IAI Chile

PROSPECTUS.

Riesgos de la **Inteligencia Artificial**

y el Rol de los Directorios para un despliegue responsable

Agosto 2026



en colaboración con: INSTITUTO DE DIRECTORES DE CHILE

Índice

01 Introducción

02 ¿Por qué la Inteligencia Artificial es un tema de Directorios y no solo de Gerencias?

03 ¿Qué es Gobierno de IA?

04 ¿Cuáles son los Riesgos de la IA?

05 Mapa de riesgos de IA: Herramienta de Priorización y Visión de Portafolio

06 Rol y deberes del Directorio frente a la IA

07 Estructura de Gobernanza propuesta

08 El rol de la auditoría interna y externa como mecanismo de aseguramiento sobre IA

09 Principios y normativas nacionales e internacionales

10 Casos ilustrativos

11 Conclusiones y recomendaciones

Sobre los Autores de este documento

Fuentes consultadas

Anexos

- Ejemplos de Metodología de Gestión de Riesgos de la IA desde el rol del Directorio
- Actuación del Directorio ante distintos Riesgos de la IA
- Checklist de autoevaluación para el Directorio
- Agenda tipo para el Directorio
- 8 preguntas clave que todo Directorio debería hacerle a la Administración



IAI Chile

PROSPECTUS.

Alcance del documento: Este documento es una síntesis de los principales riesgos de la Inteligencia Artificial (IA) que un Directorio debe conocer, supervisar y controlar. Su propósito central es servir como una guía de gobierno para la toma de decisiones estratégicas, moviendo la conversación de la IA desde un ámbito meramente técnico hacia una responsabilidad fiduciaria y de alta dirección. El documento busca cerrar la brecha entre la velocidad del despliegue de la IA y la madurez de su gobierno corporativo, entregando al Directorio el lenguaje y las preguntas necesarias para ejercer su deber de cuidado.

Este documento contiene y está centrado en aspectos de Visión Estratégica y de Gobierno, Taxonomía y Mapa de Riesgos, Marco de Gobernanza, Herramientas prácticas para los Directorios, Contexto Regulatorio y de Aseguramiento.

Este documento no es un Manual Técnico. No es un documento instructivo sobre la implementación tecnológica, programación o arquitectura de sistemas de IA. Tampoco contiene un listado exhaustivo de Riesgos, se define como una "guía referencial" basada en la experiencia empírica actual. Debido a la velocidad del avance tecnológico, el documento advierte que el listado de riesgos no es total y probablemente se incrementará con el tiempo. Así como tampoco contiene otras Materias Materiales de la IA: El alcance está acotado específicamente a la gestión de riesgos. Aunque la IA genera otros asuntos materiales para la agenda de un Directorio (como oportunidades de innovación o eficiencia operativa pura), estos no son el foco principal de este texto.



en colaboración con: INSTITUTO DE DIRECTORES DE CHILE

Prólogo

Gobernar la Inteligencia Artificial: entre la prudencia y la transformación

La irrupción de la Inteligencia Artificial (IA) en el mundo empresarial no constituye una proyección de futuro ni una tendencia pasajera: es hoy una infraestructura crítica y una fuerza transformadora que expone a las organizaciones a un escenario de alta incertidumbre. En un entorno donde las certezas que antes orientaban la toma de decisiones han perdido vigencia, los directorios enfrentan un desafío ineludible: definir criterios de inversión sobre tecnologías y mercados que se encuentran en pleno proceso de formación.

Desde el Instituto de Directores de Chile (IdDC), hemos constatado que la principal dificultad de los directorios no radica en la falta de urgencia por innovar, sino en la ausencia de un entendimiento cabal de los riesgos fiduciarios asociados a la IA, que abarcan desde la ciberseguridad y la ética de datos hasta la eventual obsolescencia del propio modelo de negocio. Dotar a una organización de herramientas de inteligencia artificial sin desarrollar en paralelo las capacidades de su liderazgo equivale, en la práctica, a automatizar la ineficiencia. Por ello, sostenemos que la primera inversión que debe aprobar un directorio no es tecnológica, sino formativa: la de su propio board y su primera línea ejecutiva.

Tradicionalmente, la gobernanza corporativa se ha entendido como un conjunto de normas y resguardos destinados a prevenir errores. Sin embargo, en el actual contexto de cambio acelerado, esa concepción resulta insuficiente. Las organizaciones que hoy logran avances significativos son aquellas que han transformado su gobernanza en un motor activo del cambio. Frente a la transformación digital, corresponde a cada directorio evaluar si su marco de gobierno corporativo impulsa la estrategia o, por el contrario, limita su desarrollo.

Esto no implica que los directores deban adquirir competencias técnicas de programación, sino que recuperen la conducción estratégica de sus organizaciones. El ejercicio efectivo del gobierno de la IA supone una evaluación permanente de su valor estratégico, la validación de los estándares de seguridad en cada etapa de su aplicación y el monitoreo continuo de su robustez, de manera de avanzar con velocidad, seguridad y escalabilidad.



IAI Chile PROSPECTUS.

en colaboración con: INSTITUTO DE DIRECTORES DE CHILE

La inteligencia artificial transformará, sin excepción, a todas las industrias. La pregunta que corresponde a cada directorio no es si dicha transformación ocurrirá, sino si será capaz de liderarla, gobernándola como una capacidad estratégica. Ello exige incorporar formalmente la IA en la agenda del directorio, elevar la calidad de las decisiones a través de métricas periódicas, anticipar riesgos emergentes y capturar oportunidades con una visión de largo plazo.

En este contexto, el Instituto de Directores de Chile (IdDC) valora especialmente el documento que hoy se presenta, elaborado por el Instituto de Auditores Internos de Chile y el equipo de Prospectus, en colaboración con nuestra institución. Este trabajo constituye una guía práctica orientada a fortalecer el ejercicio de la responsabilidad fiduciaria y el deber de cuidado, a través del modelo de las tres líneas y de la definición de un apetito de riesgo claro. Gobernar hoy no significa administrar la certeza, sino contar con el criterio, la claridad y la responsabilidad necesarios para construir, en medio de la volatilidad, organizaciones sostenibles, resilientes y preparadas para el futuro.

Junto con ello, en un entorno de creciente competitividad, la diferencia no estará dada por quién adopte primero una tecnología, sino por quién logre desarrollar las habilidades, la cultura y el liderazgo necesarios para integrarla con éxito. Los directorios están llamados a asumir un rol activo, promoviendo organizaciones en las que la tecnología amplifique el potencial humano en lugar de sustituirlo. Conocer y gestionar los riesgos constituye, en este sentido, el primer paso indispensable para transformar la incertidumbre en una ventaja competitiva real.

Reafirmamos, desde el Instituto de Directores de Chile (IdDC), nuestro compromiso con el fortalecimiento del buen gobierno corporativo como base para el desarrollo sostenible del país.

Fadua Gajardo
Directora Ejecutiva
Instituto de Directores de Chile (IdDC)



en colaboración con: INSTITUTO DE DIRECTORES DE CHILE

01 Introducción

La Inteligencia Artificial como Imperativo Estratégico

La Inteligencia Artificial (IA) ha dejado de ser un proyecto experimental para convertirse en una infraestructura operativa crítica que define la competitividad y sostenibilidad de las organizaciones modernas. No obstante, la velocidad de su despliegue ha superado con creces la madurez de los marcos de gobierno corporativo, generando una brecha donde se materializan riesgos que pueden comprometer el valor total de la compañía.

Por esta razón, desde el Think Tank **Prospectus** junto al **Instituto de Auditores Internos de Chile,** hemos convocado a distintos profesionales de empresas líderes de la industria para reflexionar y desarrollar este documento guía para Directores, que pone en valor los temas clave que se deben gestionar desde el Gobierno Corporativo.

Históricamente, la tecnología se ha gestionado como un asunto operativo delegado a las gerencias. Sin embargo, la IA rompe este paradigma debido a tres factores fundamentales: materialidad, ya que sus decisiones afectan ingresos y derechos a una escala sin precedentes; opacidad, dado que los modelos generativos pueden actuar de forma difícil de trazar; y responsabilidad, puesto que ni la complejidad técnica ni la tercerización eximen al Directorio de responder por sus resultados. Por ello, este documento establece con claridad que la IA es un riesgo de Directorio, no solo de TI, con impactos potenciales de carácter estratégico, regulatorio, reputacional y financiero.

La supervisión de la IA ya no es opcional. A nivel internacional, normativas como el EU AI Act imponen sanciones severas de hasta el 7% de la facturación global, mientras que en Chile, la Nueva Ley de Protección de Datos Personales, la Política Nacional de IA y la Ley Marco de Ciberseguridad elevan la responsabilidad legal corporativa, con multas que pueden alcanzar los ingresos globales o incluso arriesgar la disolución de la sociedad. En este contexto, el Directorio debe ejercer su deber fiduciario de cuidado, asegurando que el uso de la IA se mantenga dentro de un apetito de riesgo aprobado y alineado con los valores de la organización.

01 Introducción

Este texto no es un manual técnico de implementación; es una guía de gobierno para la toma de decisiones estratégicas. Su relevancia radica en entregar a la mesa directiva el lenguaje, las herramientas y la estructura de gobernanza necesaria (basada en el modelo de las "tres líneas") para supervisar un despliegue responsable.

En definitiva, **la adopción de IA no puede avanzar a mayor velocidad que la capacidad de la organización para visibilizar y controlar sus riesgos.** El rol del Directorio no es operar la tecnología, sino aprobar el marco de principios y control dentro del cual la administración diseña y despliega la IA, garantizando un crecimiento ético, resiliente y creador de valor a largo plazo.

La visión de los Directores permitirá que este despliegue se realice de forma responsable, acotando la probabilidad de materialización de riesgos al exigir mediciones concretas y al tener un rol activo de gobernanza. El Director que exige KPIs e indicadores de riesgo (KRIs) específicos para la IA disminuye brechas de gobernanza, asegurando que aunque la Alta Dirección reporte que 'todo va bien', esto se deberá evidenciar explícitamente con los resultados del uso de la IA y su adecuada gestión de riesgos.

Un Directorio formado en los temas estratégicos de la IA puede ejercer adecuadamente su rol. No necesita ser experto técnico, pero sí comprender los conceptos clave para hacer las preguntas correctas.

Esperamos que este documento inicial entregue a los Directorios una guía estratégica para cumplir adecuadamente su rol en un despliegue responsable que permita que el uso de la Inteligencia Artificial en las organizaciones acumule valor y no solo acumule riesgos.

02

¿Por qué la **Inteligencia Artificial** es un tema de Directorios y no solo de Gerencias?

02 ¿Por qué la **Inteligencia Artificial** es un tema de Directorios y no solo de Gerencias?

La IA ya no es únicamente una herramienta tecnológica u operacional, porque puede afectar la estrategia, el modelo de negocio, la reputación, el cumplimiento, las personas y la sostenibilidad de la organización.

La adopción de inteligencia artificial dejó de ser un proyecto experimental para convertirse en infraestructura operativa. La velocidad de despliegue supera con creces la madurez del gobierno, y es precisamente en esa brecha donde se materializan los riesgos.

Chile aún no cuenta con una ley específica de inteligencia artificial, sin embargo, el uso de la IA ya está siendo traslapado por la normativa vigente relacionada con la protección de datos personales, ciberseguridad y con la Política Nacional de IA.

En Europa, el EU AI Act, vigente desde agosto de 2024, establece obligaciones legales específicas para las organizaciones que usan IA de alto riesgo, con sanciones de hasta el 7% de la facturación global anual. ISO/IEC 42001 establece requisitos de gobernanza de IA certificables. Los marcos de gobierno corporativo internacionales (OCDE, FSB, BIS) ya incluyen la supervisión de IA como expectativa para los directorios.

