos la IA es una forma tangible de demostrar que la innovación puede ir de la mano con la ética.

1.1 Un momento decisivo para la gobernanza.

La Inteligencia Artificial (IA) es una tecnología de propósito general que emerge como en su momento lo hizo la electricidad, y cuya capacidad para transformar los cimientos de la economía, la educación, la empresa y la vida social es aún inimaginable. En Latinoamérica, su adopción se produce en un contexto de desigualdad estructural, capacidades institucionales limitadas y agendas regulatorias incipientes.

Esta situación plantea retos sustanciales para las organizaciones, sobre todo si desean asegurar un desarrollo tecnológico que respete principios básicos que han sido puestos en la balanza en la empresa y que impactan a la Ingeniería y al Derecho (los derechos humanos y la dignidad de la persona, el medio ambiente, el gobierno corporativo, entre otros). **El reto de todas las organizaciones que utilizan IA es aprender a interpretar estos retos y a minimizar los riesgos derivados del uso no regulado de sistemas de IA.**

> “En este escenario, más que una urgencia por legislar de inmediato, debemos entender nuestra realidad y buscar un camino paralelo basado en la corregulación, entendido como la interacción entre normas técnicas desarrolladas por organismos privados —como las normas ISO— y su reconocimiento por parte de autoridades gubernamentales.”

Este enfoque ya está disponible y puede ser implementado de forma ágil por el sector empresarial y gubernamental, sin necesidad de esperar a procesos legislativos largos o inciertos.

Es importante distinguir tres caminos regulatorios que a menudo se confunden: la legislación (normas jurídicas creadas por el poder legislativo), la regulación administrativa (disposiciones emitidas por órganos del Ejecutivo con facultades normativas), y la corregulación (instrumentos creados por particulares, como estándares técnicos, que son reconocidos por los gobiernos y cuya adopción ha dado grandes beneficios a los actores públicos y privados).

Esta perspectiva invita a reconsiderar el debate público: no se trata de elegir entre legislar o no, sino de construir una arquitectura regulatoria gradual, flexible y orientada a resultados. **En este proceso, las normas internacionales como la ISO/IEC 42001 pueden jugar un papel catalizador,** al ofrecer un marco robusto, ético y aplicable que permite institucionalizar principios fundamentales de transparencia, rendición de cuentas y gestión de riesgos en el uso de la IA.

> La certificación no sustituye a la ley, pero puede ser una herramienta poderosa para anticipar riesgos y asegurar que la implementación tecnológica sea confiable.

1.2 Panorama internacional y su influencia en América Latina

En 2024, la aprobación del Artificial Intelligence Act en la Unión Europea marcó un hito en la regulación tecnológica global (European Commission, 2024). Junto con iniciativas como la Declaración de Hiroshima del **G7 (G7, 2023)**, el Marco de Riesgos del **NIST (NIST, 2023)**, las Recomendaciones de la **UNESCO** sobre la ética de la IA **(UNESCO, 2021)**, y la estrategia de inteligencia artificial de la **OCDE (OECD, 2023)**, se está configurando un ecosistema internacional donde la gobernanza de la IA es prioridad política y estratégica.

A este conjunto se suman las recomendaciones del Banco Interamericano de Desarrollo **(BID, 2022)** para el desarrollo de marcos normativos en la región, así como las órdenes ejecutivas emitidas por el gobierno de los Estados Unidos, que estableció la creación de estrategias de IA en agencias gubernamentales y la designación de **Chief AI Officers (CAIOs)** para garantizar la gobernanza algorítmica en la administración pública. Latinoamérica debe insertarse en esta conversación global sin replicar modelos ajenos de manera mecánica. La regulación regional debe tener en cuenta:

- Los bajos niveles de alfabetización en IA que existen en la población.
- La brecha tecnológica en instituciones públicas y privadas.
- El potencial transformador de la IA para atacar los 2 retos previos.

Existen ya algunos esfuerzos que toman en cuenta lo anterior. Por ejemplo:

Colombia, con la Estrategia Nacional Digital 2023–2026, presentada en febrero de 2024. La estrategia busca cerrar brechas de acceso y uso de tecnologías digitales, promoviendo un entorno digital inclusivo y sostenible.

México, con la creación de la Agencia de Transformación Digital y Telecomunicaciones (noviembre de 2024), la cual tiene como meta una reestructuración de todos los trámites que realizan los ciudadanos ante las agencias de gobierno. Entre sus atribuciones se incluyen la formulación de políticas de inclusión digital, gobierno digital, informática, tecnologías de la información y telecomunicaciones. Además, se está discutiendo una ley de IA así como la creación en 2025 del laborartorio nacional de IA.

Chile, con una Política Nacional de IA lanzada en 2021 por el Ministerio de Ciencia, que articula principios éticos, inversión en capacidades y un sistema de monitoreo (Gobierno de Chile, 2021).

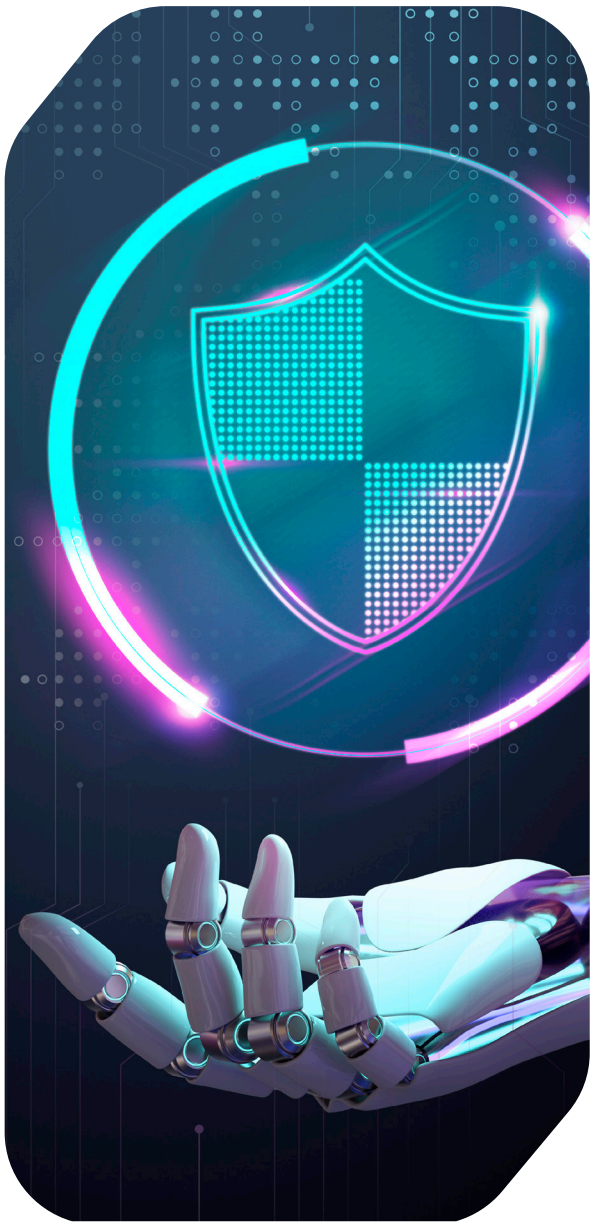
Estos casos ilustran que América Latina está comenzando a construir sus propios cimientos en materia de inteligencia artificial, aunque de forma fragmentada y con niveles desiguales de madurez. Para que estos esfuerzos nacionales realmente tengan impacto y no queden aislados, es fundamental que se inserten en una arquitectura de gobernanza para el uso de la IA articulada desde la empresa (sector privado) y con el acompañamiento de los gobiernos y expertos que conozcan opciones para una corregulación.

1.3 El vacío regulatorio: riesgos y consecuencias

En 2024, el panorama regulatorio de la inteligencia artificial en América Latina mostró avances significativos. Según el informe Radiografía Normativa: **¿Dónde, qué y cómo se está regulando la inteligencia artificial en América Latina?** publicado por Access Now en colaboración con TrustLaw de la Fundación Thomson Reuters, varios países de la región han iniciado procesos legislativos y desarrollado políticas públicas específicas para abordar el desarrollo y uso de la IA. El informe destaca que, aunque existen iniciativas en marcha, la mayoría de los países aún carecen de leyes específicas y mecanismos robustos de rendición de cuentas algorítmica, evaluación de impacto y supervisión de sistemas automatizados.

Por ello, se vuelve prioritario avanzar hacia una arquitectura de gobernanza multinivel, que combine legislación, regulación administrativa y corregulación basada en estándares técnicos. Este enfoque permite una respuesta más flexible, progresiva y adaptativa frente a la evolución acelerada de los sistemas de IA.

Cabe señalar, la falta de actualización o adopción de políticas, procesos, procedimientos y códigos de conducta para el uso de IA también dificulta la protección de derechos fundamentales (protección de datos, el debido proceso o el acceso a la reparación del daño en caso de impactos adversos). Además, sin regulaciones claras, las organizaciones tienden a adoptar tecnologías sin someterlas a pruebas rigurosas de seguridad, impacto o ética, lo cual puede generar consecuencias reputacionales, legales y operativas. Este entorno también afecta la confianza pública, reduciendo la aceptación social de la IA, especialmente en sectores sensibles como la salud, la justicia, la educación o la seguridad. Incorporar marcos como la ISO/IEC 42001 puede facilitar la transición hacia esquemas institucionales más maduros, ya que permite establecer responsabilidades, monitorear el ciclo de vida algorítmico y asegurar la trazabilidad, explicabilidad y evaluación de riesgos. **Esta norma puede ser un puente entre la autorregulación tecnológica y la futura legislación regional sobre IA.**



1.4 Elementos clave para el uso responsable de la IA

La regulación efectiva de la inteligencia artificial (IA) en América Latina requiere una aproximación integral que contemple tres pilares fundamentales: principios rectores, capacidades institucionales y metodologías para la implementación de una gestión de la IA. La norma ISO/IEC 42001:2023 se presenta como una herramienta clave para armonizar todo lo anterior y establecer un lenguaje común entre los actores del ecosistema de IA y todos los stakeholders. Por ejemplo:

a. Principios rectores:
Protección de los derechos humanos.

La base de cualquier marco regulatorio La base de cualquier marco regulatorio debe ser el respeto a los derechos humanos, la equidad, la transparencia y la rendición de cuentas. Estos principios son esenciales para garantizar que los sistemas de IA se desarrollen y utilicen de manera ética y responsable. La Recomendación de la UNESCO sobre la ética de la inteligencia artificial enfatiza la importancia de incorporar estos valores en todas las etapas del ciclo de vida de los sistemas de IA y de hacerlo siempre bajo la supervisión de un ser humano.

b. Capacidades institucionales:
Agencias gubernamentales especializadas, comités para el uso responsable de la IA y CAIOs.

La implementación efectiva de la regulación de la IA requiere instituciones sólidas capaces de supervisar y hacer cumplir las normas establecidas. Esto incluye la creación de agencias de supervisión algorítmica con la autoridad y los recursos necesarios para monitorear el desarrollo y uso de sistemas de IA, evaluar su impacto y garantizar la protección de los derechos de los ciudadanos. Estas agencias deben estar equipadas para realizar auditorías, gestionar riesgos y promover la transparencia en el uso de la IA. En el ámbito privado, este supervisor responde a un nuevo puesto en las organizaciones: el Chief Artificial Intelligence Officer.

c. Mecanismos de implementación:
Auditorías y evaluaciones de impacto.

Para asegurar la conformidad con los principios y normas establecidos, es fundamental contar con mecanismos de implementación efectivos. Esto incluye la realización de auditorías independientes y evaluaciones de impacto que permitan identificar y mitigar riesgos asociados con el uso de la IA. La norma ISO/IEC 42001 proporciona directrices para llevar a cabo estas evaluaciones de manera sistemática y documentada, facilitando la identificación de riesgos y la implementación de medidas correctivas.

En conclusión, la adopción de un enfoque integral que combine principios éticos, capacidades institucionales robustas y mecanismos de implementación efectivos es esencial para la regulación de la IA en América Latina. La norma ISO/IEC 42001 ofrece una herramienta valiosa para armonizar prácticas y establecer un lenguaje común entre los diversos actores del ecosistema de IA, promoviendo un desarrollo tecnológico ético, seguro y alineado con los derechos fundamentales.

1.5 El papel de los C-Suite en 2025

El término C-Suite hace referencia al conjunto de altos ejecutivos de una organización, incluyendo figuras como el CEO (Chief Executive Officer), CFO (Chief Financial Officer), CIO (Chief Information Officer) y, cada vez más, el CAIO (Chief Artificial Intelligence Officer). Estos líderes son responsables de la dirección estratégica, la toma de decisiones críticas y la implementación de innovaciones tecnológicas. En el contexto de la transformación digital, su rol en la gobernanza de la inteligencia artificial se ha vuelto central.

Según estudios como Gartner C-Level Leadership Vision (Gartner, 2025) y programas de MIT Sloan Executive Education (MIT Sloan, 2025), se identifica una convergencia en torno a tres ejes fundamentales: hacer que la IA sea más valiosa (es decir, orientada a resultados concretos), más confiable (con mecanismos de rendición de cuentas y ética incorporada) y más accionable (que permita una integración real con los objetivos del negocio).

Para el C-Suite en América Latina, esto implica tres prioridades estratégicas:

1.**Establecer principios de gobernanza desde el diseño:** Adoptar un enfoque by design que incorpore ética, privacidad y seguridad en cada etapa del ciclo de vida de los sistemas de IA. Esto requiere la implementación de políticas internas, códigos de conducta algorítmica y comités de gobernanza con participación interdisciplinaria.

2. **Alinear la estrategia para el uso de IA con los objetivos del negoc**io: Integrar la IA como un habilitador de eficiencia, personalización de servicios, innovación de productos y ventaja competitiva. Las decisiones sobre automatización, aprendizaje automático o sistemas de recomendación deben estar articuladas con indicadores clave de desempeño (KPIs) y planes de crecimiento sostenible.

3. **Adoptar marcos de cumplimiento como la ISO/IEC 42001:** Esta norma permite institucionalizar un sistema de gestión de IA basado en riesgos, con procesos de auditoría, monitoreo, trazabilidad y mejora continua. El C-Suite debe promover su adopción como parte de una estrategia de cumplimiento normativo, reputación corporativa y preparación para futuras exigencias regulatorias tanto locales como internacionales.

4. **Contar con un supervisor de la IA (CAIO).**: Es necesario, como ocurrió cuando se crearon los oficiales de cumplimiento en prevención de lavado de dinero o en materias como privacidad, corrupción, seguridad de datos, considerar la formación y/o creación de un Chief Artificial Intelligence Officer, que tenga las habilidades necesarias para poder proteger el modelo de IA y el modelo de negocio que le da vida.

A través de estas tres prioridades, el liderazgo ejecutivo no solo anticipa tendencias tecnológicas, sino que construye una cultura organizacional preparada para enfrentar los desafíos éticos, legales y operacionales de la inteligencia artificial.

NYCE
A QIMA COMPANY

Capítulo 2: Estado actual de la Inteligencia Artificial en Latinoamérica.

En los últimos años, la Inteligencia Artificial (IA) ha dejado de ser una promesa futura para convertirse en un motor activo de transformación en gobiernos, industrias y sociedades. Sin embargo, cuando miramos a Latinoamérica, encontramos una realidad compleja: por un lado, un potencial enorme basado en la riqueza de datos, el talento emergente y la necesidad de resolver problemas estructurales; por otro, una adopción aún desigual, marcada por brechas de infraestructura, inversión, regulación y capacidades.

Para los líderes de gobierno, empresas y academia, comprender el estado actual de la IA implica mirar más allá de las cifras de adopción, requiere evaluar las condiciones habilitadoras; es decir, infraestructura, políticas, educación, gobernanza y capacidades humanas que determinan el impacto real y sostenible de esta tecnología. Asimismo, comprender los factores que aceleran o frenan su evolución. Es también un llamado a tomar decisiones informadas, éticas y colaborativas que definan si esta tecnología será una herramienta de inclusión o una nueva fuente de desigualdad.

Perspectiva clave del capítulo

1. Aunque hay talento y datos en la región, el desarrollo de IA sigue siendo desigual, disperso y poco coordinado.

2. Algunos países avanzan, otros apenas comienzan: la brecha digital en América Latina también es una brecha en inteligencia artificial.

3. Sin infraestructura, políticas públicas ni visión compartida, la IA podría convertirse en otra oportunidad perdida.

4. A pesar de los retos, hay señales de esperanza: universidades, startups y sectores públicos están marcando el camino.

5. Este momento es decisivo: o construimos un ecosistema regional de IA, o veremos cómo otros lo hacen por nosotros.

2.1 Panorama general de adopción

Latinoamérica presenta un mosaico heterogéneo en términos de madurez digital y capacidades de adopción tecnológica que está entre la intención de implementar este tipo de tecnologías y la implementación. **Países como Brasil, México, Chile, Argentina y Colombia lideran los esfuerzos en IA**, albergando centros de investigación, startups de base tecnológica y programas gubernamentales orientados a la transformación digital **(OCDE, 2022).** El AI Readiness Index 2023 de Oxford Insights posiciona a Brasil en el lugar 49 del mundo, seguido por México (63), Chile (66), Colombia (67) y Argentina (71), reflejando una preparación relativa frente a los desafíos y oportunidades de la IA. Sin embargo, estos resultados no deben interpretarse como un indicador de madurez técnica o de impacto social, sino como una línea base que evidencia el largo camino por recorrer. A nivel regional, la implementación de sistemas de IA sigue limitado a ciertos sectores económicos y zonas urbanas, lo que genera riesgos de exclusión y de concentración de beneficios.

Un estudio reciente del Banco Interamericano de Desarrollo (BID) revela que solo el 15% de las empresas en Latinoamérica utilizan alguna forma de IA que en su mayoría se encuentran en fases piloto, cifra que contrasta con el promedio de 27% en países de la OCDE **(BID, 2023)**. Esta brecha refleja no solo la diferencia en inversión en investigación y desarrollo (I+D), sino también la falta de políticas públicas robustas que impulsen el ecosistema de IA con una visión estratégica el cómo aprovechar los sistemas de IA de una manera responsable, sostenible y escalable.

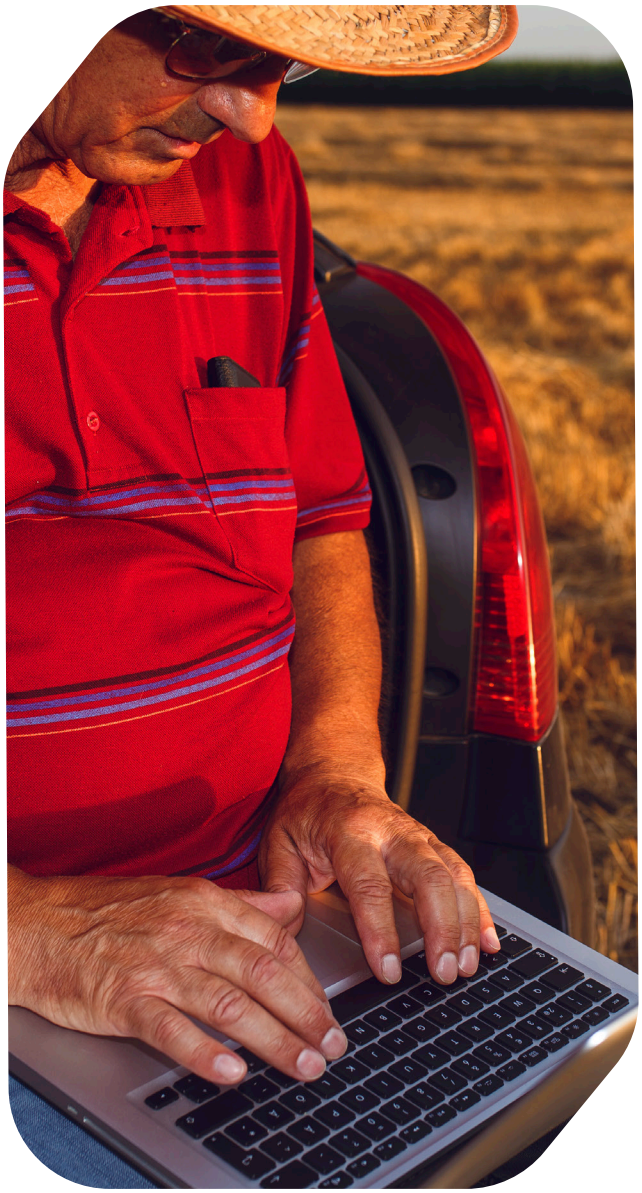
2.2 Infraestructura tecnológica y conectividad

No se puede hablar de IA sin hablar de datos, conectividad y capacidad de cómputo. América Latina enfrenta serias limitaciones en este aspecto, siendo el cuello de botella silencioso. Una cifra alarmante es que según la Unión Internacional de Telecomunicaciones **(UIT, 2023)**, cerca del 35% de la población rural en la región aún no tiene acceso regular a internet. La calidad de la conectividad, la cobertura de redes móviles y de banda ancha, así como el acceso a centros de cómputo de alto rendimiento y servicios en la nube, son variables críticas que limitan el desarrollo equitativo de la IA.

> “Muchas organizaciones públicas y privadas de la región dependen de infraestructuras internacionales para entrenar modelos o almacenar información sensible. Esto plantea riesgos de soberanía digital y dependencia tecnológica.”

Brasil destaca por su ecosistema de datos y su capacidad de procesamiento, siendo el único país latinoamericano con una estrategia nacional de IA consolidada y con centros de datos públicos de gran escala

(Secretaria de Governo Digital, 2021). México, por su parte, ha mostrado avances en la adopción de tecnologías de nube e iniciativas sectoriales, pero aún carece de un plan nacional de IA formal que articule necesidades sociales, prioridades industriales y capacidades tecnológicas propias. Aunque Brasil y México han comenzado a desarrollar centros de datos propios, aún son insuficientes para atender la demanda potencial de soluciones avanzadas basadas en IA.



2.3 Capital humano y brechas educativas: un desafío urgente

El desarrollo de la IA requiere algo más que tecnología: necesita talento calificado y una visión ética. En este punto, América Latina enfrenta una de sus brechas más profundas.

La CEPAL (2022) advierte que el déficit de profesionales en tecnologías avanzadas podría agravar las desigualdades existentes y limitar el potencial de innovación local. También la **UNESCO (2023)** advierte que el déficit de profesionales con formación especializada en IA, ciencia de datos, ética digital y gobernanza algorítmica es crítico en la región. Si bien se han creado programas académicos en universidades de México, Brasil, Argentina, Colombia y Chile, su alcance sigue siendo limitado, con baja cobertura nacional y escasa articulación con las necesidades del sector productivo. A esto se suma una fragmentación educativa: muchos programas están desconectados de la realidad socioeconómica local, se concentran en las capitales, y no incorporan las dimensiones éticas, legales ni de diversidad necesarias para una IA inclusiva.

Además, la educación básica y media aún no prepara a los estudiantes en competencias digitales fundamentales. **Según el informe Future of Jobs 2023 del World Economic Forum, el rezago en habilidades STEM,** pensamiento crítico, alfabetización digital y adaptabilidad es especialmente agudo en América Latina (WEF, 2023).

> “Formar talento en IA no implica únicamente capacitar ingenieros en ciencia de datos o desarrolladores, sino preparar profesionales capaces de diseñar, evaluar e implementar sistemas de IA con conciencia social.

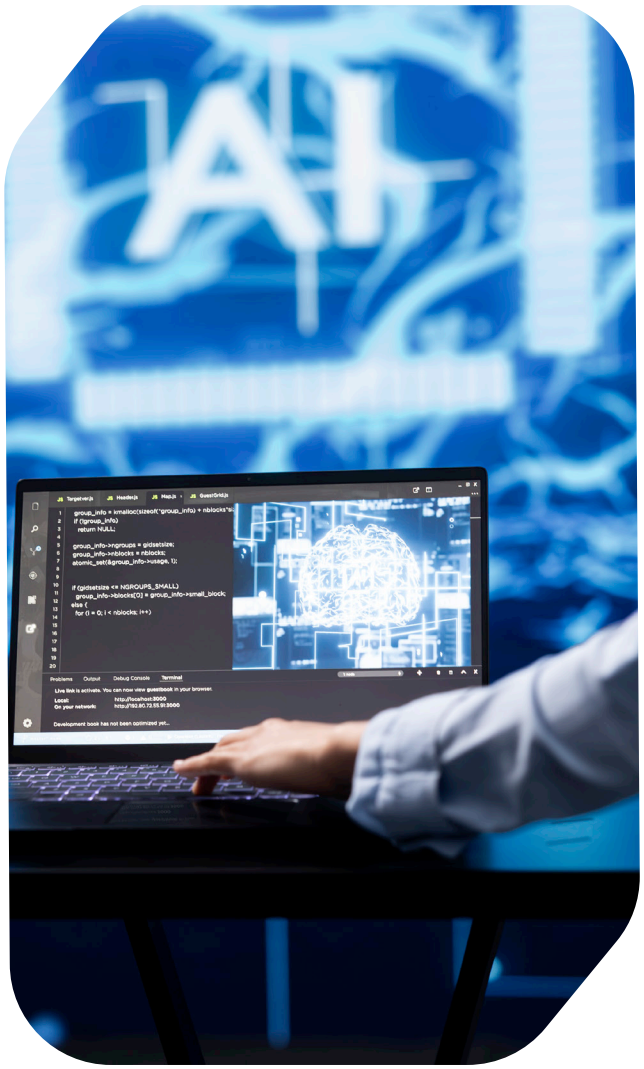
La IA requiere habilidades técnicas, pero también una comprensión profunda de su impacto en la vida cotidiana de millones de personas; no podemos permitirnos formar talento en burbujas tecnocráticas. Lo que se requiere es desarrollar capacidades interdisciplinarias, fomentar la participación de mujeres y grupos subrepresentados, e integrar la IA en los planes de estudio desde etapas tempranas. La falta de políticas educativas integrales pone en riesgo la sostenibilidad de cualquier estrategia nacional de IA.

Programas internacionales como AI4Good de la UNESCO y alianzas con universidades internacionales han sido una vía de avance, pero el reto sigue siendo masificar la educación digital desde edades tempranas, garantizar el acceso equitativo y promover la participación de mujeres y grupos subrepresentados en las disciplinas STEM, así como la alineación con los Objetivos de Desarrollo Sostenible **(ONU, 2021).**

En el ámbito de la investigación, se observa una concentración de publicaciones científicas en IA en universidades de Brasil, México, Argentina y Colombia. Sin embargo, la inversión pública en **I+D sigue siendo baja: apenas el 0.5% del PIB regional, frente al promedio del 2.4% en países desarrollados (UNESCO, 2023).** Esta limitación reduce la capacidad de generar innovación propia y dependencia de tecnologías foráneas que no necesariamente responden a los contextos sociales y culturales de la región.

2.4 I+D: innovación fragmentada e independiente

La investigación y desarrollo (I+D) en Inteligencia Artificial sigue siendo incipiente en la mayoría de los países latinoamericanos. Aunque existen centros de investigación destacados, como el Centro de IA de la Universidad de São Paulo, el CENIA en Chile o el Instituto de Investigaciones en IA de la UNAM en México, su impacto regional es aún limitado.



Según datos de la UNESCO10 (2023), menos del 1% del total global de publicaciones científicas en IA proviene de América Latina, y la inversión en I+D como porcentaje del PIB en la región no supera el 0.7%, frente al 2.5% de promedio en países de la OCDE.

En México recientemente se propuso el Plan Estratégico Nacional de I+D en IA de 2025 que se alineará con el Plan de Acción de IA, identificando prioridades estratégicas federales para la I+D de IA.

Esta baja inversión se traduce en dependencia tecnológica. Muchos modelos utilizados en la región provienen de plataformas globales, entrenados con datos que no representan el contexto latinoamericano. Esto genera riesgos de sesgo, ineficacia y pérdida de control sobre las decisiones automatizadas.

Asimismo, la desconexión entre la academia y el sector productivo impide que los avances científicos se traduzcan en innovación aplicada. La falta de mecanismos de transferencia tecnológica, incentivos fiscales y marcos de propiedad intelectual adaptados a los desarrollos de IA agrava esta brecha.

Impulsar la I+D en IA debe ser una prioridad estratégica. No solo para reducir la dependencia de modelos extranjeros, sino para desarrollar soluciones alineadas con los valores, idiomas y problemas propios de la región.

2.5 Gobernanza regional: los primeros pasos hacia una IA confiable

> La gobernanza no es solo una cuestión de compliance, sino una manifestación de visión ética y compromiso con el valor público.

A diferencia de otras regiones como la Unión Europea, que avanza con marcos jurídicos claros como el AI Act, América Latina carece de regulaciones específicas sobre IA. La mayoría de los países aún se encuentran en etapas de consulta, diagnósticos exploratorios o con normativas sectoriales que apenas rozan aspectos vinculados a la IA, como la protección de datos personales, la ciberseguridad o la contratación pública. Los pasos de Latinoamérica son incipientes, el componente normativo, ético y organizativo del desarrollo de la IA es crítico para generar confianza social y asegurar su implementación responsable.

A nivel regional, la CEPAL (2022) y la Red de Gobierno Digital de América Latina han promovido marcos éticos y orientaciones para el uso responsable de la IA en el sector público. Brasil, Chile, Colombia y Uruguay cuentan con estrategias nacionales que incorporan principios de equidad, transparencia y derechos humanos.

México, si bien ha publicado lineamientos sectoriales, aún carece de una estrategia nacional formal que articule el desarrollo de IA de forma intersectorial, se están realizando esfuerzos en varios ámbitos para promover el uso y desarrollo de la IA, como la Alianza Nacional para la Inteligencia Artificial (ANIA) conformado por representantes del Senado y la sociedad civil que han estado trabajando en la creación de estándares y buenas prácticas para la adopción de una estrategia nacional de IA, también en el Senado se presentó la Agenda Nacional de IA que tiene como objetivo contribuir a la economía global a través de la IA

explorando los retos y oportunidades. Otra de las grandes iniciativas es la Estrategia Nacional de IA que fue impulsada por el gobierno mexicano que incluye acciones específicas para integrar la IA en sectores clave, como la salud, el medio ambiente y las finanzas, con el objetivo de mejorar la eficiencia y la productividad en dichas áreas. Esta estrategia busca fortalecer la colaboración entre el gobierno, la industria, la sociedad civil y la academia para la adopción y el desarrollo de la IA. Esta sinergia es clave para garantizar un ecosistema robusto y preparado para los desafíos tecnológicos del futuro.

La colaboración entre sector público y privado es aún incipiente en la región, pero existen casos prometedores. En Argentina, el Plan Nacional de Ciencia y Tecnología 2030 promueve alianzas con el sector productivo para la adopción de IA en industrias estratégicas. **En Uruguay, la Agencia de Gobierno Electrónico lidera iniciativas piloto con modelos de IA para mejorar la gestión pública y la prestación de servicios ciudadanos (AGESIC, 2023).**

Algunos países, como Chile y Colombia, han iniciado procesos de elaboración de estrategias nacionales de IA que incluyen principios éticos, mecanismos de gobernanza algorítmica y colaboración público-privada. Sin embargo, estos esfuerzos requieren continuidad institucional, financiamiento sostenido y mecanismos efectivos de evaluación de impacto.

Estas experiencias demuestran que, si bien existen condiciones estructurales limitantes, la coordinación intersectorial y el liderazgo político pueden detonar dinámicas virtuosas de adopción tecnológica.

Un avance clave es la creciente atención a estándares internacionales como las normas ISO/IEC 22989:2022 (Conceptos y terminología de la Inteligencia Artificial), ISO/IEC 23894:2023 (Gestión de riesgos de IA), y la más reciente ISO/IEC 42001:202311, que proporciona un marco para establecer sistemas de gestión de IA con enfoque en calidad, ética, trazabilidad y mejora continua (ISO, 2023). Esta norma permite a las organizaciones, ya sea públicas o privadas, demostrar que sus sistemas de IA son responsables, confiables y auditables, lo que facilita la alineación a estándares internacionales, reduciendo riesgos legales, éticos y operativos.

Sin embargo, la adopción de marcos como ISO/IEC 42001:2023 exige una transformación cultural que involucra un liderazgo consciente, alineación estratégica y estructuras organizativas maduras. La gobernanza no es solo una cuestión de compliance, sino una manifestación de visión ética y compromiso con el valor público.

2.6 Ecosistema de innovación y colaboración público-privada: entre el entusiasmo y la incertidumbre

En los últimos años ha surgido un ecosistema emergente de innovación basado en IA, integrado por startups, centros de innovación, incubadoras y grandes empresas tecnológicas. Brasil alberga al menos 300 startups que utilizan IA como componente central de su modelo de negocio; **México y Colombia le siguen con cerca de 100 y 80 respectivamente12 (LAVCA, 2023).**

Estas startups operan principalmente en fintech, ecommerce, ciberseguridad y salud digital. Sin embargo, enfrentan barreras como el acceso limitado a financiamiento de riesgo, escasa vinculación con universidades, y dificultades para escalar sus soluciones en ausencia de marcos regulatorios claros. A esto se suma una cultura empresarial que aún privilegia la eficiencia operativa por encima de las personas y de la innovación disruptiva.

Es necesario reforzar los puentes entre la academia, el sector privado, los gobiernos y la sociedad civil. Las experiencias más exitosas en la región, como el uso de IA para monitoreo ambiental en el Amazonas o para mejorar la atención en salud pública en Medellín, surgen precisamente de la colaboración intersectorial.

Fomentar espacios de cocreación, laboratorios de innovación regulatoria (sandboxes) y marcos de ética aplicada puede generar confianza y acelerar la adopción responsable de la IA. Esta tecnología no puede madurar en silos; necesita diversidad de voces, prácticas y saberes.

2.7 Un futuro por escribir: visión compartida y liderazgo consciente

Hablar del estado de la IA en Latinoamérica es también hablar del tipo de futuro que queremos construir. **¿Será una IA que refuerce los privilegios y aumente la desigualdad, o será una herramienta para democratizar el conocimiento, mejorar la calidad de vida y proteger nuestros ecosistemas?**

El estado actual de la IA en la región es un espejo refleja nuestras fortalezas, pero también nuestras omisiones. Superar estas brechas no es responsabilidad exclusiva de los comités nacionales de ciencia y tecnología o las startups tecnológicas. Requiere la participación decidida de líderes políticos, responsables de políticas educativas, actores empresariales, comunidades científicas y ciudadanía informada.

La inteligencia artificial representa una gran promesa para América Latina, pero también plantea desafíos que no pueden ser ignorados. La región parte de una base con características únicas: una población joven y diversa, una enorme riqueza cultural y ambiental, y un fuerte impulso creativo desde lo social. Estas condiciones abren oportunidades valiosas para construir soluciones locales frente a problemas históricos que aún persisten.

