Mendoza Legal # Revista del Colegio de Abogados y Procuradores de la Primera Circunscripción Judicial – Mendoza
ISSN 2718-7667 / www.mendozalegal.com / contacto@mendozalegal.com

DOCTRINA

NOVIEMBRE DE 2026

Compliance e inteligencia artificial: la tecnología cambia, el deber se mantiene

Análisis de la importancia del compliance en materia de inteligencia artificial, a partir de los riesgos de cumplimiento identificados en los principales marcos técnicos y regulatorios de referencia internacional. Propuesta de una matriz inicial de riesgos y un conjunto de componentes mínimos que debería implementar la función de compliance y el traslado al ordenamiento jurídico argentino y de la provincia de Mendoza.



POR SANDRA GÓMEZ

Abogada y Posgrado en Derecho de Empresas y diplomatura en Compliance, Ética Corporativa y Dirección de Procesos de Integridad por la Universidad de Mendoza. Certificación Internacional Compliance Professional en Ética y Compliance (IFCA–UCEMA), ha cursado el Programa Ejecutivo en Crypto Compliance de la UCEMA. Miembro de la Asociación Argentina de Ética y Compliance (AAEC) y responsable de la Comisión de Compliance del Colegio de Abogados y Procuradores de Mendoza de la Primera Circunscripción Judicial..

Introducción

El *compliance* es la función organizacional encargada de asegurar que una entidad —pública o privada— actúe conforme al ordenamiento jurídico vigente, a los estándares éticos y de buenas prácticas aplicables a su actividad, y a sus propias políticas internas. No se limita a verificar el cumplimiento formal de normas puntuales: su objeto es identificar, prevenir y mitigar los riesgos —legales, financieros, operativos y reputacionales— que pueden derivarse de la actividad de la organización, mediante controles, políticas internas, capacitación y monitoreo continuo. En ese sentido, *compliance* opera incluso allí donde la ley aún no ha llegado, porque su parámetro no es exclusivamente la norma vigente, sino el estándar de diligencia razonable exigible a un actor responsable en su sector.

La inteligencia artificial (IA), por su parte, puede definirse como el conjunto de tecnologías que permiten a un sistema informático ejecutar tareas que tradicionalmente requerían razonamiento o percepción humana —reconocer patrones, clasificar información, generar texto o imágenes, predecir resultados o tomar decisiones— a partir del procesamiento de grandes volúmenes de datos mediante algoritmos, y en particular mediante modelos de aprendizaje automático (machine learning) y aprendizaje profundo (deep learning). Su rasgo distintivo frente a la automatización tradicional es que el sistema no se limita a ejecutar reglas predefinidas por un programador, sino que "aprende" patrones a partir de los datos con los que fue entrenado, lo que explica tanto su utilidad como buena parte de los riesgos que se desarrollan en la presente nota: un sistema entrenado con datos sesgados, incompletos o mal curados puede producir resultados sesgados, opacos o erróneos sin que exista una línea de código identificable como "la causa" del problema.

La intersección entre ambos conceptos es el objeto de este trabajo. La adopción acelerada de sistemas de IA —tanto por el sector privado como por el sector público— ha superado ampliamente la capacidad de las legislaciones nacionales para regularla de modo integral. Ese desfasaje no suspende la responsabilidad de quien usa o implementa estas tecnologías: la traslada a los marcos jurídicos generales ya existentes (protección de datos, no discriminación, responsabilidad civil y administrativa) y a los estándares internacionales de buenas prácticas que, aunque no vinculantes, definen qué se entiende por un uso diligente y responsable de la IA. Identificar esos riesgos, traducirlos en controles concretos y anticipar su encuadre normativo es, precisamente, la tarea que le corresponde a la función de *compliance*, y es el eje que se desarrolla a continuación.

I. La importancia de compliance en materia de inteligencia artificial

El *compliance* en materia de inteligencia artificial (IA) no es un ejercicio de checklist regulatorio, sino una función que gestiona un riesgo compuesto —financiero, legal y reputacional— que surge precisamente porque la regulación no logra ir al ritmo de la tecnología. De ello se derivan tres consecuencias para la función de *compliance*.

1. **El riesgo existe, aunque no haya ley específica.** La experiencia comparada muestra que los principales casos de uso indebido de sistemas de inteligencia artificial —en selección de personal, evaluación de riesgo, o interacción automatizada con el público— no fueron sancionados como "incumplimientos de una ley de IA": fueron sancionados o repudiados bajo normas generales ya existentes —antidiscriminación, protección de datos, responsabilidad civil— aplicadas a un fenómeno nuevo. El área de *compliance* no puede esperar a que exista una "Ley de IA" para actuar.