Tradicionalmente la tecnología se ha tratado como un asunto de gestión, no obstante, la IA rompe ese paradigma por las siguientes razones: **i) materialidad:** sus decisiones afectan ingresos, costos, clientes y derechos de las personas a una escala y velocidad que pueden comprometer el valor de la compañía; **ii) opacidad y autonomía:** los modelos generativos y los agentes influyen en las decisiones de forma difícil de explicar y trazar, lo que erosiona los controles tradicionales y; **iii) responsabilidad:** ni la complejidad técnica ni la tercerización eximen a las organizaciones, ni a su directorio, de responder por los resultados.

Es en este contexto que el rol del directorio no es operar la IA, sino aprobar el marco (principios, apetito de riesgo, estructura y rendición de cuentas), dentro del cual la administración diseña, despliega y disponibiliza los mecanismos de aseguramiento independientes que verifiquen que el referido marco funciona.

03 ¿Qué es **Gobierno** de IA?

03 ¿Qué es **Gobierno** de IA?

El **gobierno de la IA** es el conjunto de estructuras, políticas, roles, procesos y controles mediante los cuales una organización dirige, supervisa y rinde cuentas sobre cómo desarrolla, adquiere, despliega y usa sistemas de inteligencia artificial. No es lo mismo que "gestionar" la IA día a día (eso lo hace la Gerencia y equipos técnicos); gobernar la IA es definir **quién decide qué, con qué límites y cómo se supervisa que se cumplan.**

Elementos centrales

a. Estructura de roles y responsabilidades

- Quién aprueba el uso de un modelo de alto impacto (Directorio, Comité, Gerencia).
- Quién es "dueño" de cada sistema de IA (accountability individual, no difusa).
- Si existe un Comité de IA, un Chief AI Officer, o si la responsabilidad está repartida entre TI, Datos, Riesgos y Legal.

b. Políticas y principios

- Qué usos de IA están permitidos, cuáles requieren aprobación especial y cuáles están prohibidos.
- Principios rectores: equidad, transparencia, explicabilidad, privacidad, seguridad, supervisión humana.

c. Apetito de riesgo y líneas rojas

- Umbrales aceptables de riesgo por categoría (sesgo, privacidad, seguridad).
- Líneas rojas no negociables (ej. "no se automatizan decisiones que afecten derechos fundamentales sin supervisión humana").

03 ¿Qué es **Gobierno** de IA?



d. Gestión del ciclo de vida del riesgo

- Identificar riesgo inherente > controles > efectividad > riesgo residual > comparar con apetito > tratar > asignar responsable y plazo.

  (nota: en los anexos se pueden revisar ejemplos de la gestión del ciclo de vida del riesgo y el rol del Directorio en esta materia).

e. Cumplimiento normativo

- Alineación con regulaciones aplicables (ej. ley de protección de datos, normativa sectorial financiera/salud).
- Trazabilidad y documentación para auditorías o requerimientos regulatorios.

f. Supervisión y reporting

- Inventario actualizado de sistemas de IA en uso.
- Reportes periódicos a Comité/Directorio con indicadores objetivos.

¿Por qué no es solo "compliance" o "ética"?

Muchas organizaciones lo reducen erróneamente a un tema legal o de principios éticos. El gobierno de la IA es más amplio: es **gobierno corporativo aplicado a un tipo de riesgo específico,** con la misma lógica de rendición de cuentas que se exige para riesgos financieros o de ciberseguridad, con la diferencia de que la IA introduce riesgos nuevos (opacidad del modelo, deriva en el tiempo o dependencia de terceros) que exigen ajustes al marco tradicional.

04

¿Cuáles son los **Riesgos** de la IA?

04 ¿Cuáles son los **Riesgos** de la IA?

Riesgos emergentes específicos de IA Generativa y Agéntica

Los riesgos de la Inteligencia Artificial son una historia en desarrollo, que se ha ido escribiendo en la medida que casos empíricos muestran donde el uso de este tipo de tecnologías podrían generar daños materiales a las organizaciones. El siguiente listado está basado en la experiencia empírica de los autores de este documento así como la bibliografía documentada por distintas organizaciones a nivel internacional. No es un listado exhaustivo, sino una guía referencial que busca poner a disposición de los Directorios una base para su gestión; Sin embargo, este listado probablemente se irá incrementando en el tiempo, en la medida que más casos de uso en las organizaciones y el avance acelerado de las herramientas de inteligencia artificial nos muestren otros riesgos adicionales que se debiesen incorporar.

Alucinaciones

Los modelos generativos producen información falsa con alta confianza aparente. Si se usa sin validación humana para decisiones de negocio, el daño puede ser material.

Opacidad del razonamiento

El razonamiento de un LLM no es reconstruible. Sin capturar prompts, inputs, outputs y versiones, no es posible demostrar que un control operó como fue diseñado.

Shadow AI

Herramientas como ChatGPT o Copilot se adoptan sin autorización formal. Implica datos corporativos fluyendo hacia terceros sin control. Un inventario de uso de IA es prerrequisito para cualquier gobernanza.



04 ¿Cuáles son los **Riesgos** de la IA?

Manipulación de prompts (Prompt Injection)

Usuarios maliciosos pueden manipular instrucciones de un sistema AI para extraer información confidencial o evadir controles.

Velocidad de cambio

Los modelos se actualizan continuamente. Los ciclos de auditoría tradicionales no siguen el ritmo. Se requiere monitoreo continuo.

Dependencia de terceros

- Visibilidad limitada sobre procesamiento interno de datos.
- Cambios unilaterales en modelos del proveedor sin aviso.
- Garantías ambiguas de privacidad y retención.
- Lock-in con costos de migración elevados.

Riesgo de procesos

AI incorporar IA de forma escalada en una organización se rediseñan procesos. El problema es que el proceso originalmente documentado, ya no es válido. El nuevo proceso no está documentado, no se identifican ni evalúan los riesgos y no se consideran los controles adecuados, aumentando la exposición al riesgo de la empresa sin que nadie se dé cuenta.

Riesgos intrínsecos asociados a la IA

Falta de regulación, modelo, comercialización (extraer datos para fines comerciales), errores en los algoritmos, falsos positivos, deriva de modelo (model drift).



04 ¿Cuáles son los **Riesgos** de la IA?

Riesgos de Ciberseguridad

Phishing avanzado, Deepfake, Malware con IA, ataques automatizados, Ingeniería social avanzada, ataques a la IA, desinformación masiva, autenticación vulnerable.

Riesgo Reputacional

Contenido incorrecto o inapropiado generado por IA puede dañar la imagen de la empresa. Errores humanos que no configuran los procesos agénticos con la información adecuada o la información está desactualizada, genera respuestas incorrectas para los usuarios internos y/o clientes.

Cumplimiento Regulatorio

Se refiere a la probabilidad de infringir leyes, regulaciones o políticas de la compañía. Protección de datos ¿Qué datos se recopilan?, ¿Quién los recopila?, ¿Cómo los usa la IA? Riesgo de filtrar información confidencial o sensible, mal usar la información o almacenar fuera de la regulación, gestión del consentimiento.

Sesgos Algorítmicos

Decisiones o respuestas inclinadas o injustas, debido a los datos o supuestos con los que fue entrenada. Aprende de datos con prejuicios o incompletos, Refleja errores humanos o históricos, Generaliza mal ciertos patrones. Ej. Scoring que favorece a un tipo de cliente porque así eran los datos pasados.

Falta de conocimiento actualizado

La IA puede dar información desactualizada o incompleta.



04 ¿Cuáles son los **Riesgos** de la IA?

Riesgos de Integraciones

Uso de herramientas no autorizadas que no se integran bien, generando errores y brechas de seguridad.

La adopción de IA generativa y agéntica no puede avanzar a mayor velocidad que la capacidad de la organización para visibilizar y controlar sus riesgos, debido a que compromete la confidencialidad corporativa, la calidad de las decisiones y la responsabilidad indelegable de la mesa directiva.

Para asegurar un despliegue responsable de la IA en las organizaciones el Directorio debe tener un rol protagonista en establecer las pautas de gobernanza que permita claridad en las directrices y modo de funcionar, así como definir qué casos de uso de IA requieren toma de conocimiento, aprobación o supervisión directa del directorio y cuáles pueden gestionarse en la administración, de acuerdo a criterios definidos de materialidad y escalamiento.

Ejemplos de riesgos que debiesen llegar al Directorio, dada la implicancia que revierte para las organizaciones:

- Impacto financiero o reputacional material;
- Uso de datos personales o sensibles;
- Decisiones automatizadas que afecten derechos de personas;
- Autonomía relevante del sistema;
- Criticidad para la continuidad operacional;
- Exposición directa a clientes;
- Dependencia significativa de terceros;
- Efectos sobre estados financieros o cumplimiento regulatorio.



05 **Mapa de riesgos de IA:** Herramienta de Priorización y Visión de Portafolio

en colaboración con: INSTITUTO DE DIRECTORES DE CHILE

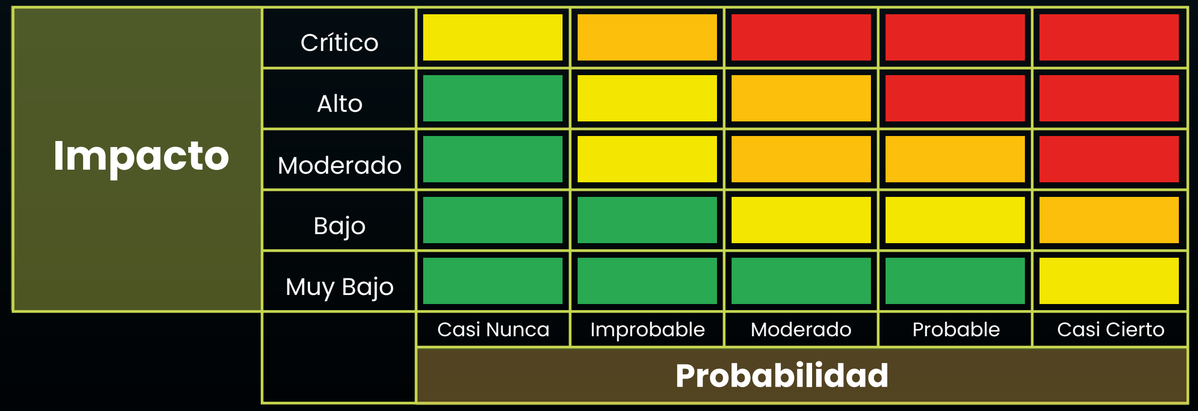
05 **Mapa de riesgos de IA:** Herramienta de Priorización y Visión de Portafolio

El mapa de riesgos es una herramienta visual de gestión, que permite a la Alta Dirección y al Directorio evaluar ágilmente la probabilidad y los distintos tipos de impacto de los riesgos que enfrentan las organizaciones.

Su valor en el gobierno corporativo combina dos enfoques complementarios reconocidos globalmente (ISO 31.000 y COSO ERM), asegurando que la exposición total al riesgo se mantenga alineada con los objetivos del negocio y el apetito de riesgo aprobado.

Metodología y Características del Mapa de Riesgos: IA como Riesgo Estratégico

El Mapa de Riesgos destinado al Directorio ("Tone at the top") debe integrarse en un marco metodológico lo suficientemente amplio como para evaluar los sistemas de IA de manera integral. Esta herramienta debe mantener la estructura y consistencia de la metodología corporativa vigente en la organización, incorporando impactos específicos que permitan abordar adecuadamente los riesgos asociados a la IA. En este sentido, la Inteligencia Artificial Agéntica y Generativa debe ser considerada y gestionada como un riesgo estratégico.



05 **Mapa de riesgos de IA:** Herramienta de Priorización y Visión de Portafolio

El directorio no requiere entender cómo funciona un modelo de Inteligencia Artificial. Necesita ver dónde la IA puede generar valor y/o exposición material para la organización, en un lenguaje que conecte con sus responsabilidades fiduciarias.

Principio rector: El mapa de riesgos para el directorio debe responder "¿Qué puede salir mal?, ¿Quién es el responsable?, ¿Dónde nos puede impactar?" y su construcción debe ser transversal considerando los distintos marcos que establecen riesgos legales (normativa vigente relacionada con la protección de datos personales, ciberseguridad y con la Política Nacional de IA).

Seis dimensiones de impacto para el Directorio

Con el propósito de garantizar la gobernanza y una supervisión estratégica en la adopción de la IA, la metodología de gestión de riesgos debe considerar la evaluación del riesgo a través de al menos las siguientes dimensiones de impacto:

Financiero y Económico

- Costos de implementación y mantenimiento que superan el retorno esperado.
- Pérdidas por decisiones automatizadas erróneas (ej. un modelo de scoring crediticio que aprueba créditos a clientes de alto riesgo).
- Multas o sanciones económicas derivadas de un mal uso del sistema.

Reputacional

- Sesgos discriminatorios de un modelo que se hacen públicos y generan controversia mediática.
- Pérdida de confianza de clientes por respuestas inapropiadas de un chatbot.
- Percepción negativa por falta de transparencia en cómo la IA toma decisiones que afectan a las personas.

05 **Mapa de riesgos de IA:** Herramienta de Priorización y Visión de Portafolio



Legal y Regulatorio

- Incumplimiento de normativas de protección de datos (ej. tratamiento indebido de datos personales por un modelo).
- Falta de cumplimiento con marcos regulatorios de IA (ej. AI Act europeo, u otras regulaciones locales).
- Riesgos de propiedad intelectual al usar contenido protegido para entrenar modelos.

Continuidad Operacional

- Caída o mal funcionamiento de un sistema de IA crítico para procesos productivos (ej. un modelo de detección de fraude que deja de operar).
- Dependencia excesiva de un único proveedor de IA (vendor lock-in) que interrumpe el servicio.
- Fallas en la infraestructura que soporta los modelos, afectando la disponibilidad del servicio.

Social (impactos internos en colaboradores y externos en la comunidad)

- Interno: desplazamiento o reconversión laboral de colaboradores por automatización de tareas.
- Externo: exclusión de ciertos grupos de la comunidad por sesgos algorítmicos (ej. en acceso a servicios financieros o de salud).
- Cambios en las dinámicas de trabajo que afectan el bienestar de los equipos.

Medioambiental

- Alto consumo energético y huella de carbono asociada al entrenamiento y operación de modelos de gran escala.
- Uso intensivo de recursos hídricos en centros de datos.
- Necesidad de evaluar proveedores de infraestructura con compromisos de sostenibilidad.

05 **Mapa de riesgos de IA:** Herramienta de Priorización y Visión de Portafolio



Este enfoque multidimensional proporciona al Directorio la visibilidad requerida para tomar decisiones informadas, salvaguardando el valor de la compañía y asegurando un despliegue tecnológico, ético y resiliente.

Evaluar la IA únicamente por su eficiencia técnica, ignorando sus impactos legales, reputacionales y sociales, expone al Directorio a asumir contingencias severas que vulneran su deber fiduciario de cuidado y protección del valor corporativo.

Mapa de calor y Tolerancia al Riesgo

La tolerancia al riesgo representa el nivel de riesgo que la Compañía está dispuesta a asumir para cumplir con sus objetivos estratégicos y su misión, así como para preservar y crear valor.
Para operativizar este parámetro, el Directorio debe establecer el mapa de calor corporativo, definiendo las zonas de tolerancia a través de rangos de criticidad que van desde niveles aceptables o tolerables hasta zonas críticas e inaceptables. Los riesgos asociados a la IA deben integrarse explícitamente en este marco para asegurar su ciclo completo de gestión: identificación, evaluación, priorización, formulación de estrategias de respuesta y seguimiento continuo.

Este tema revierte una especial relevancia para los Directorios, debido a que una tolerancia mal evaluada, podría tener impactos en sustentabilidad y sostenibilidad: El uso de inteligencia artificial (IA) ligado a la Protección de Datos Personales (PDP) o al Modelo de Prevención de Delitos (MPD) eleva el riesgo legal corporativo. Si una empresa usa IA sin control y comete delitos económicos o fallas graves de ciberseguridad, arriesga sanciones drásticas como multas de hasta UTM 40.000 o la disolución de la sociedad bajo la ley chilena de responsabilidad penal.

Nota: El Directorio debe establecer una supervisión cercana al riesgo.

06 Rol y **deberes del Directorio** frente a la IA

06 Rol y **deberes del Directorio** frente a la IA



El gobierno de la IA es una responsabilidad indelegable del Directorio. Su rol es aprobar el marco dentro del cual la administración diseña y despliega la IA, en concordancia con los principios de uso ético, como por ejemplo el definido en la Política Nacional de IA.

Una gobernanza efectiva de IA requiere una estructura clara de roles, responsabilidades y mecanismos de supervisión. El Directorio no necesita gestionar la IA directamente, pero sí debe asegurar que la arquitectura de gobierno es adecuada al nivel de riesgo de la organización.

En concreto, dentro del Rol del Directorio están las siguientes funciones:

a) Aprobar políticas y principios.

Aprobar una política y principios de IA responsable (transparencia, equidad, supervisión humana, seguridad).

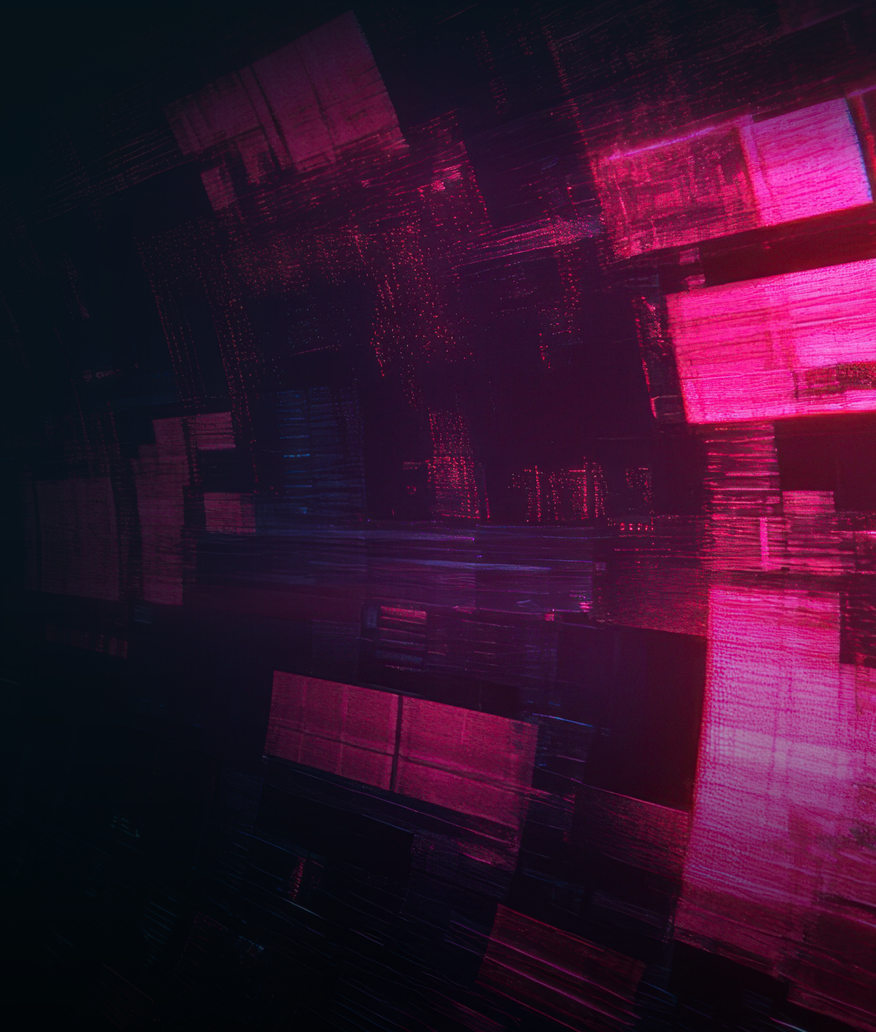
b) Asignar la supervisión y responsabilidades.

Definir explícitamente qué temas de IA corresponden al pleno del Directorio, cuáles a un comité (auditoría o riesgos) y cuáles son operativos de la administración.

c) Establecer el apetito de riesgo.

Fijar los límites de riesgo aceptable, incluidos los usos prohibidos o que requieren aprobación reforzada como la del Directorio (p. ej., decisiones autónomas de alto impacto o tratamiento de datos sensibles).

06 Rol y **deberes del Directorio** frente a la IA



d) Asegurar competencias del Directorio para ejercer una supervisión informada.

El Directorio debe procurar disponer del conocimiento suficiente, ya sea vía formación o incorporación de asesores expertos, para ejercer una supervisión efectiva, evitando depender únicamente de la administración.

e) Asignar recursos, responsables y rendición de cuentas.

Velar por que exista financiamiento, estructura de gobierno (p. ej., comité de IA o función de IA responsable) y responsables claramente identificados que rindan cuenta.

f) Exigir aseguramiento independiente.

Encargar a la Auditoría Interna, directamente o a través de un outsourcing, un plan de aseguramiento sobre IA y revisar sus hallazgos.

g) Supervisar a la Administración y reevaluar.

Recibir reportes periódicos con métricas, casos de uso de mayor riesgo, incidentes y evolución regulatoria (incl. el avance del proyecto de ley de IA) y ajustar el marco conforme la tecnología avanza.

06 Rol y **deberes del Directorio** frente a la IA

Preguntas que el Directorio debería considerar

Área de responsabilidad	Preguntas que el directorio debe poder responder	Frecuencia de revisión
Estrategia de IA	● ¿Tenemos una estrategia de IA aprobada, con objetivos, riesgos y horizonte temporal? ● ¿El uso de IA está alineado con el propósito y valores corporativos? ● ¿Se revisa la estrategia de IA ante cambios regulatorios o tecnológicos significativos?	**Anual**
Gobernanza y responsabilidad	● ¿Existe un responsable ejecutivo de IA (CAIO o equivalente) con mandato claro? ● ¿Hay un comité de gobernanza de IA con participación del directorio? ● ¿El directorio recibe informes periódicos sobre riesgos y desempeño de IA?	**Trimestral**
Gestión de riesgos	● ¿Los riesgos de IA están integrados en el mapa de riesgos corporativo? ● ¿Existen controles implementados y auditados para los riesgos críticos? ● ¿Tenemos un proceso de gestión de incidentes específico para IA?	**Semestral**
Cumplimiento regulatorio	● ¿Están todos los sistemas IA clasificados según la normativa aplicable? ● ¿Tenemos un inventario de cumplimiento actualizado por sistema y jurisdicción? ● ¿Existe un proceso para adaptarnos a nuevas regulaciones de IA con anticipación?	**Semestral**
Ética y derechos humanos	● ¿Existe una política de ética de IA aprobada por el directorio y comunicada? ● ¿Se realiza evaluación de impacto ético y en derechos humanos antes de desplegar IA? ● ¿El comité de ética tiene poder real de veto sobre despliegues controvertidos?	**Anual**
Auditoría e independencia	● ¿La auditoría interna tiene competencias y recursos para auditar sistemas de IA? ● ¿Se realizan auditorías externas de sistemas IA de alto riesgo? ● ¿Los auditores de IA reportan directamente al directorio sin filtros ejecutivos?	**Anual**

07 Estructura de **Gobernanza** propuesta

07 Estructura de **Gobernanza** propuesta

Modelo de tres líneas aplicado a IA

La estructura de gobernanza de IA se articula sobre el modelo de tres líneas, adaptado a la complejidad y dinamismo de los sistemas algorítmicos. Cada línea ejerce un rol específico con responsabilidades claramente delimitadas, según se detalla a continuación:

Línea	Rol en IA	Responsabilidades
1ª Línea: Negocio	Quienes USAN IA en operaciones	• Dueños de caso de uso • Aplican controles operacionales • Reportan incidentes • Responsables de calidad de datos de entrada
2ª Línea: Riesgo/Compliance	Quienes SUPERVISAN el uso de IA	• Comité de Gobernanza AI • Políticas y procedimientos • Evaluación de riesgos • Monitoreo de cumplimiento • Reporte al Directorio
3ª Línea: Auditoría	Quienes VERIFICAN independientemente	• Aseguramiento independiente • Evalúa diseño y efectividad de controles • Reporta directamente al directorio • Auditoría algorítmica periódica

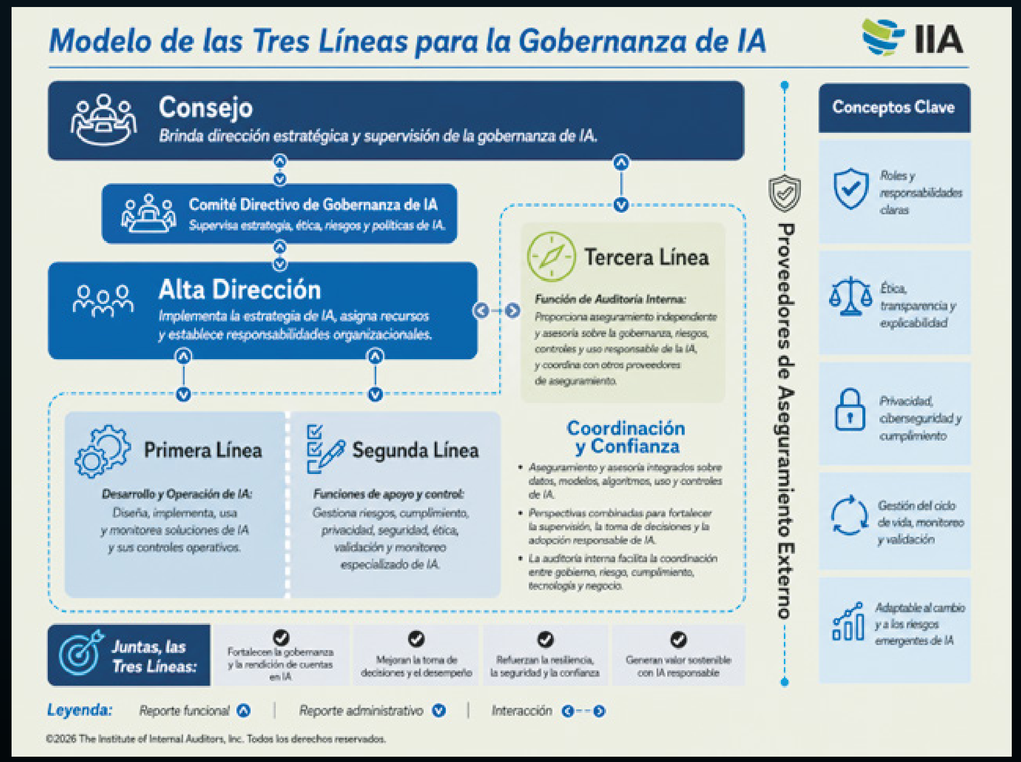
Modelo de Gobierno

La gobernanza de la IA solo funciona si las responsabilidades están claras desde el primer día: se deben evitar los esfuerzos aislados y garantizar que la supervisión sea realmente independiente. Para articular la supervisión estratégica del Directorio con la ejecución cotidiana del negocio, la organización debería adoptar un esquema escalonado en tres niveles interconectados. Esta arquitectura asegura un flujo bidireccional continuo: alineamiento y directrices desde la mesa directiva hacia la operación, y trazabilidad, reportabilidad y escalamiento de riesgos desde la gestión hacia los órganos de decisión.



07 Estructura de **Gobernanza** propuesta

En Julio de 2026, el Instituto de Auditores Internos publicó la tercera actualización del "Modelo de 3 líneas" que podemos adaptar para la Gobernanza de la IA, delimitando responsabilidades claras entre el órgano de gobierno, la gestión operativa y el aseguramiento independiente para crear valor y controlar riesgos éticos, de datos y de modelos de IA.



Nota: Adaptación del modelo de 3L de julio 2026 (www.theiia.org), efectuado por equipo editorial del presente documento.

07 Estructura de **Gobernanza** propuesta

Existencia de un Comité Directivo de Gobernanza AI

Se sitúa operativamente en la **intersección entre la gobernanza (el órgano de gobierno/consejo) y la gestión (la alta dirección)**, encargándose de traducir la estrategia ética y de valor en directrices ejecutivas.

Su composición debe ser multidisciplinaria, considerando al menos los siguientes roles:

Rol	Responsabilidad	Perfil
Representante del Directorio	Miembro y quién preside el Comité.	Director
Sponsor Ejecutivo	Accountability ante el directorio, autoridad de decisión	CEO
RRHH	IA en contratación, evaluación, impacto laboral	Director de Personas
Líder AI/ML	Visión técnica, evaluación de modelos	Head of Data Science, CAIO o CTO
Legal/Compliance	Cumplimiento regulatorio, contratos	Fiscal o CCO
Seguridad/Riesgo	Ciberseguridad, riesgo operacional	CISO o CRO
Privacidad	Protección de datos, DPIA	DPO
Negocio	Representar necesidades y contexto de uso	Líderes de áreas que usan IA

La gobernanza efectiva de la IA exige conectar la supervisión del Directorio con la operación mediante un Comité multidisciplinario. Integrar transversalmente las visiones de negocio, tecnología, riesgo, cumplimiento y ética en este órgano garantiza un análisis riguroso y holístico previo a la toma de decisiones directivas.



07 Estructura de **Gobernanza** propuesta

Políticas mínimas

Una sola política de IA que intente cubrir todo resulta demasiado general o se desactualiza en meses. Se recomienda un set de políticas específicas:

Política	Alcance	Extensión
Uso Aceptable de IA	Qué herramientas pueden usar los empleados, con qué datos, para qué fines	2-4 páginas
IA y Proveedores	Evaluación, onboarding, términos contractuales, monitoreo de vendors AI	2-4 páginas
IA en Productos / Servicios	IA visible al cliente: disclosure, transparencia, límites	2-4 páginas
Datos para IA	Qué datos pueden usarse para entrenar/promptear, clasificación, consentimiento	2-4 páginas
Gestión de Riesgos	Directrices aplicables como un estándar para la gestión de riesgos	8-10 páginas
Casos de Uso	Directrices para el desarrollo de casos de uso, estándares de priorización y focos estratégicos	2-4 páginas



Cada política debe tener: dueño nombrado, fecha de vigencia y cadencia de revisión (máximo anual).

07 Estructura de **Gobernanza** propuesta

Controles operacionales

Los controles son los mecanismos que hacen cumplir las políticas. Una política sin control es solo un documento.

Control	Qué hace	Test de efectividad
Acceso	Quién puede usar qué herramienta AI, con qué autenticación	Log de accesos, revisión trimestral de permisos
Datos	Qué datos fluyen a qué modelos, con qué clasificación	DLP activo, bloqueo automático si viola política
Output	Qué requiere revisión humana, qué se retiene como evidencia	% outputs revisados, retención documental
Vendors	Due diligence, cláusulas AI en contratos, monitoreo	Checklist completado pre-onboarding
Incidentes	Qué gatilla respuesta, quién se notifica, qué se documenta	Playbook probado, simulacros anuales
Cambios	Cómo entran nuevas herramientas, cómo se retiran	Inventario actualizado, change advisory board



07 Estructura de **Gobernanza** propuesta

Gestión de proveedores y terceros

Cuando el sistema de IA proviene de un proveedor externo, la responsabilidad no se terceriza. Es necesario definir explícitamente:

- Qué datos se comparten y bajo qué condiciones.
- Quién es responsable si el modelo genera un daño (organización, proveedor, usuario).
- Qué garantías contractuales existen sobre privacidad, retención y no-entrenamiento con datos del cliente.
- Cómo se gestiona un cambio unilateral del proveedor (nueva versión del modelo, cambio de términos).
- Criterios de exit: qué se necesita para migrar a otro proveedor (portabilidad).

La responsabilidad no puede quedar diluida entre múltiples actores. El directorio debe exigir una matriz RACI específica para IA que identifique quién es Responsable, Accountable, Consultado e Informado en cada etapa del ciclo de vida.



08

El rol de la **auditoría interna y externa** como mecanismo de aseguramiento sobre IA

08 El rol de la **auditoría interna y externa** como mecanismo de aseguramiento sobre IA

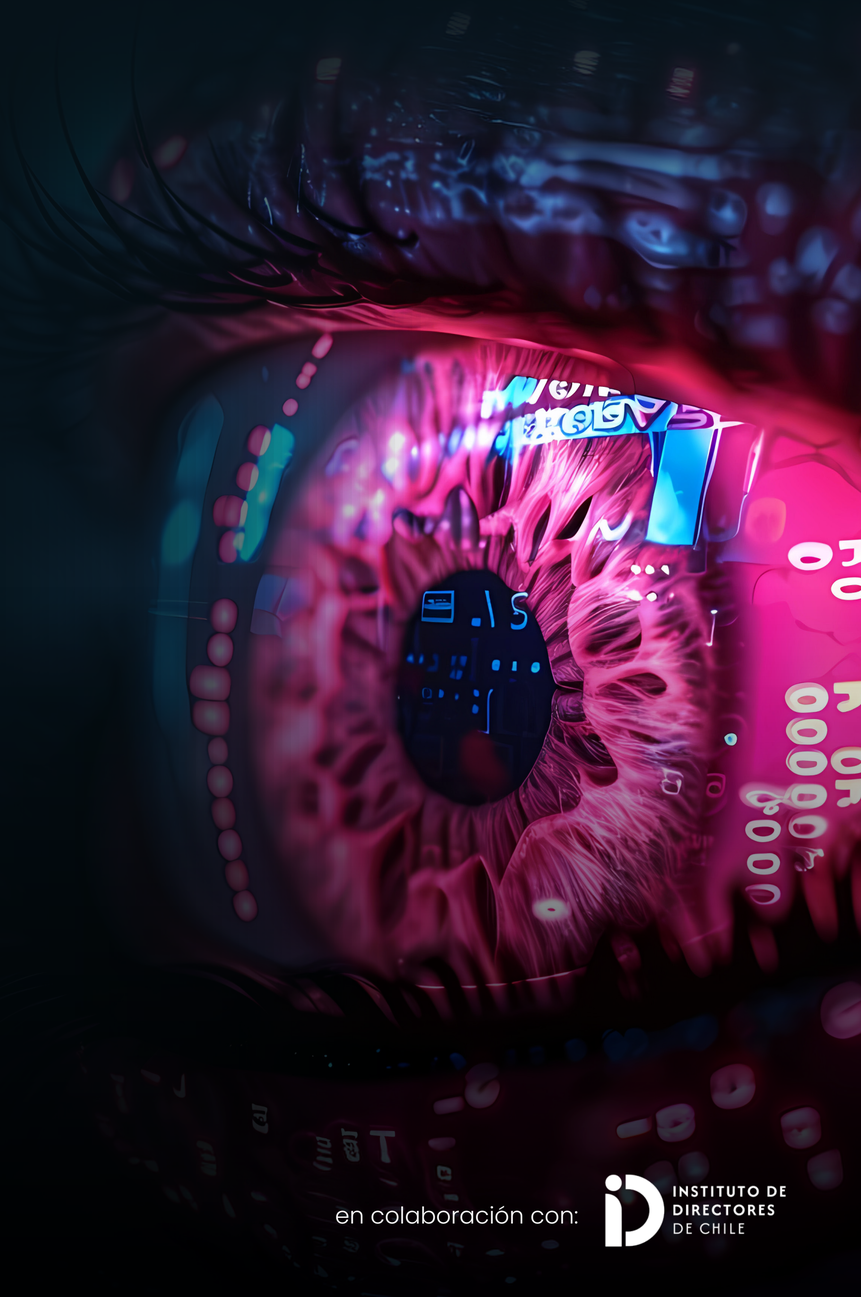
La Auditoría Interna debe proveer aseguramiento independiente sobre el gobierno, la gestión de riesgos y los controles establecidos sobre el uso de la IA. Las Normas Globales de Auditoría Interna organizan el trabajo en torno al Modelo de las Tres Líneas. En tal sentido, el rol de la Función de Auditoría Interna se relaciona con las siguientes verticales:

a) Sobre gobierno y estrategia

- Validar la existencia de una **política de IA aprobada** por el Directorio, alineada con el apetito de riesgo y con los principios organizacionales y en el caso de Chile, con la Política Nacional de IA.
- Velar por la existencia de un **inventario completo de casos de uso de IA** (incluida IA embebida en software de terceros) clasificado por nivel de riesgo.
- Cada caso de uso posea un **dueño** identificado y con roles claros de aprobación.
- Existencia de un **monitoreo** que detecta el uso de IA no autorizada (shadow AI).

b) Sobre la gestión y protección de datos

- Existencia de **Base de licitud** y, cuando corresponda, consentimiento para los datos usados en entrenamiento, ajuste e inferencia; tratamiento reforzado de datos sensibles (p. ej., datos de salud o bancarios).
- Existencia de controles de **clasificación de datos** que impidan que información personal o confidencial salga a modelos externos.
- Se evaluó la **calidad, exactitud y linaje** (trazabilidad completa del dato a lo largo de su ciclo de vida) de los datos verificados y documentados.
- Existencia de procedimiento de **notificación de brechas** y registro de actividades de tratamiento.



08 El rol de la **auditoría interna y externa** como mecanismo de aseguramiento sobre IA

c) Sobre el diseño, validación y desempeño de los modelos

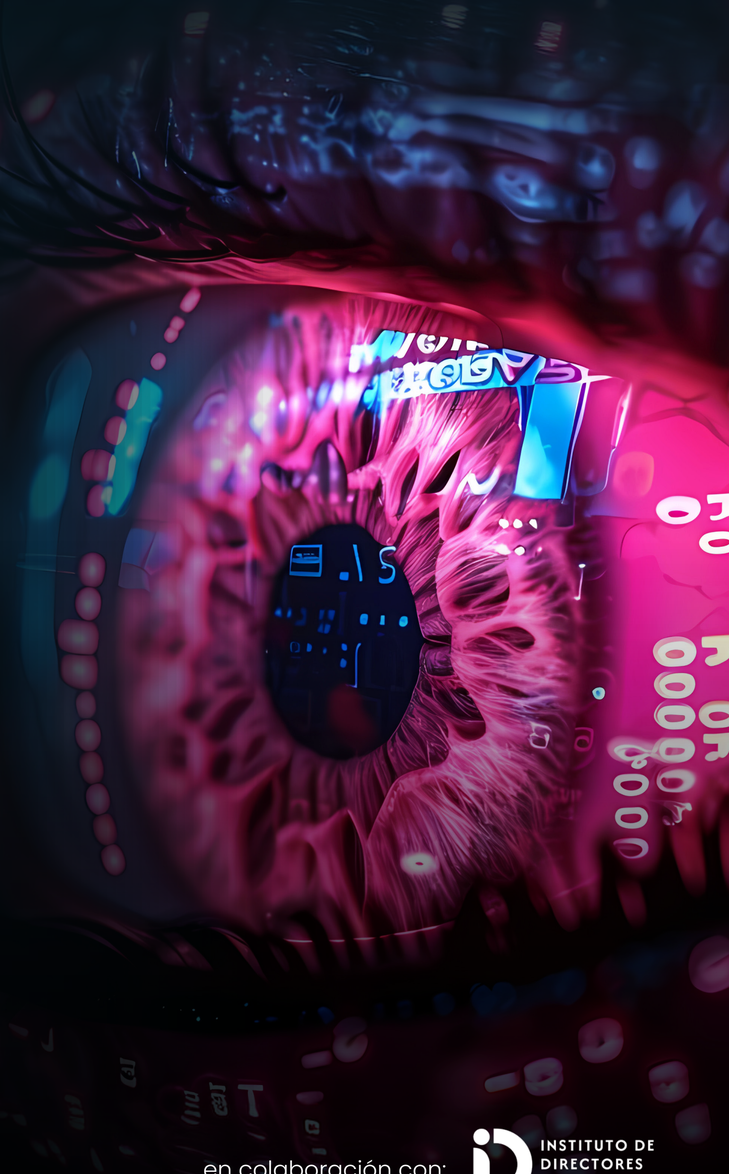
- Pruebas de **sesgo, exactitud y robustez** antes de producción, con umbrales definidos.
- Monitoreo sobre la **derivación del modelo (model drift)** y degradación del desempeño.
- Para IA generativa: existencia de controles contra **alucinaciones, inyección de prompts y fuga de datos,** y verificación humana de outputs en decisiones relevantes.
- Existencia de **documentación del modelo** y control de versiones.

d) Sobre decisiones automatizadas y la validación humana

- Validar que las **decisiones automatizadas que producen efectos jurídicos o significativos** en las personas, cuenten con intervención humana.
- Definiciones claras de dónde debe haber **intervención humana obligatoria.**
- Para agentes: **identidad propia del agente**, principio de mínimo privilegio, límites de acción y registro (log) de las cadenas de decisión autónomas; "interrupción de apagado" (kill switch) y plan de reversión.

e) Sobre ciberseguridad, terceros y cumplimiento

- Cumplimiento de la **Ley 21.663:** capacidad de **reportar incidentes al CSIRT Nacional** dentro de los plazos y controles específicos, cuando la organización es operador de importancia vital.
- **Debida diligencia de proveedores** de modelos como encargados de tratamiento: condiciones de datos, seguridad, ubicación, gestión de versiones y plan de salida.
- **Pruebas de ciberseguridad** específicas de IA (red-teaming, pruebas de adversarios).
- Mapeo del cumplimiento con la **normativa chilena vigente** (Ley 21.719, Ley 21.663 y normativa del regulador sectorial) y monitoreo del proyecto de ley de IA.



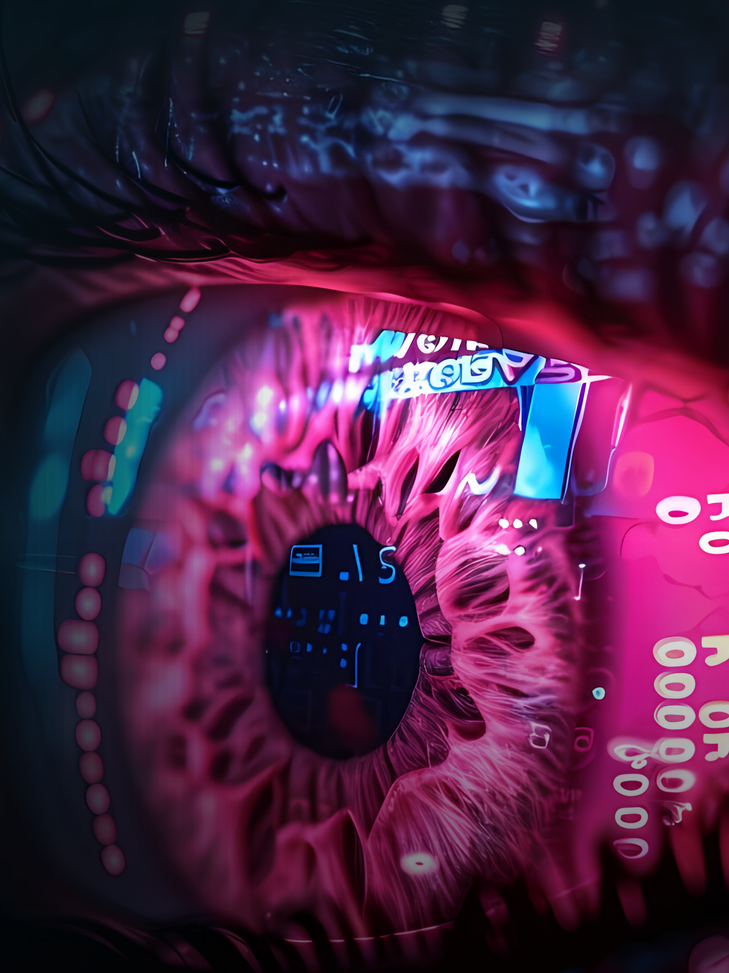
08 El rol de la **auditoría interna y externa** como mecanismo de aseguramiento sobre IA

f) Sobre el uso de IA por la propia Auditoría Interna

Las Normas Globales de Auditoría Interna 2024 habilitan a que la propia función use IA en planificación, trabajo de campo y reporte. La función de auditoría Interna debe aplicar los mismos controles que definió la organización: validando la fiabilidad de sus herramientas, evitando conclusiones basadas en outputs no verificados y resguardar la confidencialidad de la información auditada conforme a la normativa de datos vigente.

Rol de Auditoría Externa sobre el uso de IA en organizaciones que auditan financieramente

El rol de la Auditoría Externa no es certificar la IA de su cliente, sino evaluarla en tanto afecte los estados financieros, concretamente: i) identificar dónde la IA incide en cifras materiales — provisiones, valorizaciones, reconocimiento de ingresos, clasificación de transacciones—, probar los controles sobre esos modelos (calidad y linaje de datos, validación independiente, gestión de cambios, monitoreo de deriva, supervisión humana efectiva) y desafiar los supuestos detrás de estimaciones generadas algorítmicamente, exigiendo trazabilidad y evidencia auditable. Ello suele requerir especialistas en datos y modelos dentro del equipo. La responsabilidad por el uso de la IA permanece en la administración y el directorio; el auditor solo opina sobre su efecto en el riesgo de incorrección material.



09 **Principios y normativas** nacionales e internacionales

en colaboración con: INSTITUTO DE DIRECTORES

09 **Principios y normativas** nacionales e internacionales

Los principios y normativas de la inteligencia artificial son guías éticas y reglas legales que aseguran un uso seguro, transparente y justo de la tecnología. Para los directorios, son vitales porque la IA dejó de ser un asunto técnico para convertirse en una responsabilidad fiduciaria de gobierno corporativo y control de riesgos.

Principios:

UNESCO creó el Acuerdo Mundial sobre la Ética de la Inteligencia Artificial que fue firmado por más de 190 países. La Recomendación se basa en **cuatro valores** fundamentales que sientan las bases para que los sistemas de IA trabajen por el bien de la humanidad, las personas, las sociedades y el medio ambiente:

1. Derechos humanos y dignidad humana
2. Vivir en sociedades pacíficas
3. Garantizar diversidad e inclusión
4. Florecimiento del medio ambiente y los ecosistemas.

De estos se establece el enfoque de la IA en derechos humanos con los siguientes **principios:**

1. Proporcionalidad e inocuidad
2. Seguridad y protección
3. Derecho a la intimidad y protección de datos.
4. Gobernanza y colaboración adaptativas y de múltiples partes interesadas
5. Responsabilidad y rendición de cuentas
6. Transparencia y explicabilidad
7. Supervisión y decisión humanas
8. Sostenibilidad
9. Sensibilización y educación
10. Equidad y no discriminación



09 **Principios y normativas** nacionales e internacionales

Normativas:

Actualmente, la normativa más avanzada y restrictiva es el **Reglamento de IA de la Unión Europea (AI Act).** Este está basado en las siguientes clasificaciones de riesgos relacionados con el uso de la IA.

- **Riesgo Inaceptable:** Sistemas completamente prohibidos. Incluye técnicas de manipulación conductual, sistemas de puntuación social y herramientas específicas como programas que permiten desnudar personas mediante ultra falsificaciones (deepfakes) sin su consentimiento.
- **Alto Riesgo:** Tecnologías utilizadas en áreas críticas como salud, educación, empleo (recursos humanos) e infraestructuras del Estado. Deben superar auditorías estrictas antes de salir al mercado.
- **Riesgo Limitado:** Sistemas sujetos a obligaciones de transparencia. Se exige advertir explícitamente a los usuarios que están interactuando con una máquina (como un chatbot) o consumiendo contenido sintético.
- **Riesgo Mínimo:** Aplicaciones sin restricciones, como video juegos o filtros de correo basura, que representan la mayoría de los sistemas actuales.

Las penalidades económicas se implementan basándose en los niveles de gravedad:

Nivel de Gravedad	Tipo de Infracción	Multa Máxima (la que sea mayor)
Nivel 1 (máximo)	Uso o comercialización de **prácticas de IA prohibidas** (ej. manipulación cognitiva, scoring social o reconocimiento biométrico no autorizado).	**Hasta €35 millones** o el **7%** del volumen de negocio mundial anual.
Nivel 2 (significativo)	Incumplimiento de obligaciones para sistemas de **Alto Riesgo,** modelos de propósito general (GPAI) o fallas de transparencia.	**Hasta €15 millones** o el **3%** del volumen de negocio mundial anual.
Nivel 3 (menor)	Suministro de **información incorrecta, incompleta o engañosa** a las autoridades de control o laboratorios de ensayo.	**Hasta €7.5 millones** o el **1%** del volumen de negocio mundial anual.

09 **Principios y normativas** nacionales e internacionales

Otros marcos normativos relevantes

- **ISO/IEC 42001:2023:** Sistema de Gestión de IA certificable. Establece requisitos de gobernanza, gestión de riesgos y mejora continua para organizaciones que desarrollan o usan IA. Certificación auditada por terceros.
- **NIST AI Risk Management Framework (RMF):** Marco voluntario del gobierno de EE.UU. para gestionar riesgos de IA. Estructura en cuatro funciones: GOVERN, MAP, MEASURE, MANAGE. Referencia global para programas de gestión de riesgos.
- **GDPR (Art. 22):** Regula las decisiones automatizadas que afectan significativamente a personas. Exige el derecho a explicación, supervisión humana y la posibilidad de impugnar decisiones automatizadas.
- **DORA (Sector financiero):** Resiliencia operativa digital para el sector financiero europeo. Incluye requisitos específicos para sistemas de IA utilizados en procesos críticos de negocio financiero.

En Chile hoy no existen regulaciones o leyes sancionadas y vigentes enfocadas en la IA. Hay algunos proyectos de ley en tramitación.



09 **Principios y normativas** nacionales e internacionales



En 2021 se publicó la **Política Nacional de IA,** compuesta por 3 ejes: 1) Factores habilitantes, 2) Desarrollo y Adopción, 3) Gobernanza y ética. Este último eje, dado el rápido avance de la IA Generativa, se actualizó en 2024 incluyendo nuevos aspectos como por ejemplo impactos laborales, entre otros. Esta política trasciende lo técnico y se instala en los directorios como un asunto de gobierno corporativo, gestión de riesgos y competitividad estratégica. Los boards deberán alinear sus decisiones con los pilares país para evitar pasivos legales y asegurar la creación de valor.

También existen normativas vigentes que regulan algunos aspectos de la IA, como:

- **Nueva Ley de Protección de Datos Personales (Ley N.º 21.719):** Esta ley —que impone estándares equivalentes al GDPR de Europa— fija su plazo definitivo de cumplimiento forzoso. Es vital para la IA, ya que otorga a los ciudadanos chilenos el derecho explícito a impugnar y exigir una explicación sobre decisiones automatizadas tomadas por algoritmos o agentes autónomos (por ejemplo, en la evaluación de créditos o perfiles en CRM comerciales). Las multas pueden llegar al 4% de los ingresos globales de una compañía.
- **Ley Marco de Ciberseguridad (Ley N.º 21.663):** Crea la Agencia Nacional de Ciberseguridad (ANCI), la cual ya supervisa a cientos de Operadores de Importancia Vital (OIV) en sectores críticos (luz, salud, telecomunicaciones). Si estas infraestructuras usan IA en sus procesos y sufren un incidente informático o brecha de seguridad, arriesgan multas millonarias de manera directa.
- **Acción de los Tribunales:** La Corte Suprema de Chile ya ha sentado jurisprudencia utilizando la Constitución, bloqueando el uso no regulado de tecnologías biométricas y de reconocimiento facial basados en IA por vulnerar los derechos fundamentales a la privacidad, sin necesidad de esperar a que se apruebe la Ley de IA.

10 Casos **ilustrativos**

10 Casos **ilustrativos**

Luego de revisar el estado del arte normativo, es útil observar cómo organizaciones reales ya han traducido los principios de gobierno de IA en prácticas y resultados medibles. Los casos que siguen están documentados públicamente por IBM y sus socios, y son consistentes con la visión de gobernanza que IBM promueve: la gobernanza como habilitador de valor —no como freno a la innovación—, con foco en trazabilidad, rendición de cuentas y supervisión desde la alta dirección. Se incluyen tanto el caso de la propia IBM (que aplicó su modelo de gobierno sobre sí misma) como algunos casos de clientes en seguros y banca.

El caso IBM: el Integrated Governance Program (IGP)

La propia IBM aplicó sobre su operación interna el modelo de gobierno de IA que promueve a sus clientes. A través de su Office of Privacy and Responsible Technology (OPRT) y con supervisión del IBM Responsible Technology Board —órgano equivalente, en la práctica, a un comité de directorio especializado—, IBM integró sus sistemas de gestión de privacidad y de datos (PIMS) para crear el Integrated Governance Program (IGP): una visión única y de extremo a extremo de los datos y modelos usados por la compañía.

Entre inicios de 2024 y un periodo de ocho meses, la implementación de estándares reforzados de trazabilidad de datos (data provenance) dentro del IGP arrojó resultados concretos y medibles:

- 58% de reducción en el tiempo de procesamiento de solicitudes de autorización de datos de terceros.
- 62% de reducción en el tiempo de procesamiento de solicitudes de autorización de datos propios de IBM.
- Más de 1.000 conjuntos de datos y modelos aprobados para su reutilización.

Lee Cox, Vicepresidente de Gobernanza Integrada de IBM, resume el enfoque: “Un programa de gobernanza integral puede equilibrar el valor de negocio que promete la IA con la necesidad de supervisión y gestión de riesgo, habilitando una IA responsable a escala”.

10 Casos **ilustrativos**

Relevancia para el directorio: el caso muestra que un órgano de gobierno de nivel superior puede y debe exigir métricas concretas de eficiencia y riesgo —tiempos de autorización, número de modelos con trazabilidad completa, reutilización controlada de datos—, no solo la existencia de políticas o principios declarativos.

Sector financiero: trazabilidad y auditoría de modelos de IA (Vectice – IBM watsonx.governance)

Tres instituciones financieras que operan sobre IBM watsonx.governance ilustran cómo la automatización de la documentación y trazabilidad de modelos de IA se traduce en resultados de gobierno tangibles y auditable por el directorio:

- Un banco europeo líder redujo en 90% su tiempo de preparación de auditorías, al automatizar la documentación de desarrollo y validación de modelos (MDD/MVD), con generación del primer borrador en minutos y metadatos capturados y estructurados automáticamente.
- Una institución financiera del top 10 de Estados Unidos centralizó el gobierno de modelos desarrollados en múltiples plataformas, reduciendo en 50% sus ciclos de revisión de cumplimiento.
- Un banco de inversión global mejoró en 25% la eficiencia de sus revisiones de validación de modelos gracias a trazabilidad de linaje, versionamiento y autoría en tiempo real.

Relevancia para el directorio: estos casos muestran cómo la trazabilidad técnica (linaje de datos y de modelos, documentación automática) se convierte directamente en un indicador de gestión —tiempo y costo de preparación de auditorías— que el directorio puede exigir como parte de su tablero de control, conectando con el rol de la auditoría interna y externa.

Lección para el directorio: la brecha entre gobernanza declarada e implementada

El informe “The enterprise guide to AI governance”, del IBM Institute for Business Value, aporta una advertencia relevante para cualquier directorio: 87% de las organizaciones declara contar con un marco de gobierno de IA, pero menos del 25% ha implementado efectivamente los controles necesarios para gestionar sesgo, transparencia y riesgos de seguridad. El mismo informe señala que 80% de las organizaciones ya cuenta con una función de riesgo dedicada específicamente a la IA, lo que confirma que exigir rendición de cuentas sobre esta materia se ha vuelto una práctica extendida a nivel de alta dirección.

Esta brecha entre gobernanza declarada e implementada refuerza un mensaje central para este documento: no basta con que el directorio apruebe una política de IA; debe exigir evidencia periódica de su implementación efectiva —auditorías, métricas de sesgo, indicadores de trazabilidad— antes de dar por cumplido su deber de supervisión.

11 Conclusiones y **recomendaciones**

11 Conclusiones y **recomendaciones**

Liderando la Era de la Inteligencia Artificial con Responsabilidad y Visión

La Inteligencia Artificial (IA) ha dejado de ser una frontera tecnológica para convertirse en la **infraestructura operativa crítica** que definirá el éxito y la sostenibilidad de nuestras organizaciones en las próximas décadas. Este documento no es solo una advertencia sobre riesgos, sino una **hoja de ruta estratégica** para que los Directorios asuman su rol protagónico en la construcción de un futuro donde la innovación y la ética converjan para crear valor a largo plazo.

A continuación, se presentan las conclusiones estratégicas clave con una mirada hacia el horizonte transformador que enfrentamos:

- **La IA como Imperativo del Gobierno Corporativo:** La supervisión de la IA es una responsabilidad **fiduciaria e indelegable** de la mesa directiva. Ya no puede tratarse como un tema aislado de TI; es un asunto de estrategia, reputación y continuidad del negocio que requiere que el Directorio sea el arquitecto del marco de confianza dentro del cual la administración opera.
- **Gobernanza como Acelerador de Valor:** Lejos de ser un freno a la innovación, una gobernanza robusta es el habilitador que permite desplegar la IA a escala de manera segura. Las organizaciones que implementen estructuras claras de responsabilidad (como el modelo de las tres líneas y comités multidisciplinarios) no solo mitigarán riesgos, sino que alcanzarán eficiencias operativas medibles y una ventaja competitiva sostenible.
- **Resiliencia ante la "Historia en Desarrollo":** Los riesgos de la IA (alucinaciones, sesgos, opacidad, etc) son una historia que se sigue escribiendo día a día. El Directorio debe fomentar una **cultura de vigilancia continua** y aprendizaje dinámico, entendiendo que la agilidad para adaptar los controles al ritmo de la tecnología será la competencia central de las empresas resilientes.

11 Conclusiones y **recomendaciones**

- **Cumplimiento Proactivo y Ética como Diferenciador:** Con regulaciones internacionales como el EU AI Act ya vigentes y normativas nacionales en evolución, el cumplimiento deja de ser una lista de verificación para convertirse en un **compromiso ético con los stakeholders.** El Directorio debe liderar desde los valores, garantizando que cada algoritmo respete la privacidad, la equidad y los derechos humanos, transformando la transparencia en un activo reputacional.

- **El Poder de la Evidencia y la Medición:** En el futuro de la IA, lo que no se mide no existe. El directorio debe exigir métricas de riesgo (KRIs) y KPIs específicos que den visibilidad real sobre el inventario de modelos y su desempeño. El "silencio" de la administración ya no es garantía de seguridad; la verdadera tranquilidad proviene de sistemas de aseguramiento independientes y reportes basados en evidencia.

Un Llamado a la Acción...

Estamos ante una oportunidad histórica para redefinir el propósito corporativo a través de la IA. El desafío para los Directores no es comprender cada línea de código, sino tener la sabiduría estratégica para hacer las preguntas correctas, establecer un apetito de riesgo audaz pero responsable y asegurar que la tecnología esté siempre al servicio de las personas y la sostenibilidad.
El futuro pertenece a los Directorios que no solo observan la transformación digital, sino que la gobiernan con visión, integridad y un compromiso inquebrantable con la excelencia. Este es el momento de asegurar que nuestra huella tecnológica sea el legado de una organización ética, innovadora y profundamente humana.

Sobre los Autores de este documento

Este documento es fruto de la colaboración de profesionales expertos en tecnología y profesionales expertos en Auditoría Interna, Riesgos y Gobierno, que investigaron y reflexionaron alrededor de un tema que hoy es estratégico para las organizaciones y la implicancia que tiene para los Directorios.

Coautores

- José Luis Fernández, Gerente Corporativo de Auditoría Interna - ACHS
- Sergio Hernández, Gerente de Contraloría - COPEC
- Pablo Martel, Head of Audit Staff & Compliance Chile – ENEL Group
- Yessica Cartajena, Executive Director - Microsoft
- Guillermo Treister, Gerente Data e Inteligencia Artificial - IBM
- Christian Ramírez, Manager Solutions Architecture - AWS

Comité de Calidad

- Manuel Quezada, Presidente - Instituto de Auditores Internos de Chile
- Hernán Rebolledo, Director - Prospectus
- Fadua Gajardo, Directora Ejecutiva – Instituto de Directores de Chile

Editor General

- Mario Ernst, Director - Prospectus

en colaboración con: INSTITUTO DE DIRECTORES DE CHILE

Fuentes consultadas

1. Bain & Company: Responsible AI Design and Governance.
2. Boston Consulting Group (BCG): AI Risk Management Needs a Better Model (2026).
3. COSO: Internal Control Framework.
4. COBIT: IT Governance Framework.
5. Google DeepMind: Lessons from Defending Gemini Against Indirect Prompt Injections(2025).
6. IBM: Global AI Adoption Index 2023.
7. ISO/IEC 42001:2023: Information Technology — Artificial Intelligence — ManagementSystem .
8. ISO 9001:2015: Quality Management Systems — Requirements.
9. Ilieva, G., et al. (2026): A Generative AI-Based Framework for Proactive Quality Assuranceand Auditing.
10. McKinsey: State of AI 2023 - Generative AI Exposure.
11. NIST: Artificial Intelligence Risk Management Framework (AI RMF 1.0).
12. National Cybersecurity Centre (NCSC): Guidelines for Secure AI System Development .
13. The Institute of Internal Auditors (IIA): Artificial Intelligence Auditing Framework (2023).
14. The Institute of Internal Auditors (IIA): 2025 Pulse Report - Future of Internal Audit.
15. The Institute of Internal Auditors (IIA): GTAG: Understanding and Auditing Big Data.
16. Unión Europea: Regulation (EU) 2024/1689 (Artificial Intelligence Act).
17. U.S. Department of Justice (DOJ): Guidance on Evaluation of Corporate CompliancePrograms for Advanced Technologies (2025).
18. Weaver Connect: Implementing the IIA's AI Auditing Framework (2025).

en colaboración con: INSTITUTO DE DIRECTORES DE CHILE

Anexos

ANEXO 1: Ejemplos de Metodología de Gestión de Riesgos de la IA desde el rol de supervisión del Directorio

Caso aplicado 1:

Sesgo/discriminación algorítmica en un modelo de decisión (ej. scoring crediticio o selección de personal)

Riesgo inherente

Antes de controles, se evalúa el riesgo "puro" de que el modelo genere resultados sesgados o discriminatorios contra grupos protegidos, por composición de los datos de entrenamiento o por proxies indirectos de variables sensibles (código postal, nombre, historial educativo).

Dimensión	Valor	Justificación
Probabilidad	**4 (Alta)**	Datos históricos reflejan sesgos sociales preexistentes; el equipo de datos no realizó pruebas de equidad previas al entrenamiento.
Impacto	**5 (Crítico)**	Exposición regulatoria (leyes antidiscriminación), demandas, daño reputacional, pérdida de licencia para operar el modelo.
Riesgo inherente	**20 — Crítico**	**Probabilidad × Impacto en matriz 5×5.**

Controles existentes

Control	Tipo	Naturaleza
Revisión legal de cumplimiento normativo antes del lanzamiento	**Preventivo**	**Manual**
Pruebas de equidad (fairness testing) por grupo demográfico	**Detectivo**	**Automatizado / periódico**
Supervisión humana (human-in-the-loop) para decisiones de alto impacto	**Preventivo**	**Manual**
Reentrenamiento periódico del modelo con monitoreo de deriva	**Correctivo**	**Automatizado**

Evaluación de efectividad

No basta con que el control exista: se evalúa diseño, ejecución real y madurez operativa.

Control	Efectividad	Evidencia / brecha
Revisión legal	**0.7 (Efectivo)**	Checklist documentado, pero no cubre jurisdicciones nuevas donde opera el modelo.
Fairness testing	**0.4 (Parcial)**	Se ejecuta, pero solo sobre 2 de 5 variables protegidas relevantes; sin umbral de alerta formal.
Supervisión humana	**0.5 (Parcial)**	Existe, pero el operador aprueba >95% de las recomendaciones del modelo sin cuestionarlas ("automation bias").
Monitoreo de deriva	**0.6 (Moderado)**	Automatizado, pero las alertas no están vinculadas a un protocolo de re-evaluación del riesgo.
Efectividad combinada	**≈ 0.5**	**Promedio ponderado por relevancia del control frente a la causa raíz del riesgo.**

Riesgo residual

Riesgo Residual = Riesgo Inherente × (1 - Efectividad combinada) = 20 × (1 - 0.5) = 10 — Alto

Comparación con el apetito de riesgo

Parámetro	Valor
Apetito de riesgo declarado por el Directorio para IA de alto impacto (afecta derechos de personas)	**≤ 8 (Medio)**
Riesgo residual actual	**10 (Alto)**
Resultado	**EXCEDE el apetito en 2 puntos > requiere tratamiento y escalamiento al Directorio**

Plan de tratamiento

Estrategia: Mitigar (el uso del modelo se considera estratégico; no se evalúa evitar ni transferir en esta etapa).

- Ampliar el fairness testing a las 5 variables protegidas relevantes, con umbrales de alerta automatizados.
- Rediseñar el flujo de supervisión humana para exigir justificación documentada en decisiones de alto impacto (mitigar automation bias).
- Vincular las alertas de deriva del modelo a un protocolo formal de re-evaluación del riesgo cada 90 días.
- Meta de efectividad combinada: elevar de 0.5 a 0.75, llevando el riesgo residual a 5 (Bajo-Medio), dentro del apetito.

Responsable y plazo

Acción	Responsable	Plazo	Reporta a
Ampliar fairness testing	Chief Data Officer	45 días	Comité de Riesgos
Rediseñar supervisión humana	Gerente de Producto / Operaciones	60 días	Comité de Riesgos
Protocolo de re-evaluación por deriva	Chief Information Officer	30 días	Comité de Riesgos
Validación de riesgo residual post-tratamiento	Dueño del riesgo (CIO)	90 días	Directorio (vía Comité)

Caso aplicado 2:

Fuga de datos confidenciales por uso de IA generativa (empleados usando herramientas de IA externas)

Riesgo inherente

Dimensión	Valor	Justificación
Probabilidad	5 (Muy alta)	Uso extendido y no gobernado de herramientas de IA generativa por empleados, sin política formal ni bloqueo técnico.
Impacto	4 (Alto)	Filtración de información confidencial, propiedad intelectual o datos personales a proveedores externos de IA, con posible uso en entrenamiento de terceros.
Riesgo inherente	**20 — Crítico**	**Probabilidad × Impacto en matriz 5×5.**

Controles existentes

- Política de uso aceptable de IA (existe, pero fue comunicada solo por correo, sin capacitación).
- Lista de herramientas de IA aprobadas por Seguridad de la Información.
- DLP (Data Loss Prevention) configurado parcialmente para detectar cargas a dominios de IA no aprobados.

Riesgo residual

Control	Efectividad	Riesgo residual resultante
Política de uso aceptable	0.2 (Inefectivo)	Sin capacitación ni firma de aceptación; bajo cumplimiento observado en auditoría interna.
Lista de herramientas aprobadas	0.4 (Parcial)	Existe pero no se actualiza al ritmo de aparición de nuevas herramientas.
DLP	0.5 (Parcial)	Cubre navegadores gestionados, no dispositivos móviles ni BYOD.
Efectividad combinada	**≈ 0.35**	**Riesgo residual = 20 × (1 - 0.35) = 13 — Alto/Crítico**

Comparación con el apetito de riesgo

Apetito declarado para riesgos de seguridad de la información: ≤ 8 (Medio). Riesgo residual actual (13) excede ampliamente el apetito > escalamiento inmediato al Directorio, dado que involucra tanto seguridad de la información como cumplimiento de protección de datos.

Plan de tratamiento, responsable y plazo

Acción	Responsable	Plazo	Reporta a
Capacitación obligatoria + firma de política de uso de IA	Chief Information Security Officer	30 días	Comité de Riesgos
Extender DLP a dispositivos móviles y BYOD	Gerente de Seguridad de TI	60 días	Comité de Riesgos
Habilitar alternativa corporativa segura de IA generativa	Chief Information Officer	90 días	Directorio (vía Comité)

Responsabilidades explícitas del Directorio en cada etapa del ciclo

La siguiente tabla traduce cada una de las 7 etapas metodológicas en preguntas y decisiones concretas que corresponden al Directorio, diferenciándolas de las que corresponden a la Gerencia.

Etapa	Rol del Directorio
1. Riesgo inherente	Aprobar la taxonomía de riesgos de IA de la organización (sesgo, privacidad, seguridad, explicabilidad, dependencia de terceros) y exigir que todo caso de uso de IA de alto impacto sea clasificado antes de su desarrollo.
2. Controles existentes	Verificar que exista un inventario actualizado de sistemas de IA en uso ("AI inventory") y sus controles asociados; no aprobar el uso de "shadow AI" sin registro.

Etapa	Rol del Directorio
3. Evaluación de efectividad	Exigir evidencia independiente (auditoría interna, validación de modelos independiente del equipo que lo construyó) en vez de aceptar la autoevaluación de quien diseñó el control.
4. Riesgo residual	Cuestionar la metodología de cálculo (¿es creíble el factor de mitigación aplicado?) y solicitar sensibilización de escenarios adversos (ej. "¿qué pasa si el modelo falla en producción?").
5. Apetito de riesgo	Definir y aprobar formalmente el apetito de riesgo de IA (umbrales cuantitativos y líneas rojas cualitativas, ej. "no se automatizan decisiones que afecten derechos fundamentales sin supervisión humana"), revisarlo al menos anualmente.
6. Plan de tratamiento	Para riesgos que excedan el apetito, aprobar explícitamente la estrategia (mitigar/evitar/transferir/aceptar) y los recursos asociados; no delegar la aceptación de riesgo residual crítico en la Gerencia.
7. Responsable y plazo	Exigir que cada plan tenga un dueño único con autoridad real (no un comité difuso) y dar seguimiento activo al cumplimiento de plazos en cada sesión, escalando los incumplimientos reiterados.

ANEXO 2: Actuación del Directorio ante distintos riesgos de la IA

Los riesgos de IA se organizan en tres niveles de prioridad. Para cada riesgo existen acciones específicas que debe tomar o supervisar el Directorio y las señales de alerta que deben escalar obligatoriamente.

CRÍTICO — **Riesgos Críticos — Requieren atención inmediata del directorio**

Riesgo clave	Qué debe hacer el directorio	Señales de alerta
Sesgo algorítmico y discriminación Decisiones automatizadas que discriminan por género, raza u otras características protegidas.	• Exigir auditorías externas de equidad (Fairness Audits) antes de desplegar IA en decisiones de alto impacto. • Aprobar política de no uso de IA en decisiones que no puedan explicarse a los afectados. • Solicitar métricas de equidad (Disparate Impact Ratio) en informes periódicos.	• Quejas recurrentes de clientes por decisiones injustas. • Diferencias estadísticas significativas en outcomes por grupo demográfico. • Ausencia de análisis de equidad en reportes de IA.
Violaciones de privacidad y datos personales Exposición de datos sensibles por modelos de IA, incumplimiento GDPR u otras regulaciones.	• Aprobar e implementar política de IA que incluya Privacy by Design como requisito obligatorio. • Requerir Evaluaciones de Impacto en Protección de Datos (DPIA) para cada sistema IA. • Revisar anualmente los acuerdos con proveedores de IA respecto al manejo de datos.	• Ausencia de DPIA para sistemas IA con datos personales. • Incidentes de seguridad que involucren datos usados por IA. • Notificaciones de autoridades de protección de datos.
Ciberataques y robustez adversarial Manipulación de modelos IA, prompt injection, envenenamiento de datos de entrenamiento.	• Incluir los sistemas de IA en el alcance del programa de ciberseguridad y BCP/DRP de la organización. • Exigir red teaming periódico de sistemas IA críticos antes de releases y en producción. • Revisar informes de incidentes de seguridad que involucren sistemas de IA.	• Sistemas IA excluidos del programa de ciberseguridad. • Ausencia de pruebas adversariales documentadas. • Incidentes no reportados al directorio en tiempo razonable.

ALTO — Riesgos Altos — Gestión proactiva requerida

Riesgo clave	Qué debe hacer el directorio	Señales de alerta
Incumplimiento regulatorio de IA Violaciones a normativas vigentes.	• Asignar responsable ejecutivo de cumplimiento regulatorio de IA (CAIO o equivalente). • Aprobar presupuesto para clasificación de sistemas según normativa y cumplimiento de requisitos. • Recibir informes semestrales de estado de cumplimiento regulatorio de IA.	• Sin responsable ejecutivo designado para regulación de IA. • Sistemas IA de alto riesgo (según normativa) sin conformity assessment. • Correspondencia con reguladores sin escalar al directorio.
Opacidad y falta de explicabilidad Incapacidad de explicar decisiones de IA a reguladores, clientes y en litigios.	• Aprobar política de 'derecho a explicación' para todas las decisiones de IA de alto impacto. • Exigir documentación técnica (model cards) para todos los sistemas IA en producción. • Prohibir uso de IA de caja negra en decisiones que afecten derechos de personas.	• Reclamaciones o litigios donde la organización no puede explicar una decisión de IA. • Ausencia de documentación técnica de modelos en producción. Respuestas insatisfactorias a inspecciones regulatorias sobre IA.
Degradación silenciosa de sistemas IA Modelos que se deterioran en producción sin alertas, generando decisiones equivocadas.	• Exigir programa de monitoreo continuo con KPIs e indicadores de deterioro (drift) definidos. • Aprobar proceso formal de validación periódica de modelos en producción. • Revisar métricas de rendimiento de sistemas IA críticos en informes trimestrales.	• Ausencia de monitoreo automatizado de modelos IA en producción. • Deterioro en KPIs de negocio sin análisis de causa IA identificada. • Modelos en producción sin fecha de última validación documentada.
Dependencia crítica de proveedores de IA Concentración de riesgo en APIs o modelos de terceros sin alternativas o SLAs.	• Exigir inventario de todos los proveedores de IA con evaluación de riesgo de concentración. • Aprobar estrategia de multi-proveedor para sistemas IA críticos de negocio. • Revisar acuerdos de nivel de servicio (SLA) y cláusulas de continuidad con proveedores IA.	• Dependencia de un único proveedor para funciones críticas de negocio. • Ausencia de SLA documentados con proveedores de IA críticos. • Sin plan de contingencia ante caída de APIs de IA.

MEDIO

Riesgos Medios — Supervisión y mejora continua

Riesgo clave	Qué debe hacer el directorio	Señales de alerta
Impacto ético y reputacional Uso de IA en casos que generen controversia pública, daño a stakeholders o impacto social negativo.	• Crear o designar un Comité de Ética de IA con mandato y composición aprobados por el directorio. • Aprobar política de usos prohibidos de IA en la organización. • Revisar anualmente los casos de uso de IA contra criterios éticos y de reputación.	• Ausencia de política de ética de IA aprobada por el directorio. • Uso de IA en decisiones de alto impacto social sin revisión ética. • Cobertura mediática negativa sobre el uso de IA de la organización.
Falta de supervisión humana efectiva Automation bias: supervisores que aprueban decisiones IA sin revisión real.	• Definir y aprobar los casos de uso donde la supervisión humana es obligatoria e irrenunciable. • Exigir métricas de efectividad de supervisión humana en sistemas IA críticos. • Aprobar programas de formación en supervisión de IA para roles clave.	• Tasas de aprobación automática superiores al 95% en sistemas con revisión humana nominal. • Ausencia de formación en supervisión de IA para equipos operativos. • Incidentes donde la supervisión humana no detectó un error del sistema IA.
Transparencia insuficiente hacia stakeholders Falta de divulgación del uso de IA a clientes, empleados, reguladores e inversores.	• Aprobar política de divulgación del uso de IA en informes anuales, web y comunicaciones. • Exigir registro centralizado de todos los sistemas IA de la organización (AI Registry) • Incluir riesgos de IA en el informe de gestión de riesgos corporativo.	• Clientes o empleados que descubren el uso de IA sin haber sido informados. • Ausencia de AI Registry o inventario de sistemas IA. • Riesgos de IA no incluidos en el informe anual de riesgos corporativos.

ANEXO 3: Checklist de autoevaluación para el Directorio

Las siguientes 15 acciones orientan respecto a como debiese ser el plan mínimo de gobernanza de IA que el Directorio debe implementar o verificar. Este checklist puede usarse como instrumento de autoevaluación semestral.

#	Acción mandatoria del directorio	Estado
01	**Gobernanza —** Designar o confirmar un Chief AI Officer (CAIO) o equivalente con mandato formal aprobado por el directorio.	☐ **Pendiente**
02	**Gobernanza —** Crear un Comité de Riesgos de IA con participación de directores independientes.	☐ **Pendiente**
03	**Gobernanza —** Aprobar una Política Corporativa de IA que incluya principios, usos prohibidos y proceso de aprobación de nuevos usos.	☐ **Pendiente**
04	**Inventario —** Exigir un AI Asset Register completo: todos los sistemas IA en uso, propietario, datos, clasificación de riesgo y estado de cumplimiento.	☐ **Pendiente**
05	**Riesgos —** Integrar los riesgos de IA en el Enterprise Risk Management (ERM) con KRIs y umbrales de alerta definidos.	☐ **Pendiente**
06	**Regulatorio —** Completar la clasificación de sistemas IA según normativa vigente (Prohibido / Alto / Limitado / Mínimo riesgo).	☐ **Pendiente**
07	**Regulatorio —** Asegurar que todos los sistemas de Alto Riesgo tienen documentación técnica, DPIA y proceso de conformity assessment.	☐ **Pendiente**
08	**Auditoría —** Aprobar un plan anual de auditoría de IA que cubra los 12 dominios de riesgo: sesgo, privacidad, seguridad, cumplimiento, ética, entre otros.	☐ **Pendiente**
09	**Auditoría —** Contratar o designar una función de auditoría interna de IA con recursos y competencias específicas.	☐ **Pendiente**
10	**Ética —** Crear o ratificar un Comité de Ética de IA interdisciplinar con poder de veto formal sobre despliegues de alto impacto.	☐ **Pendiente**
11	**Seguridad —** Incluir los sistemas de IA en el scope del programa de ciberseguridad, BCP y DRP corporativo.	☐ **Pendiente**
12	**Reporte —** Establecer un calendario de informes de IA al directorio: KRIs mensuales, informe de riesgos trimestral, auditoría anual.	☐ **Pendiente**
13	**Formación —** Aprobar un programa de formación en IA y riesgos de IA para todos los miembros del directorio (mínimo 4 horas anuales).	☐ **Pendiente**
14	**Transparencia —** Aprobar la política de divulgación del uso de IA ante clientes, empleados, reguladores e inversores.	☐ **Pendiente**
15	**Proveedores —** Exigir due diligence de riesgos de IA para todos los proveedores y partners que aporten sistemas o modelos de IA.	☐ **Pendiente**

ANEXO 4: Agenda tipo para el Directorio

La supervisión de IA debe estructurarse en el calendario del Directorio con frecuencias diferenciadas según la criticidad de los temas. A continuación se propone una agenda tipo:

Frecuencia	Temas y contenidos a revisar	Quien reporta
Mensual (Comisión)	Alertas de KRIs críticos, incidentes de IA en el periodo, estado de remediaciones abiertas críticas.	AI Risk Officer directamente al Comité de Auditoría
Trimestral (Pleno)	Informe de estado de riesgos de IA, métricas de desempeño de sistemas críticos, actualizaciones regulatorias, avance de auditorías.	CAIO + Auditoría Interna
Semestral (Pleno)	Revisión del AI Risk Register completo, evaluación de madurez de gobernanza, informe de cumplimiento regulatorio, revisión de política de IA.	CAIO + Consejo General + DPO
Anual (Pleno)	Auditoría completa de IA con resultados y plan de remediación, revisión estrategia de IA, autoevaluación del Directorio en competencias de IA, aprobación del plan de auditoría siguiente año.	Auditoría Interna + Externa (si aplica) + CAIO

ANEXO 5: 8 preguntas clave que todo Directorio debería hacerle a la Administración

Estas preguntas buscan ser una guía que le permitan al directorio ejercitar su deber de cuidado y supervisión respecto del uso de la IA en las organizaciones que lideran, evitando riesgos que van desde la exposición a riesgos reputacionales, legales u operacionales hasta la paralización del negocio.

1. **Alineación con la estrategia y negocio:**
   ¿Esta iniciativa de IA resuelve un problema de negocio real y estratégico? ¿Cómo mediremos su retorno y su aporte al valor de la empresa? ¿Qué parte de nuestro modelo de negocio queda expuesta si no desplegamos IA al ritmo de nuestros competidores?

2. **Apetito de Riesgo:**
   ¿Tenemos un inventario centralizado y actualizado de todos los sistemas y algoritmos de IA que se usan hoy en la empresa? ¿Qué nivel de riesgo se le asignó a cada uno? ¿Cómo detectamos la IA que nadie declaró y que se está usando?

3. **Accountability:**
   ¿Quién o qué comité en la administración es el responsable final de supervisar la implementación, la ética y los riesgos de la IA? ¿Cuáles son sus atribuciones?

4. **Privacidad y ética en el uso de data:**
   ¿De dónde provienen los datos con los que entrenamos o alimentamos estos modelos? ¿Estamos garantizando el cumplimiento
   normativo (derechos de autor, protección de datos, propiedad intelectual) y evitando sesgos propios del algoritmo?

5. **Ciberseguridad y resiliencia operativa:**
   ¿Cómo estamos protegiendo nuestros modelos y datos corporativos sensibles contra filtraciones, ataques o vulnerabilidades propias de la IA de terceros? ¿Qué incidentes y cuasi incidentes de IA tuvimos en el período y qué cambiamos a partir de ellos?

6. **Supervisión Humana:**
   ¿En qué decisiones críticas la IA actúa de manera autónoma y en cuáles existe validación humana obligatoria antes de ejecutar una acción que impacte el negocio o a los clientes? ¿Contamos con mecanismo de apagado probado en casos extraordinarios?

7. **Gestión de proveedores:**
   ¿Qué auditorías o garantías exigimos a nuestros proveedores de software para asegurarnos de que los módulos de IA que nos venden cumplen con nuestros estándares de seguridad y legalidad? ¿Qué porcentaje de nuestros procesos críticos depende de un solo proveedor de IA?

8. **Talento y cultura:**
   ¿Cómo estamos preparando y reconvirtiendo a nuestros equipos para usar esta tecnología de manera segura y responsable, y cómo aseguramos que la primera línea entienda los riesgos fiduciarios de su uso?