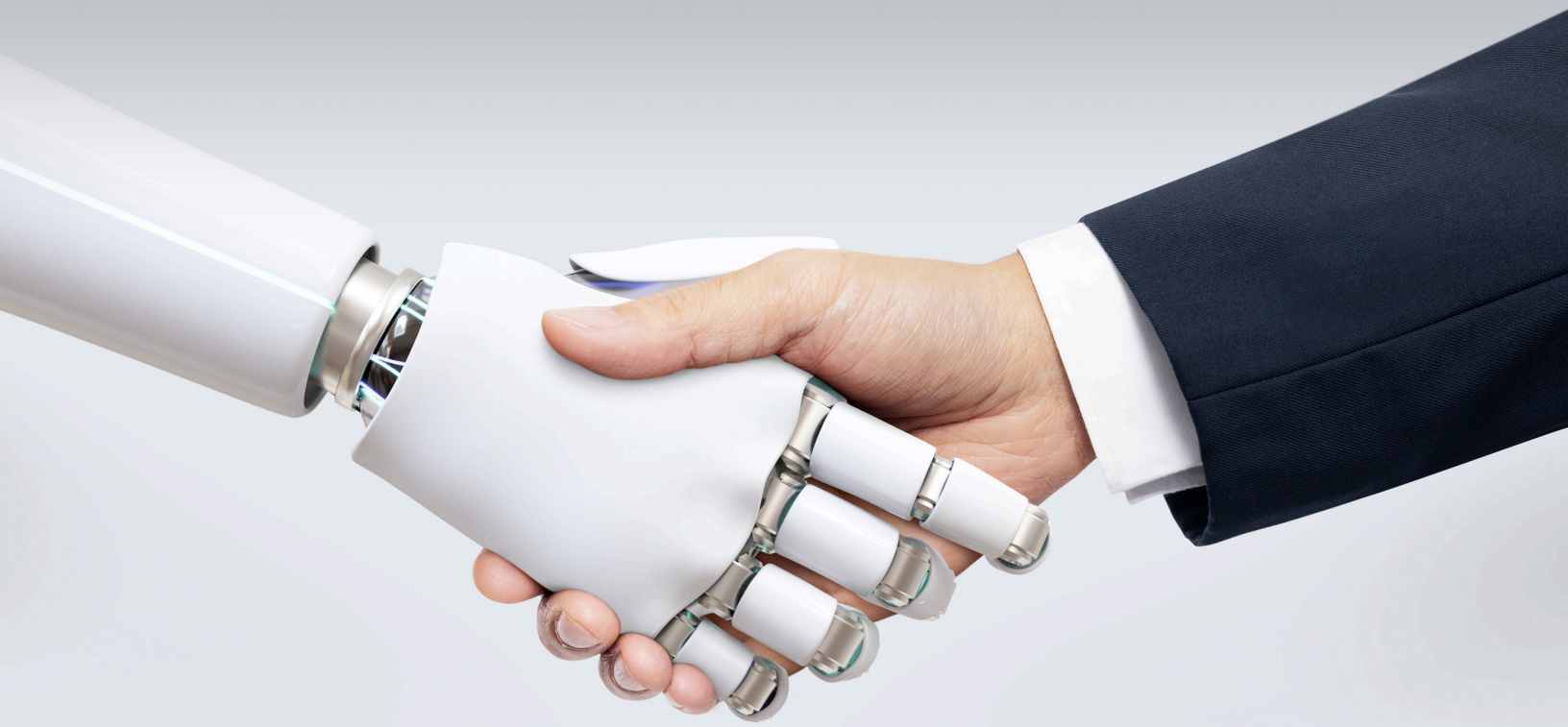
No obstante, el camino hacia una adopción responsable de la IA está lejos de ser simple. Persisten barreras estructurales como la baja inversión en ciencia y tecnología, la falta de regulación clara, la escasez de talento especializado y una cultura de innovación que aún necesita consolidarse. A esto se suma una brecha digital que excluye a grandes sectores de la población del acceso equitativo a estas tecnologías. También es necesario mirar con atención los riesgos que trae consigo el avance tecnológico. La región podría verse atrapada en una dependencia de proveedores externos sin los controles necesarios, expuesta a prácticas de vigilancia sin regulación o al uso de algoritmos que refuercen desigualdades preexistentes.

Por eso, más allá del entusiasmo por el potencial de la IA, es fundamental abrir espacios de reflexión crítica. ¿Qué tipo de desarrollo queremos impulsar con estas herramientas? ¿Quién se beneficia y quién queda fuera? Pensar en estas preguntas es clave para que la tecnología se convierta en una aliada del bienestar colectivo y no en una fuente más de exclusión.

Para ello, será fundamental adoptar enfoques centrados en las personas, que equilibren la innovación tecnológica con principios éticos, inclusión social y sostenibilidad. **Adoptar marcos como la ISO/IEC 42001:2023 es un paso en la dirección correcta, pero no suficiente por sí solo.** Se necesita voluntad política, inversión continua y una ética aplicada que sitúe a las personas, no solo a los datos, en el centro del desarrollo tecnológico.

Como región, tenemos la oportunidad de definir nuestro propio camino en la era de la IA; uno que no imite modelos externos, sino que responda a nuestras realidades, proteja nuestros derechos y potencie nuestras capacidades. La inteligencia artificial no debe ser un lujo importado, sino una herramienta soberana para transformar vidas.

NYCE
A QIMA COMPANY



Capítulo 3: Beneficios, Riesgos y Gestión Ética responsable de la Inteligencia Artificial en el Sector Empresarial

La inteligencia artificial tiene el potencial de revolucionar la manera en que las organizaciones mejoran su eficiencia, innovan en productos y servicios, y alcanzan nuevos niveles de competitividad. Sin embargo, este poder también conlleva riesgos importantes si no se maneja con responsabilidad: desde decisiones automatizadas que pueden afectar derechos fundamentales hasta impactos sociales inesperados. La clave está en adoptar un enfoque que maximice los beneficios de la IA, asegurando al mismo tiempo que su uso sea ético, transparente y equitativo, para construir organizaciones y sociedades más fuertes y justas.

Perspectiva clave del capítulo

1. La IA ya no es ciencia ficción: está tomando decisiones en empresas, muchas veces sin que sepamos cómo ni por qué.

2. Adoptarla sin un marco ético es un riesgo tan grande como no adoptarla.

3. Las empresas que gestionan bien su IA y se certifican, no solo ganan eficiencia, también construyen reputación y confianza.

4. Automatizar no es suficiente: la IA exige una nueva forma de pensar el liderazgo, la cultura y la responsabilidad.

5. En este nuevo escenario, la ética no es un freno: es una ventaja competitiva.

3.1 Inteligencia Artificial como eje estratégico en la transformación empresarial

La inteligencia artificial (IA) se ha convertido en un factor disruptivo en la transformación digital y está redefiniendo el entorno empresarial global. Su aplicación abarca desde automatizar procesos complejos, pasando por analizar grandes volúmenes de datos hasta generar decisiones autónomas basada en análisis predictivos por lo que ha generado una revolución en múltiples industrias. Sin embargo, este avance tecnológico también trae consigo una serie de riesgos que las organizaciones deben gestionar adecuadamente.

En Latinoamérica, su adopción se acelera con una mirada estratégica, aunque aún con desafíos sustanciales en cuanto a gobernanza, ética y gestión. Este capítulo explora los beneficios y riesgos de la IA, y propone una gestión responsable conforme a marcos normativos esenciales como la Norma ISO/IEC 42001:2023.

> Las empresas no deben perder de vista que los beneficios de la IA conllevan responsabilidades éticas, sociales y legales.

3.2 Beneficios transformadores de la IA en el entorno empresarial

- **Eficiencia operativa y automatización inteligente:** Numerosos estudios han demostrado que la IA mejora la eficiencia operativa a través de la automatización inteligente de tareas y de procesos repetitivos, reduciendo errores humanos, acelerando los tiempos de ejecución y aumentando la productividad **(Brynjolfsson & McAfee, 2017)**. Casos como el uso de IA en logística predictiva, la inclusión de los chats bots en la atención al cliente, la automatización de procesos robotizados **(RPA)**, el procesamiento inteligente de documentos en departamentos financieros y el mantenimiento predictivo en la industria manufacturera, entre otros permiten disminuir tiempos de inactividad y optimizar recursos.

- **Optimización de procesos y toma de decisiones basada en datos:** Los sistemas de IA integrados con analítica avanzada ofrecen a los tomadores de decisiones herramientas para analizar grandes volúmenes de datos y escenarios complejos para paoder anticipar comportamientos de mercado mediante algoritmos de aprendizaje automáticos e identificar patrones y tendencias lo que es clave en sectores como el financiero, logístico y salud. Por ejemplo, el análisis de sentimientos y tendencias en redes sociales es usado por empresas minoristas para ajustar inventarios en tiempo real.

- **Innovación, personalización de productos y/o servicios y mejora de la experiencia del cliente:** Las capacidades analíticas de la IA permite ofrecer productos y/o servicios adaptados a las necesidades individuales de los usuarios gracias a que extraen valor de los datos para anticipar comportamientos del consumidor y adaptar estrategias de marketing mediante sistemas de recomendación, asistentes virtuales y análisis predictivos. Esto facilita la segmentación de clientes en tiempo real, la personalización de experiencias digitales, la detección de oportunidades comerciales, mejoras en la retención de clientes, incremento en la satisfacción del cliente, el mejoramiento del posicionamiento en el mercado competitivo y responder más rápidamente a los cambios del entorno. En el comercio electrónico, por ejemplo, los sistemas de recomendación aumentan significativamente las tasas de conversión.

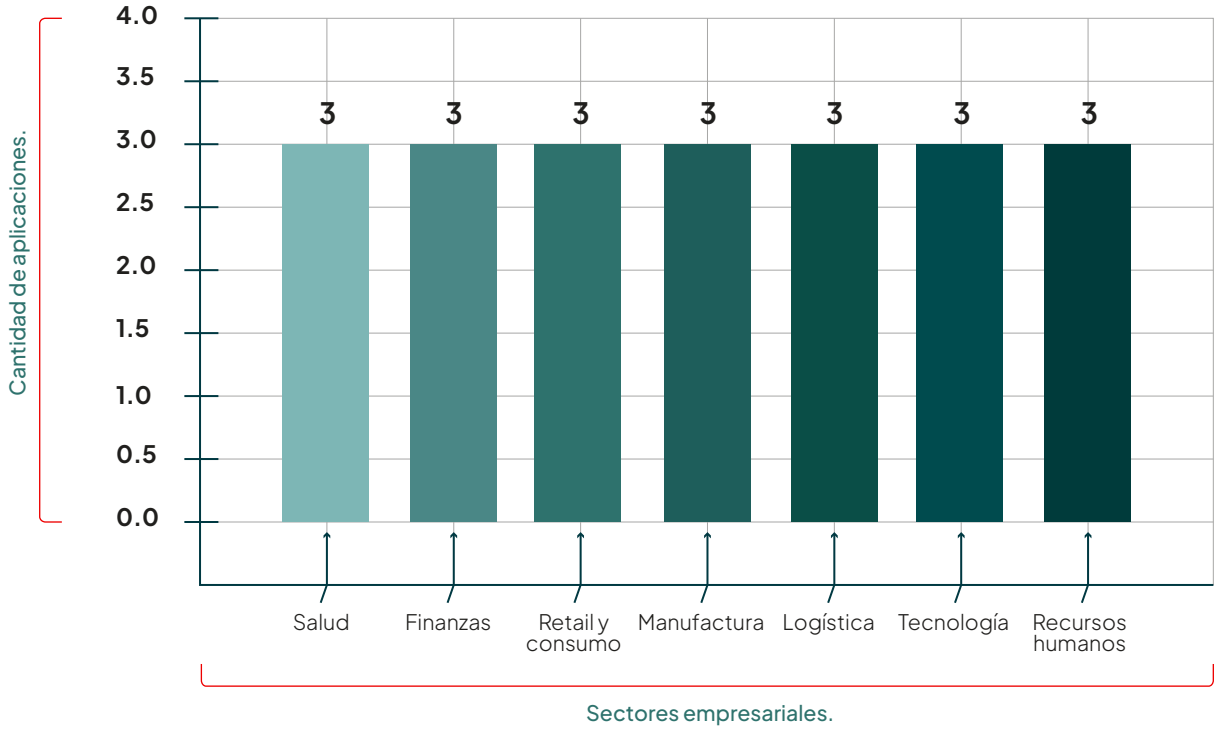
- **Generación de nuevos modelos de negocio:** El uso de IA permite a las empresas reinventar sus ofertas de valor, desarrollando modelos de negocio centrados en plataformas digitales y servicios basados en datos lo que ha dado origen a modelos de negocio disruptivos y soluciones de IA como servicio **(AIaaS)**, fintech algorítmica y soluciones de salud digital personalizadas.

Aplicaciones estratégicas de la IA por sector (Adaptado de PwC, 2022)

SECTOR	APLICACIONES ESTRATÉGICAS DE LA IA
Salud	Diagnóstico asistido por IA, desarrollo de fármacos, gestión hospitalaria
Finanzas	Detección de fraudes, análisis predictivo, automatización de procesos
Retail y consumo	Recomendaciones personalizadas, gestión de inventarios, atención al cliente automatizada
Manufactura	Mantenimiento predictivo, control de calidad, optimización de procesos
Logística	Ruteo inteligente, gestión de almacenes, previsión de demanda
Tecnología	Desarrollo de software autónomo, ciberseguridad inteligente, asistentes virtuales
Recursos humanos	Reclutamiento automatizado, análisis de desempeño, bienestar laboral

Gráfico 1. Aplicaciones estrategicas de la IA en sectores empresariales clave

Aplicaciones estrategicas de la IA en sectores empresariales clave - Fuente: Adaptado de PwC (2022)



3.3 Riesgos críticos de la IA y su impacto en las organizaciones

- **Riesgos éticos, sesgos algorítmicos y discriminación automatizada:** Los modelos de IA pueden replicar y amplificar sesgos presentes en los datos históricos, afectando la equidad en procesos como la selección de personal, la concesión de créditos o la justicia penal, lo que pone en riesgo la reputación de las empresas por posible discriminación. **La norma ISO/IEC 42001:2023 destaca la importancia de la transparencia y la explicabilidad del modelo.** Por ejemplo, en Latinoamérica, se han documentado sistemas de puntuación crediticia que penalizan a sectores no bancarizados, exacerbando desigualdades sociales (IDB, 2021), también estudios han revelado casos en los que sistemas de reconocimiento facial tienen menor precisión en personas con tonos de piel más oscuros, afectando poblaciones vulnerables.

> “La adopción de la IA puede representar una ventaja competitiva, pero también implica riesgos que deben ser gestionados desde una perspectiva integral.”

- **Falta de transparencia y explicabilidad:** Muchos algoritmos, especialmente en deep learning, funcionan como "cajas negras", lo que genera desconfianza cuando las decisiones no pueden ser justificadas especialmente en sectores regulados como la salud o los servicios financieros. Esto va en contra de los principios de rendición de cuentas y derechos de los usuarios.

- **Amenazas a la privacidad, seguridad y protección de datos:** La IA se alimenta de grandes volúmenes de datos para su entrenamiento y funcionamiento, muchos de ellos sensibles. La recopilación excesiva y el uso indebido pueden violar principios fundamentales de privacidad de datos personales y puede vulnerar leyes como el GDPR o la Ley 1581 de 2012 en Colombia. Legislaciones como la Ley de Habeas Data en Colombia establecen límites claros sobre el tratamiento automatizado de información personal. Además, los sistemas de IA pueden ser blanco de ciberataques, poniendo en peligro la información crítica del negocio.

- **Impactos laborales y dilemas éticos:** La automatización avanzada puede generar desplazamiento de puestos de trabajo sin una estrategia de reconversión laboral especialmente en sectores operativos. Aunque se crean nuevos roles, existe una brecha de capacitación y adaptación. Además, surgen dilemas sobre la autonomía de las máquinas, la toma de decisiones críticas y la asignación de responsabilidad legal ante el fallo de un sistema algorítmico.

- **Riesgos estratégicos y de reputación corporativa:** Errores en sistemas de IA pueden acarrear daños reputacionales severos. Por ejemplo, decisiones automatizadas erróneas que afectan a clientes pueden volverse virales y dañar la confianza institucional. Las organizaciones deben evaluar el impacto estratégico de la IA no solo desde la eficiencia, sino desde la percepción pública y la sostenibilidad.

- **Riesgos operacionales y dependencia tecnológica:** La dependencia excesiva de sistemas de IA puede generar vulnerabilidades ante fallos técnicos o errores del modelo. Asimismo, existe el riesgo de desalineación entre los objetivos empresariales y los resultados generados por la IA.

- **Riesgos regulatorios y de cumplimiento:** La regulación de la IA está en desarrollo a nivel global. Normas como la ISO/IEC 42001:2023 y legislaciones regionales emergentes exigen a las empresas establecer controles de gobernanza, auditorías y mecanismos de rendición de cuentas en sus sistemas de IA.

3.4 Casos de estudio en Latinoamérica y lecciones aprendidas

- **Sector financiero en México - Fintech y calificación crediticia:** Una startup financiera implementó un sistema de IA para evaluar riesgos crediticios en tiempo real mejorando los tiempos de aprobación de préstamos. Aunque redujo costos operativos, los usuarios señalaron la falta de transparencia y ausencia de mecanismos para apelar decisiones lo que evidenció la necesidad de implementar políticas claras de explicabilidad y revisión. Lección: incluir revisiones humanas y canales de transparencia es esencial.

- **Reconocimiento facial y vigilancia pública en Brasil:** El uso de IA en sistemas utilizados para vigilancia urbana por parte de autoridades locales mostraron un alto índice en falsos positivos en poblaciones afrodescendientes. Este caso motivó la intervención de la Defensoría Pública y generó un debate nacional sobre los sesgos en tecnologías de seguridad y exigencias de auditoría externa. Lección: Necesidad de validar los modelos con diversidad de datos y evaluación continua por parte de terceros.

- **IA en agricultura de precisión en Colombia:** Empresas emergentes junto a universidades y agricultores implementaron sistemas de IA para predecir pronósticos de cosechas, rendimientos y optimizar uso de fertilizantes. El éxito estuvo en la inclusión de desarrolladores, prestadores de servicios y usuarios campesinos, quienes participaron en la validación de las herramientas. Lección: Esta experiencia muestra cómo una gestión ética y contextualizada favorece la adopción responsable de la IA. Así, como el enfoque participativo mejora la aceptación y efectividad del sistema.

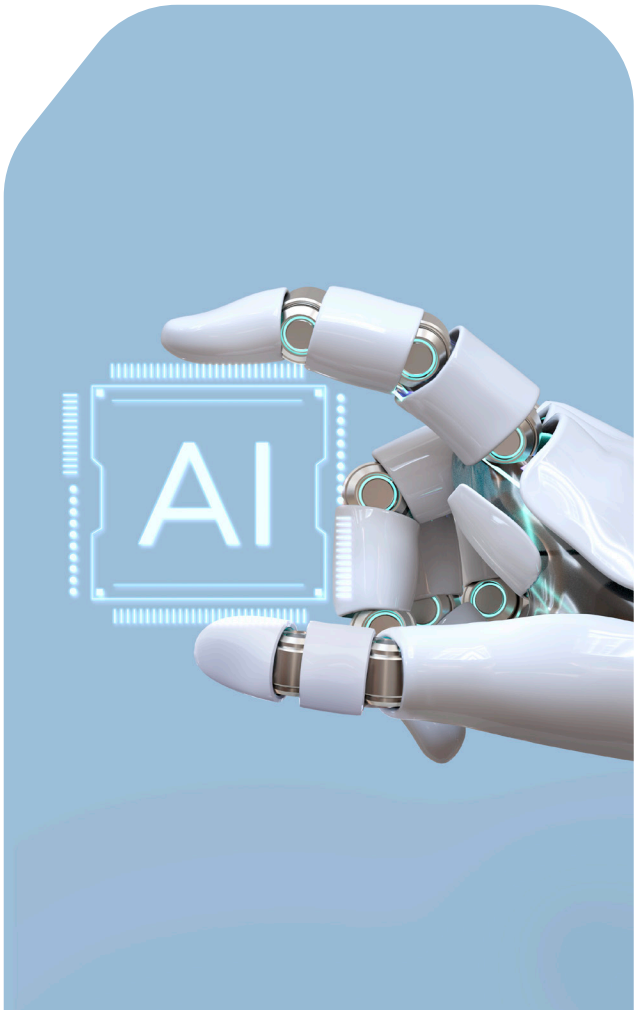
3.5 Recomendaciones y reflexiones para tomadores de decisión y especialistas

Para que la IA aporte valor real, las organizaciones deben adoptar un enfoque holístico y proactivo. Esto implica:

- **Identificar** oportunidades de aplicación con retorno de inversión claro.
- **Involucrar** a los distintos actores del ecosistema de IA (desarrolladores, prestadores de servicios y usuarios) en las fases de diseño, implementación y monitoreo.
- **Invertir** en formación del talento humano y cambio cultural.
- **Desarrollar** una estrategia de IA alineada con los objetivos de negocio y el contexto regulatorio.
- **Adoptar** marcos de referencia como la norma ISO/IEC 42001:2023 para establecer un sistema de gestión robusto.
- **Incorporar** criterios éticos desde la fase de diseño de soluciones de IA.
- **Evaluar** continuamente la calidad de los datos y la equidad de los algoritmos.
- **Establecer** protocolos de auditoría interna y externa de modelos y datos.
- **Formar** equipos multidisciplinarios que incluyan áreas legales, técnicas y sociales.
- **Fomentar** una cultura organizacional centrada en la formación continua y el desarrollo responsable de la IA.

La inteligencia artificial representa un eje estratégico de competitividad empresarial. No obstante, su adopción debe realizarse desde una perspectiva técnica, ética y organizacional equilibrada. A medida que evoluciona el ecosistema normativo y tecnológico, se hace necesario avanzar hacia modelos de gobernanza adaptativos que integren la innovación con la protección de los derechos humanos y la integridad institucional. **La norma ISO/IEC 42001:2023 brinda las herramientas necesarias para avanzar en ese camino**, garantizando una integración segura, confiable y sostenible de la IA en los sistemas empresariales.

La inteligencia artificial no es un fin en sí mismo, sino una herramienta poderosa cuyo éxito depende de su integración con los valores y objetivos estratégicos de la organización.



NYCE
A QIMA COMPANY

Capítulo 4:
El papel de los estándares internacionales: ISO/IEC 42001 como eje de una IA confiable y alineada con el negocio.

Luego de haber revisado en los capítulos anteriores el potencial de la inteligencia artificial (IA) en América Latina, sus retos estructurales y los riesgos y beneficios para el sector empresarial, este capítulo se enfoca en una herramienta concreta para habilitar una gobernanza efectiva: la adopción de estándares internacionales como la ISO/IEC 42001. Este nuevo marco normativo surge como respuesta a la creciente necesidad de gestionar de forma responsable los sistemas de IA, estableciendo un modelo de sistema de gestión que combina principios de ética, transparencia, mitigación de riesgos y alineación con los objetivos organizacionales.

Perspectiva clave del capítulo

1. La ISO/IEC 42001 es el primer estándar mundial que ayuda a las organizaciones a gestionar su uso de IA con orden, transparencia y valor estratégico.

2. Frente al context de regulaciones fragmentadas y aún en desarrollo, esta norma ofrece un camino inmediato y applicable al convertirse en un puente entre la ética y la operación.

3. La norma es aplicable a cualquier organización identificando 3 actores clave: desarrolladores, implementadores de servicios o ususarios, brindando un marco flexible y adaptable.

4. La certificación bajo ISO/IEC 42001 es una forma concreta de generar confianza con clientes, autoridades y usuarios.

5. Latinoamérica puede ser pionera en certificación de IA, no solo consumidora de soluciones externas.

4.1 ¿Qué es la ISO/IEC 42001 y cuál es su importancia?

Publicada en diciembre de 2023 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), la norma ISO/IEC 42001:2023 establece los requisitos para un Sistema de Gestión de la Inteligencia Artificial (AI Management System, AIMS). A diferencia de otros marcos regulatorios que establecen principios éticos o exigencias legales, ISO/IEC 42001 provee un marco operativo basado en procesos, pensado para organizaciones que diseñan, desarrollan, despliegan o utilizan sistemas de IA.

El objetivo central de esta norma es ayudar a las organizaciones a gestionar los riesgos asociados a la IA, asegurando que los sistemas sean seguros, confiables, legales y alineados con los valores organizacionales y sociales. Incluye controles relacionados con la transparencia, explicabilidad, auditorías de IA, monitoreo continuo, y gestión de datos y modelos.

> La ISO/IEC 42001 incluye 3 perfiles: Empresas que desarrollan IA (o entrenan y diseñan), empresas que prestan servicios con IA y empresas usuarias de IA

4.2 Gestión ética y responsable de la IA bajo ISO/IEC 42001:2023

La ISO/IEC 42001:2023 propone un sistema de gestión de inteligencia artificial (AIMS, por sus siglas en inglés), integrable con otros sistemas de gestión. Aborda aspectos como:

- **Gobernanza de IA:** establecimiento de políticas, roles, funciones y mecanismos de supervisión.
- **Evaluación de riesgos:** identificación y mitigación de impactos éticos, legales y técnicos.
- **Trazabilidad y explicabilidad:** requisitos para mantener evidencia documentada y justificar decisiones algorítmicas.
- **Mejora continua:** aprendizaje organizacional mediante revisiones periódicas del rendimiento y cumplimiento.
- **Ciclo de vida del sistema de IA:** desde su diseño, entrenamiento, validación y operación hasta su retiro.

Gráfico 2: Marco de Gestión AIMS según ISO/IEC 42001

Figura: Ciclo del Sistema de Gestión de IA (AIMS), conforme a ISO/IEC 42001:2023.

El marco incluye 38 controles agrupados en 10 objetivos, que cubren aspectos como gestión del ciclo de vida, ética, la evaluación de impacto y la mejora continua. Estos controles permiten a las organizaciones no sólo mitigar riesgos, sino también demostrar diligencia debida ante clientes, reguladores y audiencias externas.

Esquema visual de los 10 objetivos y los 38 controles.

1. Gobernanza de IA
- Políticas y liderazgo
- Roles y responsabilidades
- Comité de gobernanza
- Revisión por la dirección

2. Gestión de Riesgos
- Identificación y evaluación
- Mitigación
- Revisión periódica

3. Ciclo de Vida del Sistema de IA
- Diseño y desarrollo
- Validación, implementación
- Retiro planificado

4. Uso Responsable
- Guías éticas
- Supervisión humana
- Formación interna

5. Sesgos y Discriminación
- Detección de sesgos
- Equidad algorítmica
- Revisión continua

6. Transparencia
- Explicabilidad
- Documentación técnica
- Comunicación al usuario

7. Privacidad y Protección de Datos
- Minimización
- Consentimiento
- Seguridad de datos

8. Seguridad de IA
- Resiliencia ante ataques
- Pruebas técnicas
- Auditorías de seguridad

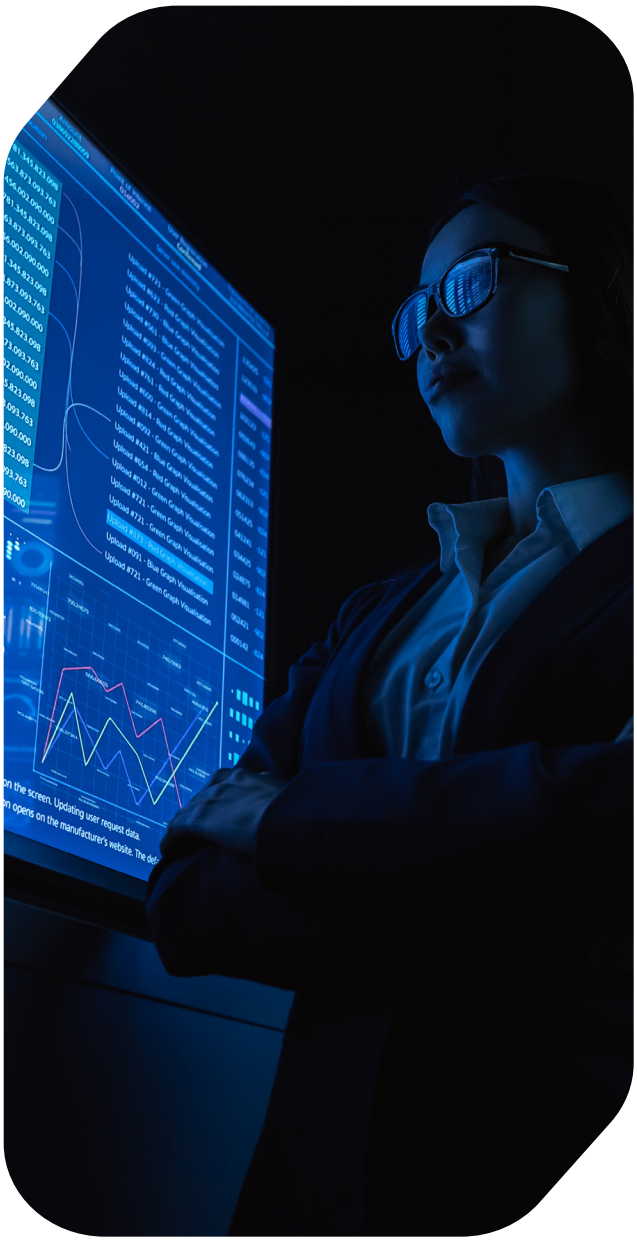
9. Partes Interesadas
- Canales de retroalimentación
- Participación y quejas
- Gestión de relaciones

10. Mejora Continua
- KPIs y métricas
- Auditorías y no conformidades
- Revisión + cambio continuo

4.3 Comparación crítica con otros marcos

La adopción de sistemas de gestión como el propuesto por la ISO/IEC 42001:2023 no ocurre en el vacío. En el ecosistema global de regulación y gobernanza de la Inteligencia Artificial, existen diversos marcos normativos que abordan aspectos específicos como la privacidad, la seguridad, la gestión de riesgos o el impacto social de la IA. En esta sección se presenta una comparación crítica entre la **ISO/IEC 42001** y algunos de los marcos más influyentes a nivel internacional, incluyendo el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, el Reglamento Europeo de IA (EU AI Act), el Marco de Gestión de Riesgos de IA del NIST (AI RMF) en Estados Unidos y normas ampliamente adoptadas en ciberseguridad como **ISO/IEC 27001 y SOC 2.**

Mientras que estos marcos difieren en enfoque, obligatoriedad y origen, comparten una preocupación central: la necesidad de garantizar que los sistemas de IA sean seguros, transparentes y alineados con valores éticos. La **ISO/IEC 42001** se distingue por ofrecer un enfoque holístico y certificable, integrando elementos técnicos, organizacionales y éticos en un Sistema de Gestión de IA (AIMS). Esta perspectiva no busca reemplazar a otros marcos, sino actuar como una plataforma estructural que los complementa: provee el andamiaje necesario para incorporar prácticas de privacidad (como en GDPR), evaluaciones de riesgo (como en el NIST AI RMF) o cumplimiento legal (como en el EU AI Act).



En términos de similitudes, todos los marcos analizados promueven la transparencia, la gestión de riesgos y el enfoque centrado en el usuario. En cuanto a diferencias, varían en su nivel de prescriptividad (norma voluntaria vs. ley obligatoria), en su aplicabilidad (sectorial, regional o transversal) y en la profundidad técnica que exigen. **La ISO/IEC 42001** se posiciona como una herramienta certificable, lo que la distingue como un mecanismo concreto de verificación y generación de confianza.

Una comparación detallada se muestra a continuación

Marco / Normativa	País / Región	Año de creación	Enfoque principal	¿Obligatorio?	Complementariedad y diferencias frente a ISO/IEC 42001
ISO/IEC 42001	Internacional (ISO)	2023	Sistema de gestión para IA (gobernanza, ética, riesgos)	Voluntaria (certificable)	N/A – Es el marco base de comparación. Su enfoque sistémico y certificable lo distingue de marcos legales.
GDPR	Unión Europea	2018	Privacidad y protección de datos personales	Sí (en UE y para empresas con usuarios europeos)	ISO 42001 puede complementarse con SOC 2 para abordar cumplimiento comercial. Diferencia: SOC 2 es reporte técnico externo; ISO 42001 establece un sistema de gestión integral de IA.
EU AI Act	Unión Europea	Aprobado 2024 (aplicación en 2025–2026)	Regulación de IA según niveles de riesgo	Sí (gradual)	ISO 42001 puede facilitar el cumplimiento del AI Act, especialmente para sistemas de alto riesgo. Diferencia: el AI Act es regulatorio/legal, ISO es voluntario y flexible en su implementación.
NIST AI RMF	Estados Unidos	2023	Gestión de riesgos en IA (principios y prácticas)	No, voluntario	IISO 42001 transforma principios del RMF en procesos auditables y sistemáticos. Diferencia: NIST es guía técnica, ISO es estándar certificable con enfoque organizacional.
ISO/IEC 27001	Internacional (ISO)	2005 (última versión 2022)	Seguridad de la información	Voluntaria (certificable)	ISO 42001 expande el enfoque a riesgos éticos y sociales de la IA. Similitud: ambos usan estructuras de gestión tipo ISO. Diferencia: 27001 se limita a seguridad de la información.
SOC 2	Estados Unidos	2011	Seguridad, disponibilidad, confidencialidad (auditoría de sistemas)	Voluntaria / comercial	ISO 42001 puede complementarse con SOC 2 para abordar cumplimiento comercial. Diferencia: SOC 2 es reporte técnico externo; ISO 42001 establece un sistema de gestión integral de IA.

Este comparativo muestra cómo la ISO/IEC 42001 no pretende reemplazar estos marcos, sino actuar como un marco integrador, creando sinergias entre lo técnico, lo legal y lo organizacional. Su estructura permite adoptar los principios de marcos como NIST, cumplir con obligaciones del **AI Act o GDPR**, y articularse con **normas de ciberseguridad como ISO 27001**, ofreciendo así un enfoque sistémico, escalable y certificable para la gobernanza responsable de la IA.

4.4 Potencial en Latinoamérica: aplicabilidad y desafíos

La adopción del estándar ISO/IEC 42001 en América Latina se ubica en un punto de inflexión: puede convertirse en una herramienta catalizadora para el desarrollo ético, competitivo y sostenible de los ecosistemas de inteligencia artificial (IA), o bien consolidarse como otro referente internacional poco aplicado si no se abordan sus barreras de entrada. Su implementación ofrece beneficios diferenciados según el tipo de actor involucrado, al tiempo que expone desafíos estructurales que exigen soluciones colaborativas.

Oportunidades estratégicas por sector

Para gobiernos y autoridades reguladoras, ISO/IEC 42001 puede servir como hoja de ruta para el diseño de marcos normativos nacionales, actuando como base técnica para políticas públicas que aborden la IA desde un enfoque preventivo y propositivo. Su adopción temprana puede posicionar a los Estados latinoamericanos como promotores de la IA confiable, facilitando el alineamiento con marcos internacionales como el EU AI Act o el NIST AI Risk Management Framework, y fortaleciendo su voz en foros multilaterales.

Para el sector empresarial, especialmente grandes corporativos y exportadores, la certificación representa un activo estratégico. En mercados globales crecientemente regulados, contar con un sistema de gestión de IA certificado puede ser decisivo para el acceso a licitaciones públicas, acuerdos de cooperación internacional o procesos de compra responsable. De hecho, se espera que grandes compradores o inversores comiencen a exigir este tipo de certificaciones como parte de sus evaluaciones de cumplimiento ético y técnico en IA.

Para las PyMEs y startups tecnológicas, ISO/IEC 42001 representa una oportunidad de diferenciación. En un entorno de alta competencia, contar con credenciales en gestión responsable de IA puede abrir puertas a aceleradoras, fondos de inversión con criterios ESG, así como generar confianza en alianzas con clientes de mayor tamaño. Al tratarse de un estándar con enfoque sistémico, puede ser adaptado a distintos niveles de madurez tecnológica.

Para la academia y los centros de investigación, el estándar ofrece un marco estructurado para vincular el desarrollo técnico de algoritmos con principios éticos y de gobernanza, fomentando programas de formación interdisciplinaria y promoviendo proyectos piloto con instituciones públicas o privadas.

> “Adoptar la norma es una estrategia para asegurar que la IA no solo sea ética y responsable, sino también una herramienta alineada con los objetivos del negocio”

Sector	Oportunidades Estratégicas
Gobiernos y autoridades	• Hoja de ruta para marcos normativos nacionales. • Base técnica para políticas públicas preventivas y propositivas. • Posicionamiento como promotores de IA confiable. • Facilita alineamiento con marcos internacionales (EU AI Act, NIST AI RMF). • Fortalece voz en foros multilaterales.
Sector empresarial	• Activo estratégico para grandes corporativos y exportadores. • Facilita acceso a licitaciones públicas y acuerdos internacionales. • Cumplimiento ético y técnico exigido por grandes compradores e inversores.
PyMEs y startups tecnológicas	• Diferenciación competitiva. • Acceso a aceleradoras y fondos de inversión ESG. • Genera confianza para alianzas con clientes mayores. • Adaptable a distintos niveles de madurez tecnológica.
Academia y centros de investigación	• Marco para vincular desarrollo técnico con ética y gobernanza. • Fomenta formación interdisciplinaria. • Promueve proyectos piloto con sector público y privado.

Barreras y desafíos clave en Latinoamérica

No obstante, la adopción en la región enfrenta varios desafíos estructurales que deben ser atendidos con visión sistémica:

• **Escasez de organismos de certificación acreditados** y de auditores con experiencia específica en IA. Esto genera cuellos de botella que elevan los costos e impiden escalar procesos de evaluación confiables.

• **Brecha de capacidades técnicas.** Muchas empresas, especialmente las PyMEs, carecen del conocimiento necesario para implementar un sistema de gestión de IA conforme a la norma, lo cual requiere inversión en capacitación, consultoría y acompañamiento técnico.

• **Marco institucional aún débil.** La mayoría de los países latinoamericanos carecen de una estrategia nacional de IA consolidada. En este contexto, no existen aún incentivos regulatorios ni fiscales que promuevan activamente la adopción de estándares internacionales.

• **Percepción de la certificación como un lujo y no como una inversión estratégica.** Para muchas organizaciones, el cumplimiento normativo aún se percibe como un costo y no como una ventaja competitiva o mecanismo de mitigación de riesgos reputacionales, legales y operativos.

Recomendaciones para una adopción efectiva

Para aprovechar el potencial del estándar ISO/IEC 42001 en la región, se propone un enfoque de acción múltiple que involucre tanto al sector público como privado, con énfasis en la certificación como una herramienta clave de confianza, trazabilidad y alineación con estándares internacionales:

1. **Crear centros regionales de competencia en IA confiable,** con participación académica y del sector privado, que promuevan la formación técnica, la preparación para auditorías y la generación de capacidades locales para implementar y certificarse conforme a ISO/IEC 42001.

2. **Desarrollar mecanismos de cofinanciamiento y apoyo técnico a PyMEs,** por medio de programas públicos o fondos multilaterales de desarrollo (como CAF, BID o CEPAL), que incluyan recursos destinados a acompañar procesos de certificación en IA como parte de sus estrategias de transformación digital responsable.

3. **Incluir la norma ISO/IEC 42001 como referente técnico en políticas nacionales de IA,** normativas sectoriales o lineamientos para contratación pública de sistemas automatizados, especificando que su certificación puede funcionar como criterio de cumplimiento, control de riesgos y buenas prácticas institucionales.

4. **Formar auditores y especialistas locales en gestión y certificación de IA,** a través de diplomados, certificaciones profesionales o alianzas con organismos de normalización, para garantizar que la región cuente con capacidades propias para evaluar y validar el cumplimiento del estándar.

5. **Difundir casos de éxito latinoamericanos que hayan adoptado o se hayan certificado conforme a ISO/IEC 42001** o principios alineados, para demostrar su valor estratégico, aumentar la demanda del estándar en sectores críticos y generar confianza en su aplicabilidad en contextos locales.

4.5 Beneficios clave de implementar ISO/IEC 42001

Alineación de la tecnología con el negocio

Uno de los mayores retos en la adopción de soluciones de Inteligencia Artificial es evitar que la tecnología se convierta en un fin en sí misma o en un conjunto de proyectos aislados que no aportan valor real ni sostenible a la organización. La norma ISO/IEC 42001 se destaca precisamente por su enfoque holístico, que articula la gestión tecnológica con los objetivos estratégicos y los valores corporativos, asegurando que la IA sirva para impulsar el crecimiento, la innovación y la confianza en el negocio.

Definición de metas claras vinculadas a la gestión responsable de IA

La norma impulsa a las organizaciones a traducir su visión estratégica en metas específicas relacionadas con el uso de IA, tales como:

- **Mejorar** la experiencia del cliente mediante sistemas inteligentes que respeten la privacidad y eviten sesgos discriminatorios.
- **Optimizar** procesos internos (automatización, análisis predictivo, control de calidad) sin comprometer la ética ni la transparencia.
- **Innovar** con responsabilidad, desarrollando productos y servicios que generen beneficios tangibles para usuarios y sociedad, respetando principios éticos y legales.

Este alineamiento claro facilita que los proyectos de IA se diseñen, implementen y evalúen con criterios medibles, lo que permite identificar si realmente están contribuyendo a los objetivos del negocio.

Valor sostenible y gestión del riesgo

ISO/IEC 42001 establece que las inversiones en IA deben generar valor sostenible, no solo beneficios inmediatos. Esto implica:

- **Evitar** desarrollos tecnológicos aislados o impulsivos que pueden generar riesgos operativos, legales o reputacionales a largo plazo.
- **Integrar** la gestión de riesgos desde la concepción hasta la operación continua de los sistemas de IA, garantizando que la tecnología respalde la continuidad y resiliencia del negocio.
- **Promover** revisiones periódicas y ajustes para que las soluciones evolucionen en línea con cambios de mercado, normativos y tecnológicos.

Este enfoque ayuda a proteger la inversión, asegurando que la IA aporte ventajas competitivas duraderas y no se convierta en una fuente de vulnerabilidades o costos ocultos.

Toma de decisiones informada y gobierno corporativo

La norma impulsa la implementación de controles y métricas que aseguran que las decisiones basadas en IA estén sustentadas en datos confiables y procesos transparentes. Esto tiene un impacto directo en:

- El fortalecimiento del gobierno corporativo, al disponer de mecanismos claros para supervisar proyectos de IA, evaluar riesgos y medir resultados.

• La reducción de incertidumbre para la alta dirección, que puede confiar en informes y auditorías que evidencian el cumplimiento normativo y ético.

• La mejora en la comunicación interna y externa, con evidencia transparente que facilita explicar el uso responsable de IA ante stakeholders, reguladores y clientes.

Este nivel de control y trazabilidad contribuye a que la tecnología no solo sea una herramienta operativa, sino un activo estratégico para la toma de decisiones.

Posicionamiento como líder en innovación responsable

Finalmente, **la adopción de ISO/IEC 42001** puede convertir a la organización en un referente de innovación responsable, con beneficios tangibles:

• Apertura de nuevos mercados y oportunidades comerciales, especialmente en regiones y sectores que valoran la ética y la transparencia en tecnología.

• Atracción y retención de talento especializado, que busca trabajar en entornos que priorizan valores éticos y una cultura organizacional madura.

• Mejora en la percepción pública y la reputación corporativa, fortaleciendo la confianza de clientes, socios, reguladores y la sociedad en general.

En un mundo donde la confianza en la tecnología es cada vez más crucial, esta ventaja competitiva puede ser decisiva para el éxito y la sostenibilidad a largo plazo.

Identificación del rol dentro del ecosistema de IA: clave para una gestión responsable.

Una de las primeras y más críticas etapas que propone **la norma ISO/IEC 42001** es que toda organización que implemente sistemas de inteligencia artificial debe comprender y definir claramente su rol específico dentro del ecosistema de IA en el que opera. Esta identificación no solo es un ejercicio formal, sino una pieza estratégica para construir una gobernanza robusta y efectiva, adaptada a las responsabilidades, riesgos y expectativas asociadas.T

¿Qué implica definir el rol en el ecosistema de IA?

El ecosistema de IA está compuesto por múltiples actores interrelacionados que contribuyen en distintas fases del ciclo de vida de una solución inteligente: desde el desarrollo, entrenamiento y validación de modelos, hasta su implementación, operación, mantenimiento, supervisión y auditoría. La norma insta a que cada entidad analice su participación para:

• Mapear sus responsabilidades concretas: No es lo mismo ser el proveedor del algoritmo, que el integrador de soluciones o el usuario final que toma decisiones apoyado en IA.

• Identificar las interdependencias y cadenas de valor: Cómo se conecta y depende de otros actores, por ejemplo, proveedores de datos, reguladores o auditores externos.

• Alinear sus procesos internos con su función: Para asegurar que los controles, protocolos y mecanismos de supervisión sean los adecuados al tipo de actividad que realiza

Roles típicos y sus responsabilidades en la práctica

A continuación se ejemplifican algunos roles clave y sus principales responsabilidades dentro de un esquema de gestión alineado a ISO/IEC 42001:

Actor	Responsabilidades principales
1. Desarrolladores de sistemas de IA	• Diseñar, entrenar y validar modelos algorítmicos. • Asegurar calidad y representatividad de datos. • Garantizar transparencia y explicabilidad. • Implementar controles para minimizar sesgos y errores. • Documentar procesos y resultados para auditorías.
2. Proveedores de plataformas y servicios tecnológicos	• Proveer infraestructura, herramientas y soporte técnico. • Garantizar seguridad y privacidad de datos en tránsito y almacenamiento. • Facilitar monitoreo continuo y actualización de sistemas.
3. Usuarios finales (empresas, entidades públicas, consumidores)	• Comprender capacidades y limitaciones del sistema de IA. • Supervisar resultados y detectar fallos o sesgos. • Asumir responsabilidad en decisiones soportadas por IA y su impacto ético y legal.
4. Reguladores y entidades de supervisión	• Marco para vincular desarrollo técnico con ética y gobernanza. • Fomenta formación interdisciplinaria. • Promueve proyectos piloto con sector público y privado.
5. Auditores y certificadores	• Evaluar conformidad con ISO/IEC 42001 y otros marcos. • Verificar efectividad de controles y cumplimiento ético-técnico. • Proveer confianza externa a usuarios y consumidores.

Importancia de esta identificación para la gestión de riesgos y oportunidades

Al tener claro el rol dentro del ecosistema, una organización puede:

- **Diseñar un sistema de gestión específico y efectivo:** Los controles no son genéricos sino adaptados a las tareas y riesgos particulares.

- **Evitar solapamientos o lagunas en la gobernanza:** Cada actor sabe qué debe hacer, cómo colaborar y qué esperar de los demás.

- **Responder con agilidad y transparencia ante incidentes:** Con roles claros, se identifican rápidamente las causas y responsabilidades, lo que mejora la rendición de cuentas.

- **Aprovechar oportunidades estratégicas:** Por ejemplo, desarrolladores pueden demostrar competencia técnica y ética, usuarios pueden mitigar riesgos reputacionales, reguladores pueden focalizar esfuerzos supervisores.

Mitigación de riesgos en IA

La norma ISO/IEC 42001 establece un sistema de gestión integral que permite a las organizaciones abordar de manera sistemática y estructurada los riesgos asociados al desarrollo, implementación y operación de sistemas de Inteligencia Artificial. Estos riesgos no solo incluyen aspectos técnicos, sino también operativos, éticos y legales, que son fundamentales para garantizar una adopción segura, confiable y socialmente responsable de la IA.

Identificación y evaluación sistemática de riesgos

Uno de los pilares centrales del estándar es la identificación temprana y continua de riesgos inherentes al uso de IA. Esto abarca:

- **Sesgos algorítmicos:** Se evalúan posibles parcialidades en los datos o en el diseño del modelo que puedan derivar en discriminación o decisiones injustas hacia ciertos grupos o individuos. La norma promueve la implementación de metodologías para detectar, medir y corregir estos sesgos.

- **Privacidad y protección de datos:** Se analizan los riesgos vinculados a la recopilación, almacenamiento y procesamiento de datos personales, asegurando que se respeten los derechos de privacidad y se cumplan normativas como GDPR u otras leyes locales.

- **Seguridad informática:** Se considera la protección contra ataques o manipulación maliciosa de los sistemas de IA que puedan afectar su integridad o disponibilidad, incluyendo vulnerabilidades técnicas y posibles vectores de amenaza.

- **Discriminación y efectos no deseados:** Más allá de sesgos directos, la norma obliga a evaluar impactos sociales y éticos no previstos, como consecuencias económicas o sociales adversas, daños reputacionales o pérdida de confianza en la tecnología.

Esta evaluación sistemática se basa en métodos de gestión de riesgos reconocidos internacionalmente, permitiendo priorizar acciones correctivas y preventivas según la gravedad e impacto potencial.

Implementación de controles y procesos de mitigación

Tras la identificación, la norma establece controles específicos para mitigar estos riesgos, entre ellos:

- **Auditorías internas periódicas:** Revisiones continuas para asegurar el cumplimiento de políticas y controles, detectar desviaciones y oportunidades de mejora.

- **Monitoreo en tiempo real:** Seguimiento constante del desempeño y comportamiento de los sistemas de IA en producción, con alertas tempranas sobre anomalías o desviaciones.

- **Pruebas de robustez y validación:** Evaluación constante de la capacidad del modelo para manejar datos nuevos o situaciones imprevistas, asegurando resiliencia ante cambios y evitando resultados inesperados o erróneos.

- **Mecanismos de rendición de cuentas:** Establecimiento de roles y responsabilidades claras para cada etapa del ciclo de vida de la IA, con transparencia sobre las decisiones automatizadas y posibilidad de revisión humana cuando sea necesario.

Fomento de una cultura organizacional responsable

Más allá de controles técnicos, la ISO/IEC 42001 enfatiza la necesidad de integrar la gestión de riesgos en la cultura corporativa. Esto implica

- Capacitación continua para que todos los niveles de la organización — desde desarrolladores hasta la alta dirección — comprendan los riesgos asociados y la importancia de su mitigación.
- Promoción de valores de transparencia y responsabilidad en el uso de IA, facilitando la comunicación abierta sobre desafíos y errores para aprender y mejorar.

- Impulso de políticas internas que alineen la innovación tecnológica con principios éticos, asegurando que las decisiones de negocio consideren impactos sociales y legales.

> “En la práctica, organizaciones certificadas reportan mejores relaciones con reguladores, mayor confianza por parte de sus clientes y una reducción significativa en incidentes relacionados con sesgos, privacidad o fallas técnicas.”

4.6 La certificación como ventaja estratégica en la implementación de Inteligencia Artificial

Es fundamental entender que l**a implementación de ISO/IEC 42001 y su certificación son dos etapas distintas pero complementarias** dentro del proceso de adopción responsable de sistemas de IA.

Implementación: la base para la gestión responsable

La implementación de ISO/IEC 42001 implica integrar en la organización un sistema de gestión estructurado que aborda desde la identificación y mitigación de riesgos hasta la alineación estratégica y la cultura ética en el uso de IA. Como se abordó anteriormente, este proceso interno genera beneficios esenciales, como:

- Mejora en los controles de calidad y seguridad tecnológica.
- Reducción de riesgos legales, éticos y operativos.
- Mayor claridad en roles y responsabilidades dentro del ecosistema de IA.
- Fomento de una cultura organizacional de transparencia y responsabilidad.

Sin embargo, esta etapa depende principalmente del compromiso interno y de la disciplina organizacional para mantener las buenas prácticas.

Certificación: un sello externo que impulsa la competitividad

La certificación es un paso adicional y crucial que consiste en someter el sistema de gestión implementado a una auditoría externa por un organismo acreditado, que evalúa la conformidad con los requisitos normativos. Obtener la certificación ISO/IEC 42001 ofrece beneficios estratégicos que van más allá de la implementación:

- **Confianza y legitimidad:** La certificación otorga una evidencia objetiva y reconocida internacionalmente de que la organización no solo ha adoptado las mejores prácticas, sino que estas son verificadas y sostenidas en el tiempo. Esto fortalece la credibilidad ante clientes, socios, inversionistas y reguladores.

- **Reducción de riesgos con procesos auditables:** La certificación implica no solo la existencia de controles, sino la obligación de mantenerlos y mejorarlos mediante auditorías periódicas, garantizando la gestión continua del riesgo y evitando desviaciones o prácticas laxas.

- **Acceso a mercados exigentes:** En regiones con regulaciones avanzadas como la Unión Europea o Estados Unidos, contar con certificación ISO/IEC 42001 puede ser un requisito o una ventaja competitiva decisiva para participar en licitaciones, alianzas estratégicas y cadenas de suministro internacionales.

- **Impulso a la cultura de mejora continua:** La certificación obliga a la organización a establecer ciclos regulares de revisión, actualización y optimización de sus procesos relacionados con la IA, asegurando que la gestión evolucione conforme a los avances tecnológicos, regulatorios y sociales.

Evidencia académica y práctica

Desde una perspectiva académica, estudios como el de **Cihon et al. (2021)** han demostrado que la certificación en marcos de gestión ética y técnica no solo reduce las asimetrías de información entre actores del mercado, sino que también potencia la ética organizacional, promoviendo una adopción más responsable y confiable de la IA (fuente: arxiv.org).

En síntesis, mientras que la implementación es indispensable para construir un sistema robusto y responsable de gestión de IA, la certificación actúa como un catalizador estratégico que amplifica la reputación, reduce riesgos y abre puertas en mercados globales competitivos. Por ello, combinar ambas etapas es la mejor fórmula para que organizaciones de cualquier tamaño puedan liderar la adopción ética y segura de IA en un entorno cada vez más regulado y consciente.

Conclusiones y Reflexiones

La Inteligencia Artificial (IA) representa un eje transformador en el desarrollo social y económico de América Latina, caracterizado por un potencial significativo y desafíos estructurales que limitan su plena implementación. El análisis realizado en este estudio ha revelado la complejidad del panorama actual, donde el avance tecnológico coexiste con realidades de desigualdad, falta de infraestructura, y déficits en la educación y la regulación.

Uno de los aspectos más destacados es la necesidad imperante de establecer marcos regulatorios adecuados. **La norma ISO/IEC 42001 se presenta como una solución estratégica, no solo para vincular la innovación tecnológica con principios éticos y de gestión responsable**, sino también como una herramienta que permite estructurar ese compromiso mediante un sistema de gestión auditable y certificable. En un contexto donde la confianza pública se convierte en un elemento crucial para la aceptación de la IA, la certificación bajo esta norma puede facilitar un entorno favorable para la implementación de sistemas confiables, seguros y alineados con los valores sociales.

Es importante subrayar que la adopción de la IA no deberá ser una mera replicación de experiencias externas, sino un proceso adaptado a las realidades latinas. La capacidad de la región para formar un capital humano diverso y capaz es un reto significativo. **La falta de profesionales capacitados en tecnologías emergentes limita el desarrollo de soluciones adaptadas a las necesidades sociales y culturales del continente.** Por tanto, es imperativo fomentar una educación inclusiva en ciencias y tecnologías, promoviendo además la integración de perspectivas éticas y sociales en la formación técnica.

El camino hacia una gobernanza efectiva de la IA incluye el compromiso de todos los actores involucrados: líderes políticos, empresas, académicos y ciudadanos. La colaboración intersectorial es clave para buscar sinergias, y hacer de la tecnología una herramienta que realmente contribuya a la equidad social y a la sostenibi-

lidad ambiental. En este proceso, los esquemas de certificación ofrecen una vía concreta para alinear los esfuerzos de múltiples actores bajo un lenguaje común, verificable y reconocido a nivel internacional.

Asimismo, el informe señala que la IA puede servir como motor de innovación, brindando oportunidades para la creación de nuevos modelos de negocio y la optimización de procesos existentes. Sin embargo, las organizaciones deben ser conscientes de los riesgos asociados, como la automatización de sesgos y los dilemas éticos que surgen de la toma de decisiones algorítmicas. Implementar y certificar marcos de gestión como la **ISO/IEC 42001** permite a las empresas no solo mitigar estos riesgos, sino también demostrar un compromiso activo con la ética, la transparencia y la mejora continua, generando credibilidad tanto ante sus clientes como entre sus reguladores.

Finalmente, la reflexión que emerge de este estudio es que la IA, en su esencia, es una herramienta, y su impacto dependerá de cómo sea utilizada. La región tiene la capacidad de definir su propio destino en la era digital, posicionando su diversidad y su rica cultura como ventajas competitivas en el desarrollo de soluciones de IA innovadoras y éticas. Para alcanzar esta meta, es vital adoptar un enfoque integral que considere tanto las oportunidades como los desafíos, estableciendo un marco colaborativo que priorice el bienestar colectivo sobre intereses individuales o de corto plazo.

La fuerza transformadora de la inteligencia artificial en América Latina está en nuestras manos; con visión estratégica y el respaldo de mecanismos como la certificación, podemos asegurar que sus beneficios sean compartidos por todos y no se conviertan en nuevas fuentes de desigualdad. La invitación es clara: líderes, empresas y ciudadanía deben unirse en la construcción de un futuro donde la IA respete la dignidad humana y promueva un desarrollo sostenible para todos.

Referencias

• A-LIGN. (2025). *Understanding ISO 42001: The world's first AI management system.* https://www.a-lign.com/resources/understanding-iso-42001

• ArXiv. (2024). *Interplay of ISMS and AIMS in context of the EU AI Act.* https://arxiv.org/abs/xxxx.xxxxx

• ArXiv. (2025). *Enhancing trust through standards: A comparative risk impact framework.* https://arxiv.org/abs/xxxx.xxxxx

• Banco Interamericano de Desarrollo (BID). (2021). *Ética y regulación de IA en América Latina.*

• Banco Interamericano de Desarrollo (BID). (2022). *Guía de políticas para la IA en América Latina.*

• Banco Interamericano de Desarrollo (BID). (2023). *Tecnologías emergentes en América Latina y el Caribe: Adopción, oportunidades y desafíos*. https://www.iadb.org

• Brasil. (2023). *Marco legal da inteligência artificial. Câmara dos Deputados.* https://www.camara.leg.br

• Brynjolfsson, E., & McAfee, A. (2017). *Machine, platform, crowd.*

• CEPAL. (2022). T*ransformación digital y desarrollo productivo en América Latina.* Comisión Económica para América Latina y el Caribe.

• Cihon, P., et al. (2021). *AI certification: Advancing ethical practice by reducing information asymmetries.*

• Colombia TIC. (2022). *Marco ético para el desarrollo de la IA en Colombia.*

• European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence-act

• European Commission. (2024). *Artificial Intelligence Act.* https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence-act

• EY. (2025). ISO 42001: *Paving the way for ethical AI.* https://www.ey.com/en_gl

• Floridi, L. (2019). *Establishing the rules for building trustworthy AI.*

• G7. (2023). *Hiroshima AI Process.* https://www.g7hiroshima.go.jp

• Gartner. (2025). *C-Level Leadership Vision for 2025. Gartner Research.*

• Gobierno de Chile. (2021). *Política nacional de inteligencia artificial.*

• Gobierno de Colombia. (2012). *Ley 1581 de 2012. Protección de datos personales.*

• Gobierno Digital Colombia. (2022). *Guía de ética para servicios digitales con IA.*

• IA2030Mx. (2021). *Propuesta de política nacional de IA para México.* https://ia2030.mx

• IEEE. (2021). *Ethically aligned design for intelligent systems.*

• ISO. (2023). ISO/IEC 42001:2023 *Artificial Intelligence Management System. International Organization for Standardization.*

• ISO/IEC JTC 1/SC 42. (2023). ISO/IEC 42001:2023 – *AI management systems.* https://www.iso.org/committee/6794475.html

• Jobin, A., Ienca, M., & Vayena, E. (2019). *The global landscape of AI ethics guidelines. Nature Machine Intelligence.*

• LAVCA. (2023). *Latin American Startup Directory 2023. Latin American Venture Capital Association.*

• MIT Sloan Executive Education. (2025). *Future-Ready Enterprise Academy.*

• NIST. (2023). *AI Risk Management Framework.* https://www.nist.gov/itl/ai-risk-management-framework

• OECD. (2022). *Latin American Economic Outlook 2022: Digital Transformation for Building Back Better. Organisation for Economic Co-operation and Development.*

• OECD. (2023a). *OECD framework for the classification of AI systems.* https://www.oecd.ai

• OECD. (2023b). *AI and jobs: Evidence from labour markets in Latin America.*

• ONU. (2021). *Recomendación sobre la ética de la inteligencia artificial.*

• Oxford Insights. (2023). *Government AI readiness index 2023.* https://www.oxfordinsights.com/government-ai-readiness-index

• PwC. (2022). *AI predictions.*

• Scybers. (2025). *Introduction to ISO/IEC 42001: The first standard for AI management systems.* https://www.scybers.com/iso-42001

• Secretaria de Governo Digital. (2021). *Estratégia brasileira de inteligência artificial. Governo Federal do Brasil.*

• Sigman, J. (2025). ISO 42001: *Lessons learned from auditing and implementing the framework. Cloud Security Alliance.*

• UNESCO. (2021). *Recomendación sobre la ética de la inteligencia artificial.* https://unesdoc.unesco.org

• UNESCO. (2023). *Global investments in AI research: Challenges for the global south. United Nations Educational, Scientific and Cultural Organization.*

• White House. (2019). *Executive order on maintaining American leadership in artificial intelligence.*

• World Economic Forum (WEF). (2023). *The future of jobs report 2023.* https://www.weforum.org/reports/the-future-of-jobs-report-2023


NYCE
A QIMA COMPANY
ESR
Empresa
Socialmente
Responsable
EMPRESAS
EXCEPCIONALES