2. **La exposición es multinivel.** Un mismo sistema de IA puede activar simultáneamente riesgo de privacidad, riesgo de discriminación, riesgo contractual frente a proveedores y riesgo reputacional, sin que estos compartimentos operen de manera aislada.

3. **El estándar de diligencia debida ya existe, aunque sea de naturaleza "blanda".** Documentos no vinculantes —los Principios de la OCDE sobre Inteligencia Artificial, el AI Risk Management Framework del NIST o las guías de la Agencia de Acceso a la Información Pública (AAIP)— funcionan como el piso de conducta esperable; aunque no sean exigibles como ley, sí son invocables para establecer si una organización actuó con la diligencia razonable, del mismo modo en que un estándar técnico de industria, sin ser ley, define el parámetro de negligencia en un litigio.

Esa diligencia debida tiene contenido concreto en los tres marcos internacionales de referencia, pese a que cada uno la articula desde un enfoque distinto.

Los Principios de la OCDE sobre Inteligencia Artificial (2019) fijan cinco valores rectores: crecimiento inclusivo y bienestar; respeto del Estado de derecho, los derechos humanos y los valores democráticos, incluyendo equidad y no discriminación; transparencia y explicabilidad;

robustez, seguridad y protección a lo largo de todo el ciclo de vida del sistema; y rendición de cuentas de los actores que desarrollan, despliegan u operan el sistema.

El AI Risk Management Framework del NIST (Estados Unidos) estructura la gestión del riesgo en cuatro funciones operativas: Gobernar (cultura y políticas de gestión de riesgo), Mapear (identificar el contexto y los riesgos del caso de uso concreto), Medir (evaluar y cuantificar esos riesgos con métricas) y Gestionar (priorizar y mitigar los riesgos detectados, con monitoreo continuo). Es el marco de mayor contenido operativo de los tres, por lo que resulta el más adecuado para diseñar la matriz de riesgo y los controles.

La Ley de Inteligencia Artificial de la Unión Europea adopta, en cambio, un enfoque basado en niveles de riesgo: prohíbe directamente ciertas prácticas consideradas de riesgo inaceptable (por ejemplo, la puntuación social); impone obligaciones reforzadas de evaluación de conformidad, documentación técnica y supervisión humana a los sistemas de "alto riesgo" (salud, empleo, administración de justicia, acceso a servicios esenciales); exige transparencia simple —declarar que se interactúa con un sistema de IA— en los de riesgo limitado; y no regula los de riesgo mínimo. Aporta así el criterio de clasificación por nivel de riesgo.

Pese a partir de enfoques distintos —valores, proceso de gestión y riesgo normativo, respectivamente— los tres marcos convergen en los mismos ejes:

– Transparencia y explicabilidad

– Supervisión humana

– Gestión continua del riesgo

– Rendición de cuentas

Esos ejes son, precisamente, la base de las seis categorías de riesgo que se desarrollan a continuación.

II. Riesgos de cumplimiento identificados a partir de fuentes internacionales

A partir de la literatura técnica relevada y de los marcos internacionales que en ella se citan —la Ley de Inteligencia Artificial de la Unión Europea, el NIST AI RMF, los Principios de la OCDE y el Informe Belmont aplicado a la IA— los riesgos de cumplimiento pueden agruparse en seis categorías:

Categoría	**Descripción del riesgo**	**Fuente**
Gobernanza y supervisión humana	Ausencia de responsables claros; falta de "humano en el bucle" antes de decisiones de impacto.	Principios OCDE; NIST AI RMF (función "Gobernar")
Sesgo y discriminación	Datos de entrenamiento no representativos que producen resultados discriminatorios (contratación, crédito, salud).	Ley de IA de la UE (prácticas de alto riesgo)

Transparencia y explicabilidad	Modelos de "caja negra" que impiden justificar una decisión ante el afectado o el regulador.	IA explicable; Ley de IA de la UE (obligaciones de transparencia)
Privacidad y datos personales	Recolección sin consentimiento; reutilización de datos para entrenamiento; fuga de datos por inyección de instrucciones.	RGPD; guías de la AAIP.
Integridad del modelo (deriva, colapso, alucinación)	Degradación del desempeño en el tiempo; generación de información falsa presentada con alta confianza.	NIST AI RMF (riesgos operacionales); estudios sobre colapso del modelo
Terceros y cadena de suministro	Proveedores de modelos de IA de propósito general sin trazabilidad de datos de entrenamiento ni cláusulas de auditoría.	Ley de IA de la UE (obligaciones a proveedores GPAI)

III. Qué debería hacer compliance

Identificados los riesgos y el estándar internacional que los enmarca, corresponde traducir ambos en una función operativa concreta. No se trata de "cumplir una ley de IA", sino de instalar una función de gestión de riesgo específica dentro de la organización, que tome el proceso del NIST AI RMF (gobernar, mapear, medir, gestionar) como estructura y los riesgos antes señalados como contenido. Esa función se despliega, como mínimo, en los siguientes componentes:

1. Inventario y clasificación de sistemas de IA: identificar qué se usa, con qué finalidad, y clasificar cada sistema por nivel de riesgo, siguiendo como método de priorización la lógica del enfoque basado en riesgo.

2. Evaluación de impacto previa (equivalente a un "AI Impact Assessment") antes de adoptar o desarrollar un sistema, documentando los datos de entrenamiento, el propósito y las limitaciones conocidas.

3. Política interna de gobernanza de IA que defina roles: quién aprueba, quién audita y quién responde ante un incidente.

4. Supervisión humana obligatoria ("human-in-the-loop") en toda decisión de alto impacto, debidamente documentada.

5. Monitoreo continuo de deriva y sesgo, en el entendimiento de que no se trata de un control de instancia única.

6. Debida diligencia de proveedores, con cláusulas contractuales de transparencia, auditabilidad y responsabilidad cuando se contrata inteligencia artificial de terceros.

7. Canal de registro y documentación que permita reconstruir por qué el sistema arribó a determinado resultado, a fin de sostener la trazabilidad como defensa ante eventuales reclamos.

Lo expuesto permite advertir que el *compliance* en materia de inteligencia artificial no introduce una disciplina nueva ni exige reinventar la función: aplica el mismo método que el *compliance* officer ya emplea en cualquier otra materia —identificar el riesgo, clasificarlo por probabilidad e impacto, controlar antes de actuar, vigilar después de actuado y documentar todo el proceso— a un objeto de riesgo hasta hace poco ajeno a su ámbito de actuación.

El inventario y clasificación por riesgo (punto 1) es la misma lógica de la matriz de riesgo de clientes o terceros en materia de cumplimiento normativo; la evaluación de impacto previa (punto 2) es una debida diligencia con otro nombre; la política interna con roles definidos (punto 3) es el programa de integridad, con un riesgo más en su agenda; la supervisión humana obligatoria (punto 4) replica el principio de doble control que ya rige la aprobación de cualquier operación sensible; el monitoreo continuo (punto 5) es el equivalente del monitoreo transaccional o de la auditoría periódica; la debida diligencia de proveedores (punto 6) es la cláusula de auditoría y de derecho de inspección que ya se exige a cualquier tercero en un programa anticorrupción; y la trazabilidad documental (punto 7) es el expediente de *compliance* de toda la vida, que permite demostrar ante un regulador, un juez o una auditoría que la decisión fue el resultado de un proceso controlado y no de un acto arbitrario. Lo que cambia, en definitiva, no es el método sino el objeto: donde antes había un cliente, un intermediario o una transacción, hoy hay también un algoritmo.

IV. Matriz de riesgo inicial

Con sustento en las premisas antes desarrolladas, se puede ensayar una matriz de riesgo genérica. En tal sentido, se propone a continuación una matriz elaborada sobre las seis categorías de riesgo previamente identificadas y ponderada conforme al criterio de probabilidad e impacto propio de los marcos internacionales de gestión de riesgo reseñados.

Se trata de un punto de partida orientativo y no de un relevamiento exhaustivo: no sustituye la evaluación de impacto que corresponde realizar sobre cada sistema en particular, y deberá revisarse y ajustarse a medida que avance el inventario de sistemas de IA de la organización y conforme a los resultados del monitoreo continuo de su desempeño.

Riesgo	**Probabilidad**	**Impacto**	**Prioridad**	**Control sugerido**
Sesgo o discriminación en decisiones automatizadas	Media-alta	Alto	1	Auditoría de datos de entrenamiento y revisión humana
Falta de explicabilidad ante reclamo o recurso	Media	Alto	1	Documentación técnica y motivación humana adicional
Uso no autorizado de IA por el personal (“shadow AI”)	Alta	Medio-alto	1	Política de uso, capacitación y monitoreo de herramientas

Filtración de datos personales o sensibles a través de sistemas de IA	Media	Alto	1	Minimización de datos, cifrado y evaluación de impacto
Deriva del modelo no detectada	Media	Medio	2	Monitoreo periódico de desempeño
Dependencia de proveedor sin cláusulas de auditoría	Media	Medio	2	Debida diligencia contractual
Alucinación o desinformación generada por IA	Alta	Medio	2	Generación aumentada por recuperación (RAG) y revisión humana de resultados críticos
Daño reputacional derivado de un incidente de IA	Baja-media	Alto	2	Plan de respuesta a incidentes

De tal forma que efectuado el inventario o relevamiento de los sistemas de inteligencia artificial en uso, resulta posible elaborar en concreto la matriz de riesgo correspondiente a la organización, que constituye el punto de partida para la elaboración del plan de acción: la asignación de responsables y plazos para cada control, la priorización de las intervenciones según el orden de prelación resultante y la revisión periódica de dicha priorización conforme avance el monitoreo continuo y se incorporen nuevos sistemas o usos de inteligencia artificial.

Como se dijo, la matriz precedente fue elaborada sobre la base de los marcos internacionales de referencia, sin anclaje en una jurisdicción determinada. Corresponde ahora trasladar ese mismo esquema de riesgos al ordenamiento jurídico argentino y, en particular, al de la Provincia de Mendoza, a fin de identificar en qué medida cada uno de esos riesgos encuentra ya un correlato normativo concreto —y no meramente una referencia de buenas prácticas— en el derecho vigente.

V. Encuadre en la normativa argentina y de Mendoza

El marco internacional reseñado se traduce localmente del siguiente modo.

Argentina no cuenta a la fecha con una ley integral de inteligencia artificial: entre 2024 y 2025 se presentaron ante el Congreso de la Nación más de cincuenta proyectos vinculados a la materia, sin que ninguno haya sido sancionado. En este contexto, el “piso normativo” opera de manera análoga al plano internacional: rige el soft law antes que la ley dura.

La Disposición N° 2/2023 de la Subsecretaría de Tecnologías de la Información y la Resolución N° 161/2023 de la Agencia de Acceso a la Información Pública constituyen el equivalente argentino a los Principios de la OCDE: recomendaciones no vinculantes que, sin embargo, fijan el estándar de diligencia exigible al sector público en materia de transparencia, explicabilidad, equidad, protección de datos, supervisión humana y rendición de cuentas.

La Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable, publicada por la AAIP en 2024,

recomienda la realización de evaluaciones de impacto y la conformación de equipos multidisciplinarios, en coincidencia directa con lo previamente señalado en presente nota.

La Ley N° 25.326 de Protección de Datos Personales alcanza el riesgo de privacidad y de datos sensibles cuando un sistema de IA procesa datos personales o de salud.

La Ley N° 9003 de Procedimiento Administrativo de la Provincia de Mendoza, en su artículo 45, exige motivar con explicación de las razones de hecho y de derecho los actos que decidan sobre derechos subjetivos o resuelvan recursos. Esta disposición constituye el anclaje legal de derecho duro —no soft law— del riesgo de falta de explicabilidad para cualquier organismo público que emplee inteligencia artificial como apoyo decisorio.

La Ley regulatoria del Sistema Administración Pública Digital de la Provincia de Mendoza (Ley 9625) y la Ley de Ciberseguridad de Mendoza (Ley N°9726), actualmente en trámite legislativo, cubren el riesgo de gobernanza de datos y ciberseguridad en el ámbito provincial, este último exigiendo evaluaciones de riesgo y comunicación de incidentes a los organismos alcanzados.

La Ley N° 23.592 provee una vía de acción concreta frente al riesgo de sesgo y discriminación derivado de decisiones asistidas por inteligencia artificial.

El repaso precedente permite verificar que, de los seis riesgos identificados en el plano internacional, al menos cuatro cuentan ya con un anclaje normativo concreto en el derecho argentino y provincial, a saber: privacidad y datos personales, transparencia y explicabilidad, sesgo y discriminación, y gobernanza de datos. Los dos restantes —gobernanza interna de los sistemas de inteligencia artificial y debida diligencia de proveedores— no cuentan, en cambio, con una norma específica sobre inteligencia artificial, pero ello no las sitúa fuera del ordenamiento vigente. Ambos aspectos integran el contenido exigible a los programas de integridad previstos en el artículo 22 de la Ley N° 27.401, en tanto ninguna entidad que cuente con un programa de integridad puede prescindir de una estructura de gobernanza interna con roles y responsables definidos, ni de mecanismos de debida diligencia sobre sus terceros y proveedores. La inteligencia artificial no es, en este sentido, una excepción que requiera una norma propia, pues es un riesgo más que ya debería estar contemplado dentro de ese programa.

VI. Conclusión

El *compliance* en materia de inteligencia artificial no depende de la existencia de una ley específica que lo exija: nace de la naturaleza misma del riesgo que la IA introduce, un riesgo compuesto, multinivel y de evolución más rápida que la capacidad regulatoria de cualquier Estado. Los casos de fracaso citados en la literatura —sesgo en procesos de reclutamiento, error en sentencias penales, filtraciones de datos, chatbots que reproducen conductas tóxicas— no fueron anticipados por una norma de inteligencia artificial, sino que se sancionaron o repudiaron bajo marcos jurídicos preexistentes —antidiscriminación, protección de datos, responsabilidad civil— aplicados a una tecnología nueva.

Esa es, precisamente, la lección para la función de *compliance*: el vacío legal no es ausencia de riesgo, sino ausencia de certeza sobre cómo habrá de calificarse jurídicamente ese riesgo una vez que se materialice.

Los marcos internacionales no vinculantes —los Principios de la OCDE, el NIST AI RMF y la Ley de IA de la Unión Europea como referencia de mejores prácticas— y sus equivalentes locales —la Disposición N° 2/2023, la Resolución AAIP N° 161/2023 y la Guía AAIP de 2024— cumplen la misma función que cualquier estándar técnico o de industria en materia de responsabilidad, pue si bien no son exigibles por sí mismos, pero sí constituyen el parámetro con el que se mide si una organización actuó razonablemente o con negligencia una vez ocurrido el daño.

La matriz de riesgo propuesta traduce ese estándar en una hoja de ruta operativa. Los riesgos de mayor prioridad —sesgo, falta de explicabilidad, uso no autorizado de herramientas de IA por el personal y filtración de datos sensibles— son también los que cuentan con anclaje normativo argentino más concreto (Ley N° 25.326, artículo 45 de la Ley N° 9003, Ley N° 23.592), lo que permite a la función de *compliance* priorizar recursos allí donde el riesgo internacional y el riesgo jurídico local coinciden. La ausencia de una ley integral de inteligencia artificial en Argentina no constituye, en este sentido, una razón para postergar la implementación de controles, sino precisamente la razón por la cual esos controles deben construirse desde ya sobre la base de los marcos internacionales disponibles y de la normativa general vigente —protección de datos, procedimiento administrativo, no discriminación—, en lugar de esperar una regulación específica.

La tecnología cambia de forma. El deber, nunca de fondo.

Bibliografía

Organismos internacionales

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (OCDE). *Recomendación del Consejo sobre Inteligencia Artificial*, OECD/LEGAL/0449, modificada el 3 de mayo de 2024. Disponible en: https://legalinstruments.oecd.org/api/download/?uri=/public/db5053b5-93e0-4cf5-a7cf-edce5ee6e893.pdf&name=OECD-LEGAL-0449%20-%20Spanish%20(as%20amended%20on%2003052024).pdf [Fecha de consulta: 2 de octubre de 2026].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1. Gaithersburg: NIST, 2023. Disponible en: https://doi.org/10.6028/NIST.AI.100-1 [Fecha de consulta: 2 de octubre de 2026].

UNIÓN EUROPEA. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. *Diario Oficial de la Unión Europea*, 2024. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02024R1689-20260727 [Fecha de consulta: 2 de octubre de 2026].

Normativa argentina

ARGENTINA. Ley N° 25.326 de Protección de Datos Personales. *Boletín Oficial de la República Argentina*, 2 de noviembre de 2000. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm [Fecha de consulta: 2 de octubre de 2026].

ARGENTINA. Ley N° 27.401 de Responsabilidad Penal de las Personas Jurídicas. *Boletín Oficial de la República Argentina*, 1 de diciembre de 2017. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/295000-299999/296846/norma.htm [Fecha de consulta: 2 de octubre de 2026].

ARGENTINA. JEFATURA DE GABINETE DE MINISTROS. SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN. Disposición N° 2/2023. *Recomendaciones para una Inteligencia Artificial Fiable*, 2023. Disponible en: https://www.argentina.gob.ar/normativa/nacional/norma-384656/texto [Fecha de consulta: 2 de octubre de 2026].

ARGENTINA. AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA (AAIP). