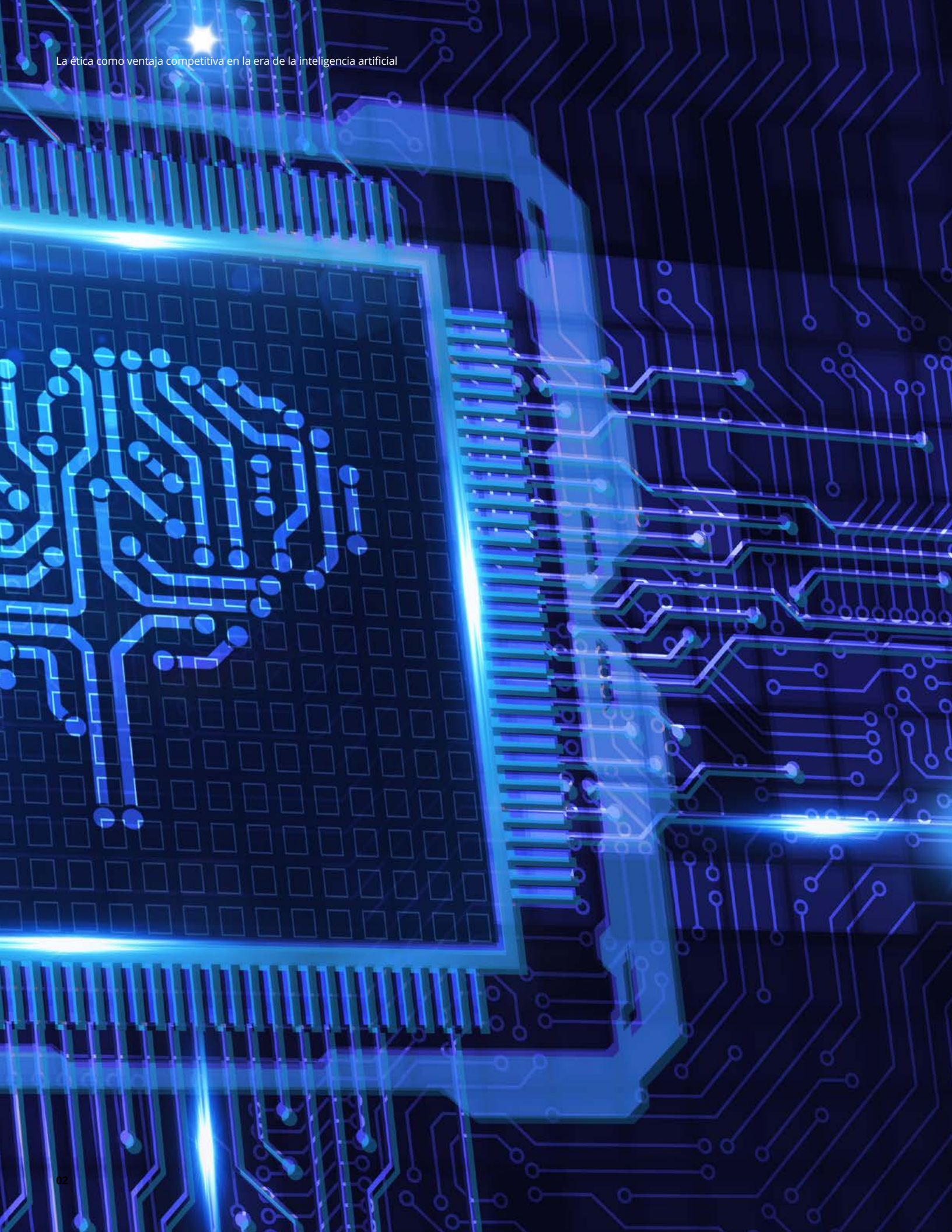
Deloitte.

La ética como ventaja competitiva en la era de la inteligencia artificial



Introducción

La inteligencia artificial (IA) se ha integrado de forma acelerada en las operaciones empresariales de todo el mundo, impulsando la automatización, la personalización y la eficiencia a gran escala. Su auge se ha visto impulsado por avances recientes (como la IA generativa y los agentes digitales), por las perspectivas de desarrollo tecnológico hacia los próximos años (como la computación cuántica) y por su creciente uso. Por ejemplo, desde 2019 la demanda en el uso de IA se disparó 130%, mientras que la proporción de grandes empresas que la utilizan se ha duplicado en los países que conforma la Organización para la Cooperación y el Desarrollo Económicos (OCDE). En paralelo, gobiernos de al menos 70 países han emitido más de mil iniciativas para abordar la IA, entre estrategias nacionales, proyectos de ley y políticas públicas[1].

Desde la automatización de procesos hasta la toma de decisiones basadas en datos, la integración de este fenómeno tecnológico en las operaciones corporativas está redefiniendo industrias completas. Sin embargo, el empleo de IA genera una polarización razonable: hay quienes abogan por una adopción acelerada para no quedar atrás, y hay quienes, con prudencia, alertan sobre los peligros de avanzar sin preparación.

Asimismo, conforme las organizaciones aceleran sus despliegues de IA, surge la pregunta: ¿podemos confiar al 100% en la inteligencia artificial? Casos sonados de algoritmos con resultados discriminatorios, decisiones opacas o uso indebido de datos han encendido las alarmas sobre los riesgos de una IA sin control ético. Para contextualizar este debate, resulta indispensable referir el trabajo de Beena Ammanath, directora ejecutiva del Instituto Global de IA de Deloitte y fundadora de *Humans for AI*, quien, en su obra *Trustworthy AI: A Business Guide for Navigating Trust and Ethics in AI*, ofrece una guía pragmática para que los líderes empresariales gestionen los riesgos relacionados con la IA. A través de su vasta experiencia en distintas industrias, Ammanath aborda las cualidades esenciales de una IA confiable y establece consideraciones éticas fundamentales que toda organización debiera atender antes de implementar soluciones inteligentes[2].

Este documento ofrece un análisis ejecutivo de los riesgos principales que enfrentan las empresas al implementar la inteligencia artificial sin una estructura de gobernanza sólida, así como al decidir por no implementarla. La premisa es clara: la IA es un imperativo actual del mercado, pero si no se administra adecuadamente, también puede convertirse en una amenaza significativa.

Entre innovación y dilemas éticos

Cada minuto, las soluciones de inteligencia artificial procesan tres mil millones de consultas en la Nube, reconfigurando industrias como la de salud y la de logística. Para asumir esto, tomamos en cuenta, por ejemplo, el estudio de MedTech Pulse y su hallazgo sobre lo que llegan a procesar las plataformas de *BigTech* y proveedores de IA solo en el ámbito sanitario: más de mil millones de preguntas de salud cada día[3]. Si aplicamos este patrón a otras industrias y a proveedores de servicios en la Nube, es razonable suponer que la IA en la Nube supera esa cifra en diversos casos de uso, como finanzas y *retail*, entre otros.

Ahora imaginemos un tablero de ajedrez en el que las piezas no son peones ni torres o alfiles, sino datos, algoritmos e infraestructuras de Nube. Cada movimiento de esta partida determina quién lidera un mercado o quién queda rezagado. La inteligencia artificial, con un crecimiento estimado de mercado de 200 mil millones de dólares para 2025 a nivel global[4], redefine la competitividad de empresas y sectores enteros. No obstante, detrás de esta promesa de eficiencia y rentabilidad, se esconden dilemas éticos que si no son abordados a tiempo pueden tener costos millonarios en multas y sanciones. Por ejemplo, cuando un algoritmo decide recortar personal sin una revisión humana exhaustiva, o cuando segmenta clientes de manera discriminatoria, surgen consecuencias que trascienden a nuestro tablero de ajedrez.

En este contexto, entender la importancia de una IA ética representa una condición para garantizar la viabilidad y la reputación de cualquier organización dispuesta a liderar en la economía digital. Al respecto, Deloitte realizó la encuesta *Technology Trust Ethics* a 100 ejecutivos corporativos en los Estados Unidos, de los cuales, 62% considera como prioridad lograr una IA que reúna criterios de transparencia, robustez y supervisión humana[5], pues, de lo contrario, asumen que un único error ético en IA podría significar pérdidas que superen 10% de sus ingresos anuales. La cifra ilustra una realidad ineludible: la IA no es solo una herramienta de optimización, sino un ecosistema que, de no manejarse con integridad, puede alumbrar sesgos, socavar la privacidad o incluso provocar graves fallos operativos.

Antes de abordar los dilemas éticos, es preciso distinguir entre desarrollo de IA y uso de IA. La diferencia radica en la clásica disyuntiva de "construir vs. comprar", ya que las empresas pueden crear sus propios algoritmos, modelos o plataformas de IA; o bien, pueden aplicar herramientas y servicios de IA de terceros en sus operaciones. Es decir, las grandes organizaciones pueden permitirse desarrollar IA cuando buscan soluciones únicas alineadas a su estrategia; mientras que las pequeñas y medianas empresas, generalmente, optan por usar herramientas ya creadas para obtener resultados rápidos con menor inversión. Cada enfoque tiene sus méritos: desarrollar IA propia puede impulsar una ventaja competitiva única; en cambio, utilizar IA existente acelera la adaptación digital y reduce riesgos iniciales. En la práctica, hay organizaciones que combinan ambas estrategias según el contexto, aprovechando lo mejor de cada una para incorporar la inteligencia artificial de manera efectiva. En tanto, implementar IA en las empresas plantea distintos dilemas éticos fundamentales, por lo que a continuación, describimos algunos:

Sesgos algorítmicos y equidad

Muchos sistemas de IA aprenden de datos históricos que pueden contener prejuicios. Sin intervenciones humanas, la IA puede perpetuar o amplificar la discriminación contra grupos por género, raza, edad u otros atributos. Por ejemplo, un algoritmo de selección de personal mal calibrado podría filtrar candidatos de cierta edad o zona geográfica, reproduciendo sesgos del pasado. La falta de imparcialidad —además de ser éticamente inaceptable— expone a la empresa a riesgos legales por discriminación.

Transparencia y explicabilidad

Con frecuencia, las decisiones de la IA ocurren dentro de una "caja negra" algorítmica. Esto dificulta entender cómo o por qué se llegó a un resultado. La falta de transparencia mina la confianza de usuarios y reguladores; además, sin explicabilidad es complejo auditar decisiones o corregir errores. De ahí lo esencial que resulta comprender y comunicar el funcionamiento interno de los modelos de IA, permitiendo que incluso quienes no son científicos de datos comprendan sus procesos y los fundamentos de cada resultado.

Privacidad de datos

La IA empresarial suele alimentarse de grandes volúmenes de datos, incluyendo información personal de clientes y empleados. Esto conlleva preguntas sobre consentimiento, anonimización y protección de la información. Un dilema común es equilibrar la personalización o eficiencia que brinda la IA con el respeto estricto a la privacidad y a regulaciones de datos (como el *Reglamento General de Protección de Datos de la Unión Europea. GDPR*, por sus siglas en inglés). Sin controles adecuados, existe el riesgo de usos indebidos o filtraciones que vulneren la confianza.

Autonomía humana y control

A medida que la IA asume tareas decisorias —desde aprobar créditos hasta diagnósticos médicos— surge la preocupación por mantener al ser humano involucrado: ¿en qué punto delegar decisiones críticas a una máquina? La autonomía de las personas puede verse comprometida si un sistema automatizado toma determinaciones sin posibilidad de apelación humana. Beena Ammanath destaca que, antes de implementar cualquier solución de IA, los líderes

empresariales deben cuestionar su necesidad y las implicaciones éticas de su uso, asegurando que siempre debe existir supervisión humana adecuada.

Responsabilidad y rendición de cuentas

Finalmente, se plantea quién es responsable de las acciones y errores de la IA. Si un algoritmo comete un fallo costoso o perjudicial, ¿responde el desarrollador, el proveedor o el usuario empresarial? La responsabilidad es un dilema crítico, ligado a la necesidad de marcos legales claros. Las organizaciones deben asumir la responsabilidad de las acciones y decisiones de sus sistemas de IA, estableciendo mecanismos de supervisión y procesos de rendición de cuentas que involucren a todas las áreas implicadas.

Si bien la discusión a menudo se centra en la imparcialidad y el sesgo, Ammanath enfatiza que la confianza en la IA abarca dimensiones adicionales que deben ser consideradas de manera holística:

- **Robustez y fiabilidad**
- **Explicabilidad y transparencia**
- **Seguridad y privacidad**
- **Responsabilidad y rendición de cuentas**
- **Responsabilidad ética**

La inteligencia artificial debe ser robusta y fiable, manteniendo su precisión y funcionalidad con el paso del tiempo y adaptándose a datos diversos y situaciones imprevistas. Para lograrlo, es fundamental someter los modelos a pruebas de estrés que aseguren su resistencia frente a cambios en la calidad de los datos o en el entorno de operación. Además, la explicabilidad y transparencia son esenciales, lo que implica diseñar modelos que permitan comunicar sus decisiones a todos los interesados, desde técnicos hasta ejecutivos o clientes. Al informar a los usuarios sobre el uso de la IA, se les permite tomar decisiones informadas respecto al intercambio de sus datos y evaluar la confiabilidad de los resultados obtenidos.

Por otro lado, la seguridad y privacidad son aspectos cruciales, ya que la IA debe operar sin causar daño físico, financiero o emocional. Proteger la información personal y garantizar que los sistemas sean resistentes a manipulaciones externas, como ataques adversarios o robo de datos, es tan importante como optimizar la precisión de los algoritmos. En este sentido, la responsabilidad y la rendición de cuentas también juegan un papel fundamental. Según Ammanath, es vital asignar roles claros sobre quién vigila el correcto funcionamiento de los sistemas de IA y quién toma acciones correctivas ante comportamientos inadecuados.

Finalmente, la responsabilidad ética debe ser una consideración primordial antes de desplegar un sistema de inteligencia artificial. Los equipos de tecnología deben preguntarse si realmente necesitan esa solución, pues el entusiasmo por implementar IA, aunque comprensible, no debería ser el motor principal para tomar decisiones sobre su adopción. Es crucial que las organizaciones evalúen la necesidad real de una solución de IA, considerando tanto su viabilidad técnica, como también las implicaciones éticas y sociales que conlleva. La presión por adoptar tecnologías emergentes no debe eclipsar el análisis crítico de si estas herramientas realmente aportan valor. Al centrar las decisiones en principios éticos y en el bienestar general, más allá del simple cumplimiento normativo, se promueve un uso de la IA que es verdaderamente responsable y beneficioso.

Este enfoque holístico subraya que no existe un conjunto único de reglas éticas aplicables a todas las implementaciones de IA. La importancia de cada dimensión varía según el contexto: en sistemas de conducción autónoma, la precisión es vital para evitar accidentes; en análisis de comportamiento en estadios deportivos, la exactitud puede ser menos crítica. Esta variabilidad obliga a evaluar cada caso individualmente, considerando sus particularidades y riesgos asociados.

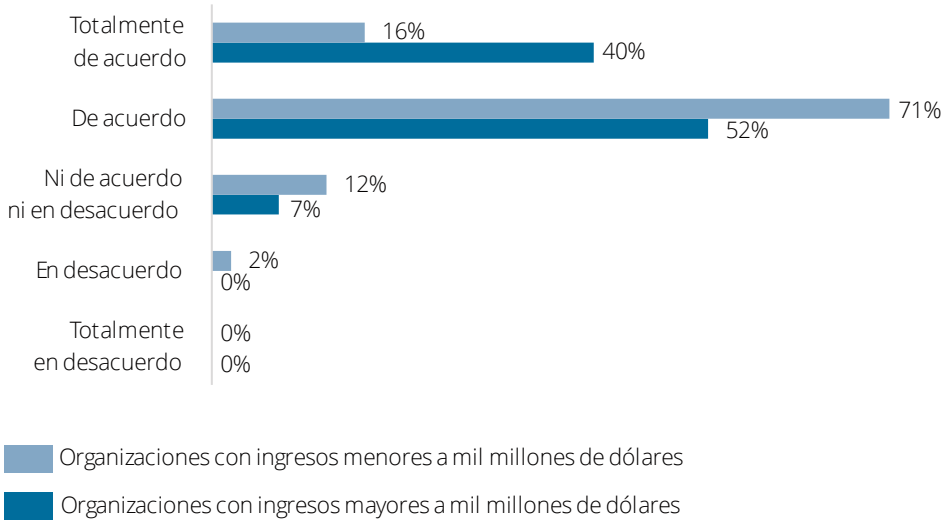
Riesgos de una IA sin gobernanza ética

No gestionar de forma adecuada la ética de la IA es tanto un problema filosófico, como un riesgo empresarial tangible. El artículo publicado por Deloitte, "Riesgos éticos en el uso de la inteligencia artificial"[6], publicado por Deloitte, destaca las principales amenazas corporativas de una IA sin la debida gobernanza ética:

- **Riesgo reputacional.** Posiblemente el más inmediato. Surge cuando clientes, empleados u otras partes interesadas perciben que el uso de IA de la empresa no está alineado con principios éticos o valores corporativos. Casos de discriminación algorítmica, decisiones opacas o violaciones de privacidad pueden erosionar la confianza en la marca. En un mundo hiperconectado, un desliz ético puede volverse "viral" y dañar la imagen de la organización a largo plazo.
- **Riesgo legal y regulatorio.** Si la IA toma decisiones contrarias a las leyes (por ejemplo, denegar servicios a colectivos protegidos) o maneja datos personales sin cumplimiento normativo, la empresa se expone a sanciones legales y acciones regulatorias. Cada vez más jurisdicciones contemplan multas cuantiosas por infracciones relacionadas con IA (tal como ocurre con la protección de datos). Por ejemplo, la *Ley de Inteligencia Artificial de la Unión Europea* establece, en su Artículo 99, sanciones económicas que clasifica en tres dimensiones: infracciones muy graves, infracciones graves e infracciones leves[7].
- **Riesgo financiero.** Una IA defectuosa o mal gobernada puede ocasionar pérdidas económicas directas. Por ejemplo, errores en sistemas automatizados de *trading* pueden costar millones en segundos, o un algoritmo sesgado podría priorizar de forma errónea inversiones. Asimismo, los costos indirectos —como retirar un producto basado en IA por falla ética o invertir urgentemente en remediar problemas— pueden ser sustanciales. Todo ello sin contar potenciales litigios o multas que golpearían los resultados financieros.
- **Riesgo estratégico.** La confianza es un activo estratégico. Si los *stakeholders* pierden la confianza en la empresa por mal uso de IA, se pueden perder oportunidades de mercado. Además, depender de modelos de IA poco fiables puede llevar a decisiones estratégicas erróneas, poniendo a la organización en desventaja competitiva. Por otro lado, las empresas que enfrenten escándalos éticos pueden ver frenada la adopción interna de IA por resistencia cultural, quedándose atrás en innovación.
- **Riesgo operativo.** Hoy, muchas operaciones críticas descansan en sistemas automatizados. Fallas o comportamientos inesperados de la IA pueden interrumpir procesos clave, desde cadenas de suministro hasta atención al cliente, causando caos operativo. Un ejemplo podría ser una IA mal entrenada que bloquea transacciones legítimas creyendo que son fraude, afectando ingresos y saturando los canales de soporte.

En síntesis, la falta de gobernanza ética en IA expone a las empresas en 360°: puede mermar la confianza pública, atraer consecuencias legales, impactar financieramente y limitar el éxito a largo plazo. Por ello, las juntas directivas y altos ejecutivos están cada vez más involucrados en supervisar estos riesgos. Retomando la encuesta *Technology Trust Ethics*, 89* de cada 100 directivos de nivel *C* creen que contar con estructuras de gobernanza ética en IA no solo mitiga riesgos, sino que mejora la innovación tecnológica dentro de la empresa. Esto refuerza la idea de que una gestión ética de la IA es parte integral de la resiliencia y la estrategia corporativas:

Los marcos éticos y las estructuras de gobernanza existentes en mi organización fomentan y apoyan la innovación tecnológica en mi organización



*En general, 89% de todos los encuestados está muy de acuerdo o de acuerdo con el planteamiento. El porcentaje incluye a las organizaciones con ingresos anuales inferiores y superiores a mil mdd.

Fuente: Recuperado de la encuesta *Technology Trust Ethics. Leadership, governance, and workforce decision-making about ethical AI: C-suite perspectives.* Deloitte 2024.

Gobernanza corporativa y buenas prácticas

Para aprovechar la inteligencia artificial de forma responsable, las organizaciones deben adoptar marcos de gobernanza de IA ética y mejores prácticas internas. A continuación, sugerimos algunas de ellas:

Comités de ética en IA. Formar instancias de gobernanza dedicadas que supervisen la implementación y uso de la IA. Un comité de ética de IA debe incluir perfiles multidisciplinarios —además de expertos técnicos, perfiles legales, de cumplimiento, recursos humanos y áreas de negocio afectadas— para analizar el impacto desde todas las perspectivas. Esta colaboración interdisciplinaria garantiza que se consideren múltiples panoramas, enriqueciendo el desarrollo y la implantación de soluciones de IA más equitativas y responsables. El comité establece una visión integral y puede asesorar en dilemas complejos, sirviendo de puente entre la tecnología y los valores corporativos.

Políticas claras, roles y responsabilidades. Desarrollar políticas internas que definan límites y directrices para el uso de IA. Además, asignar responsabilidades específicas: quién revisa y valida los modelos, quién autoriza su despliegue en ciertos casos de uso, y quién responde si ocurre un incidente. Es crucial establecer mecanismos de rendición de cuentas, pues debe saberse quién da la cara ante un fallo de IA y cómo se remediará. Al establecer estas políticas, cada organización debe evaluar sus propias necesidades y contexto, pues no es factible contar con un conjunto único de reglas éticas para todos los casos de uso; las directrices deben adaptarse a la misión, al sector y a los riesgos particulares de cada empresa.

Auditorías algorítmicas y monitoreo continuo. Implementar revisiones periódicas de los sistemas de IA para detectar y corregir sesgos u otros comportamientos no deseados. Esto incluye pruebas de equidad (verificar que las decisiones no discriminen a subpoblaciones), validación de la calidad de los datos de entrenamiento y *stress tests* de ciberseguridad. Las auditorías externas independientes también son una buena práctica para aportar objetividad. Adicionalmente, es recomendable el monitoreo en producción de los modelos, para alertar sobre desviaciones en su desempeño o resultados anómalos con implicaciones éticas.

Principios rectores y cultura organizacional. Muchas organizaciones establecen un código de principios de IA ética que guía a los equipos en el día a día. Citando nuevamente el artículo "Riesgos éticos en el uso de la inteligencia artificial": aunque cada empresa puede formular sus propios principios, suelen abarcar valores como transparencia, responsabilidad, seguridad, imparcialidad, robustez, confiabilidad y privacidad.

Estos principios se integran en la cultura corporativa mediante programas de capacitación continua a los desarrolladores, analistas y usuarios de IA, de forma que la consideración ética sea parte natural del ciclo de vida de cualquier proyecto. De acuerdo con Ammanath, la IA confiable es una responsabilidad compartida: no basta con que los científicos de datos se ocupen solos de la ética, sino que profesionales de diversas disciplinas deben participar activamente en las discusiones y decisiones para enriquecer la perspectiva y asegurar que se respeten valores corporativos y sociales.

Evaluación de impacto y enfoque "ética desde el diseño". Antes de desplegar sistemas de IA, es aconsejable realizar evaluaciones de impacto algorítmico que anticipen posibles efectos en los derechos de las personas. Este enfoque, alineado con la premisa de Ammanath, implica incorporar las consideraciones éticas desde la fase de concepción y diseño del sistema: definir desde el inicio qué datos son necesarios, cómo se procesarán, qué efectos podría tener el modelo en diferentes poblaciones y cuáles son los criterios para su eventual desactivación o ajuste. De esta manera, los equipos pueden identificar y mitigar riesgos antes de que la IA se utilice en producción.

Herramientas y controles técnicos. Apoyarse en herramientas tecnológicas para facilitar la gobernanza. Existen soluciones de auditoría algorítmica que revisan modelos en busca de sesgos, plataformas de *MLOps* (operaciones de aprendizaje automático) con controles de versión y trazabilidad, e incluso algoritmos diseñados para ser más interpretables. La inversión en estas herramientas demuestra un compromiso de la empresa por mantener sus sistemas de IA bajo control y alineados con estándares éticos. Además, integrarlas en los procesos de desarrollo agiliza la detección temprana de problemas y refuerza la robustez de las soluciones.

Implementar estas prácticas requiere liderazgo claro. Tanto el Consejo de Administración como la Dirección deben respaldarlas e integrarlas en el gobierno corporativo general, asignando recursos adecuados y definiendo métricas de éxito para la gobernanza de IA. Los Consejos y Comités de Auditoría tienen que incluir en sus agendas el seguimiento de los riesgos de IA, asegurando que los marcos de ética y gobernanza estén alineados con la estrategia de negocio y se revisen periódicamente frente a cambios tecnológicos y regulatorios.

Marcos regulatorios y normativas internacionales relevantes

El panorama regulatorio de la IA ética está evolucionando rápidamente a nivel global. De ahí que las empresas deban prestar atención a marcos legales y estándares internacionales que orientan al desarrollo y uso responsable. La Unión Europea lidera el esfuerzo regulatorio con la *Ley de Inteligencia Artificial (AI Act)*, propuesta en 2021 y con entrada en vigor en 2024 (será plenamente aplicable a partir del 2 de agosto de 2026)[8]. Se trata del primer reglamento exhaustivo sobre IA formulado por una potencia económica, el cual, establece un enfoque basado en niveles de riesgo[9]. Por lo tanto, la *AI Act* clasifica los sistemas de IA en las siguientes categorías:

- **Riesgo inaceptable:** aplicaciones prohibidas por considerarse contrarias a valores fundamentales o con potencial de daño extremo. Ejemplos: algoritmos de *social scoring* gubernamental o IA que vulnere derechos humanos básicos. Estas quedan vetadas totalmente bajo la ley.
- **Alto riesgo:** sistemas de IA que impactan significativamente la vida de las personas (por ejemplo, herramientas que evalúan CV para empleo, algoritmos usados en diagnósticos médicos, decisiones crediticias, etc.). Estos sistemas serán permitidos, pero fuertemente regulados, sujetos a requisitos estrictos de transparencia, trazabilidad, gestión de datos, supervisión humana y evaluación de conformidad. Las empresas que desarrollen o implementen IA en áreas designadas de alto riesgo deberán cumplir con estándares técnicos y pueden tener que registrar sus sistemas ante autoridades competentes.
- **Riesgo limitado y riesgo mínimo:** para aplicaciones de IA no incluidas en las categorías anteriores (por ejemplo, un filtro de *spam* o sistemas comerciales de recomendación no sensibles), la ley no impone obligaciones adicionales más allá de ciertas transparencias voluntarias. En esencia, se permite su uso con relativa libertad, aunque se alienta la autorregulación y buenas prácticas.

El objetivo principal de la *AI Act* es garantizar una inteligencia artificial segura en el mercado europeo, además de ser transparente y respetuosa de los derechos fundamentales, sin ahogar la innovación. Se le compara con el rol pionero que tuvo el *Reglamento General de Protección de Datos de la Unión Europea*, anticipando que la normativa europea de IA podría convertirse en un estándar global de facto. De hecho, su influencia ya se siente en Brasil, donde han avanzado en marcos legales nacionales inspirados en principios similares: en diciembre de 2024, el Senado de ese país aprobó un proyecto de ley para crear un marco legal de IA, en sintonía con la ola regulatoria internacional[10]. En síntesis, Europa está marcando la pauta regulatoria, y cualquier empresa que opere en su ámbito (o que provea tecnología a clientes europeos) deberá alistarse para cumplir con la *AI Act* en el corto plazo.

En contraste, Estados Unidos ha adoptado un enfoque menos centralizado y más orientado a directrices voluntarias y estándares técnicos. Hasta ahora no existe una ley federal integral sobre IA, aunque hay regulaciones sectoriales (por ejemplo, en transporte o sanidad) y recientes iniciativas del Poder Ejecutivo. Un hito importante es el *Marco de Gestión de Riesgos de IA* (*AI RMF*, por sus siglas en inglés) desarrollado por el Instituto Nacional de Estándares y Tecnología (*NIST*, por sus siglas en inglés), un reconocido organismo de estandarización en EE. UU. que, en 2023, publicó este marco voluntario para ayudar a las organizaciones a gestionar los riesgos de la IA de manera responsable y ética[11]. El *AI RMF* provee un lenguaje común y una serie de funciones (mapear, medir, gestionar y gobernar riesgos de IA) que las empresas pueden implementar para garantizar que sus sistemas sean confiables, explicables, justos, seguros y respetuosos de la privacidad[12].

Además del *NIST*, la Casa Blanca emitió en 2022 una *Carta de Derechos de la IA* (*AI Bill of Rights*, en forma de guía no vinculante) que establece principios como la protección contra algoritmos inseguros o sesgados, la no discriminación algorítmica, la privacidad de datos, explicabilidad y alternativas humanas[13]. Y, en 2023, una Orden Ejecutiva del Presidente de EE. UU. reforzó obligaciones para que desarrolladores de IA avanzados compartan resultados de pruebas de seguridad con el gobierno, entre otras medidas para asegurar una IA más segura y ética[14]. Asimismo, agencias reguladoras como la Comisión Federal de Comercio (*FTC*, por sus siglas en inglés), la Comisión para la Igualdad de Oportunidades en el Empleo (*EEOC*, por sus siglas en inglés) o la Oficina para la Protección Financiera del Consumidor (*CFPB*, por sus siglas en inglés) han advertido que aplicarán las leyes vigentes —que implican comercio justo, igualdad de oportunidades o protección al consumidor— a productos de IA que causen daño o discriminación.

Principios globales: OCDE y UNESCO

A nivel internacional, organismos multilaterales han establecido marcos de principios éticos para orientar tanto a gobiernos como al sector privado. Destaca la OCDE que, en 2019, emitió los *Principios sobre Inteligencia Artificial*, los cuales han sido adoptados ya por 47 países. Se trata del primer estándar intergubernamental en IA que, incluso, ha inspirado distintas estrategias nacionales.

En esencia, dichos principios abogan por una IA que sea innovadora y ética, alineada con derechos humanos, valores democráticos y bienestar social. Entre los valores que promueven están el crecimiento inclusivo y desarrollo sostenible; centricidad en el ser humano y equidad (la IA debe respetar la ley, derechos y valores democráticos, asegurando equidad y no discriminación); transparencia y explicabilidad; robustez, seguridad y protección; y responsabilidad clara de los actores de IA. Complementando los principios basados en valores, la OCDE emitió recomendaciones para los formuladores de políticas, que incluyen invertir en *I+D* responsable, fomentar ecosistemas de IA fiables, capacitar talento en ética de IA y cooperar internacionalmente para la gobernanza de esta tecnología[15].

Y, en aras de mantener los marcos éticos al ritmo de la tecnología, la OCDE actualizó, en 2024, los ya citados *Principios*, para abordar desafíos emergentes —como la IA generativa—, reforzando temas de privacidad, propiedad intelectual, seguridad e integridad de la información[16]. Por su parte, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) adoptó, en 2021, la *Recomendación sobre la ética de la inteligencia artificial,* con el apoyo de prácticamente todos sus Estados Miembro[17]. Esta recomendación es amplia, incorporando dimensiones de derechos humanos, diversidad cultural, medio ambiente y paz, e instando a los países a desarrollar herramientas de evaluación y planes éticos nacionales. Incluso, la UNESCO desarrolló la metodología *Readiness Assessment (RAM)* para ayudar a los gobiernos a diagnosticar su preparación en ética de IA[18].

Pese a que la UNESCO y la OCDE no imponen regulaciones, sus marcos sirven de guía y establecen un punto de referencia global que diversas empresas multinacionales están tomando en cuenta al definir sus propias políticas internas de IA.

Latinoamérica: estrategias emergentes

Todavía es incipiente la regulación específica de IA en Latinoamérica; sin embargo, hay países que han lanzado estrategias nacionales donde la ética ocupa un lugar central. México, por ejemplo, fue de los primeros en presentar, en 2018, una Agenda Nacional de IA[19]; y, en marzo de 2023, se impulsó la creación de la Alianza Nacional de IA (ANIA), un mecanismo colaborativo orientado a ajustar el debate de IA hacia lo social y lo ético, poniendo al ser humano y su bienestar en el centro. Incluso, esta coalición de expertos en IA emitió, en mayo de 2024, la Propuesta de Agenda Nacional de la Inteligencia Artificial para México 2024 – 2030, un documento que tiene como objetivo principal establecer un marco estratégico para el desarrollo y la implementación de la IA en el país, de manera que se promueva la innovación, el crecimiento económico y el bienestar social. Se trata de una agenda que busca alinear los esfuerzos del gobierno, la industria, la academia y la sociedad civil para fomentar un ecosistema de IA que sea inclusivo, ético y sostenible[20].

El énfasis mexicano —alineado con la visión de la OCDE y la UNESCO— es utilizar la IA para cerrar brechas de desigualdad y promover el desarrollo sostenible con respeto a la dignidad, los derechos humanos y los valores democráticos. En Chile, por su parte, fue publicada una *Política Nacional de IA*, en 2021, que fue actualizada tres años después y dedica capítulos a la gobernanza y aspectos éticos, estableciendo principios y acciones para un uso responsable de la IA tanto en sectores productivos como en el gobierno. Mientras que, en Brasil, el antes mencionado proyecto de ley representa un esfuerzo pionero en la región para normar la IA a la par de Europa.

Asimismo, existen esfuerzos regionales de cooperación como el Índice Latinoamericano de Inteligencia Artificial, el cual, promueve el intercambio de buenas prácticas en ética de IA, entre los 19 países de América Latina y el Caribe que lo conforman[21]. Gobiernos como el de Argentina, Colombia y Uruguay han constituido consejos asesores o grupos de expertos para recomendaciones éticas. Aunque la madurez regulatoria varía, la tendencia común en Latinoamérica es adoptar la IA con precaución y visión humanista, anticipando la futura necesidad de marcos legales más sólidos.

Para empresas que operan en la región, esto se traduce en la conveniencia de autorregularse con estándares altos (en sintonía con OCDE/UNESCO) antes de que lleguen exigencias formales, demostrando así, compromiso con las sociedades locales. Las empresas que lideren con una postura ética seguramente van a influir en la formulación de políticas públicas y ganarán legitimidad ante consumidores cada vez más conscientes.

Beneficios de una postura proactiva en ética de IA

Adoptar una perspectiva proactiva y corporativa frente a la ética de la inteligencia artificial no es solo "lo correcto", conlleva también beneficios estratégicos significativos para las organizaciones. A nivel global, pocas leyes obligan de forma expresa la emisión pública de principios éticos sobre IA; no obstante, distintos marcos regulatorios —como los antes citados— sí exigen que las empresas los desarrollen internamente como parte de su gobernanza y cumplimiento.

Ante el escrutinio social y regulatorio crecientes, la publicación de principios éticos se ha convertido en una práctica casi obligatoria para organizaciones que usan IA a gran escala. Ejemplo de ello son Google, con *Our AI Principles*[22], Microsoft con *Principles and approach*[23], y otras empresas como SAP, Meta y OpenAI que también han adoptado marcos similares para hacer públicos los principios éticos que guían el desarrollo y el uso de inteligencia artificial. Incluso, empresas como Mastercard, IBM y Telefónica, entre otras, firmaron con la UNESCO un compromiso de aplicar los valores de la ya citada *Recomendación sobre la ética de la inteligencia artificial*.

En este contexto, destacamos algunas ventajas de integrar la ética en el corazón de la agenda de IA empresarial:

Confianza de los clientes y del mercado. Una empresa que en su núcleo opera de forma cotidiana con ética las herramientas de IA, tiene la oportunidad de proyectar esas prácticas hacia afuera y, con ello, la posibilidad de generar mayor confianza en sus clientes, usuarios y aliados. La transparencia y el respeto a la privacidad, por ejemplo, son recompensados con lealtad. Una encuesta reciente de *Termly* —la plataforma integral de gestión de privacidad y cumplimiento legal parasitios web, aplicaciones y empresas— destaca que 91% de las organizaciones está dispuesto a priorizar la privacidad de los datos, si saben que ello aumentará la confianza y la fidelidad de sus clientes[24].

Diferenciación competitiva. Las empresas pioneras en establecer principios claros o en someter sus algoritmos a auditorías externas pueden promocionar ese compromiso como parte de su propuesta de valor. De hecho, un sinnúmero de ejecutivos globales señala que diferenciar su organización en productos y servicios es uno de los tres principales objetivos al invertir en prácticas responsables de IA. Es decir, ven la ética como un elemento clave para destacarse frente a la competencia. La reputación, a través de una IA ética, puede ser un poderoso intangible que atraiga clientes, socios de negocio e incluso inversionistas (cada vez más interesados en criterios Ambientales, Sociales y de Gobernanza que ahora incluyen el uso ético de la tecnología).

Innovación más sólida y sostenible. Contrario al temor de que la ética frena la innovación, la evidencia sugiere lo opuesto: la gobernanza ética adecuada impulsa la innovación. La encuesta efectuada por Deloitte y citada con anterioridad, *Technology Trust Ethics*, nos hace recordar que una mayoría de los directivos de nivel *C* está convencido de que los marcos éticos y de gobernanza de IA en sus organizaciones fomentan la innovación tecnológica. ¿Por qué? Porque una IA desarrollada dentro de límites claros y valores bien definidos tiende a ser más robusta, segura y adaptable. Los equipos que operan con lineamientos éticos tienden a explorar soluciones más creativas para lograr objetivos de negocio sin comprometer principios, lo cual, deriva en productos y servicios de mayor calidad. Además, la innovación responsable tiende a ser más sostenible en el tiempo, al evitar sobresaltos (por ejemplo, tener que retirar o rehacer proyectos por problemas éticos).

Atracción de talento y cultura organizacional positiva. Los profesionales más calificados —especialmente en tecnología— a menudo prefieren organizaciones cuyos valores se alinean con los suyos. Una empresa percibida como ética en IA atraerá y retendrá mejor a talento consciente y comprometido. Internamente, cultivar una cultura de integridad donde la gente se siente cómoda planteando preocupaciones éticas, redunda en un ambiente de trabajo más seguro y colaborativo. Empleados empoderados para tomar decisiones responsables aportan a la agilidad y resiliencia de la organización. El resultado es una fuerza laboral orgullosa de sus logros tecnológicos y, al mismo tiempo, de su impacto social positivo.

Preparación y ventaja ante regulaciones futuras. Ser proactivo en ética de IA prepara a la empresa para cumplir —e incluso superar— los requerimientos de nuevas leyes y normas. En vez de reaccionar a multas o a escándalos, las compañías éticas ya habrán internalizado prácticas alineadas con las regulaciones más estrictas (por ejemplo, documentación, evaluaciones de riesgo o gobernanza transparente). Esto les da una ventaja competitiva cuando sean implementados marcos internacionales, pues estarán listas para certificar conformidad y continuar operando sin sobresaltos, mientras competidores rezagados podrían enfrentar retrasos o sanciones por intentar ponerse al día de última hora. La ética se convierte así en un escudo estratégico contra riesgos regulatorios y jurídicos.

Conclusión

La inteligencia artificial no es una moda, es una nueva capa estructural del sistema económico. Las organizaciones, hoy, se encuentran ante la oportunidad de adoptarla y aprovechar todo su potencial; sin embargo, también enfrentan el gran desafío de regular su uso y de tratarla adecuadamente.

La IA es, en realidad, una disrupción que exige gobernanza, liderazgo ético y visión estratégica. Adoptarla sin preparación puede destruir reputaciones, generar injusticias o poner en riesgo la continuidad operativa. No adoptarla, por otro lado, implica perder clientes, competitividad y capacidad de supervivencia. El rol del Consejo de Administración debe garantizar que la organización navegue esta transición con inteligencia, prudencia y visión de largo plazo.

Es importante destacar que la ética de la IA genera grandes beneficios: crea confianza y fidelidad en los clientes —lo que, a su vez, sostiene los ingresos de las organizaciones—; diferencia positivamente a la marca; estimula la innovación responsable; atrae al mejor talento; y, blinda a la empresa ante un entorno normativo cada vez más exigente.

Las empresas visionarias entienden que la IA ética no es una limitante, sino un habilitador de ventaja competitiva en la economía digital. Como suele señalarse en los círculos de negocio, la confianza es un nuevo agregado, y, en el terreno de la IA, la ética es el motor que permite robustecer esa confianza y hacerlo sostenible.

Referencias:

1. Cámara de Tecnologías de Información y Comunicación (2024). "OCDE actualiza principios de IA para mantenerse al tanto de rápidos avances tecnológicos". CAMTIC. https://www.camtic.org/actualidad-tic/ocde-actualiza-principios-de-ia-para-mantenerse-al-tanto-de-rapidos-avances-tecnologicos/
2. Ammanath, B. (2022). *"Trustworthy. A business guide for navigating trust and ethics in AI"*. Trustworthy AI. https://trustworthyaibook.com/
3. MedTech Pulse (2022). *"BigTech's ambitions and strategies in the healthcare market"*. https://www.medtechpulse.com/article/insight/bigtechs-ambitions-and-strategies-in-the-healthcare
4. Goldman Sachs Research proyecta esta inversión en IA (hardware, software, consultoría y adopción empresarial), considerando desarrollo de modelos, expansión de infraestructura en nube y centros de datos especializados. Goldman Sachs (2023). *"AI investment forecast to approach $200 billion globally by 2025"*. https://www.goldmansachs.com/insights/articles/ai-investment-forecast-to-approach-200-billion-globally-by-2025
5. Deloitte (2024). *"Technology Trust Ethics. Leadership, governance, and workforce decision-making about ethical AI: C-suite perspectives"*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-ent-pulse-survey.pdf
6. Deloitte (2024). *Riesgos éticos en el uso de la inteligencia artificial*. https://www.deloitte.com/latam/es/services/risk-advisory/perspectives/riesgos-eticos-en-el-uso-de-la-inteligencia-artificial.html
7. EU Artificial Intelligence Act (2024). *Ley de Inteligencia Artificial. Artículo 99. Sanciones*. https://artificialintelligenceact.eu/es/article/99/
8. European Commission (2024). *AI Act*. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
9. EU Artificial Intelligence Act (2024). "La Ley de Inteligencia Artificial de la UE. Evolución y análisis actualizados de la Ley de AI de la UE". https://artificialintelligenceact.eu/es/
10. Pacheco, R. (2023). *Proyecto de Ley No. 2338*. Senado Federal, Brasil. https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720545987618&disposition=inline
11. National Institute of Standards and Technology (2023). *NIST AI Risk Management Framework (AI RMF 1.0) Launch*. NIST. U. S. Department of Commerce. https://www.nist.gov/news-events/events/2023/01/nist-ai-risk-management-framework-ai-rmf-10-launch
12. National Institute of Standards and Technology (2025). *AI RMF Development*. NIST. U. S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development
13. The White House. *Blueprint for an AI Bill of Rights*. https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/
14. Barbour, D. (2024). "Orden Ejecutiva de EE. UU. sobre inteligencia artificial exige un desarrollo seguro, confiable y de confianza". Kiteworks. https://www.kiteworks.com/es/gestion-de-riesgos-de-ciberseguridad/executive-order-ai/
15. Organización para la Cooperación y el Desarrollo Económicos (2024). *Recommendation of the Council on Artificial Intelligence*. OCDE. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
16. Cámara de Tecnologías de Información y Comunicación (2024). "OCDE actualiza principios de IA para mantenerse al tanto de rápidos avances tecnológicos". CAMTIC. https://www.camtic.org/actualidad-tic/ocde-actualiza-principios-de-ia-para-mantenerse-al-tanto-de-rapidos-avances-tecnologicos/
17. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2022). Recomendación sobre la ética de la inteligencia artificial. UNESCO. https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial
18. Lagos, A. (2024). "México avanza con su plan nacional para el desarrollo ético de la inteligencia artificial". WIRED. https://es.wired.com/articulos/mexico-avanza-con-su-plan-nacional-para-el-desarrollo-etico-de-la-inteligencia-artificial
19. Casados, D., Et al (2020). Agenda nacional mexicana de inteligencia artificial. https://wp.oecd.ai/app/uploads/2022/01/Mexico_Agenda_Nacional_Mexicana_de_IA_2030.pdf
20. Alianza Nacional de Inteligencia Artificial (2024). Propuesta de Agenda Nacional de la Inteligencia Artificial para México 2024 – 2030. ANIA. https://www.ania.org.mx/propuestadeagendanacionaldeia
21. Índice Latinoamericano de Inteligencia Artificial. *Home ILIA*. https://indicelatam.cl/
22. Google AI. *Our AI Principles*. Google. https://ai.google/principles/
23. Microsoft AI. *Principles and approach*. Microsoft. https://www.microsoft.com/en-us/ai/principles-and-approach
24. Dragutinovic, M. (2025). "La opinión de las empresas sobre la protección de datos". Termly Inc. https://termly.io/es/recursos/laboratorio-de-datos/opinion-de-las-empresas-sobre-la-privacidad-de-datos/

Contacto

Pablo Peso
Socio de *Engineering and Operations*
Deloitte Spanish Latin America
ppeso@deloitte.com

Deloitte.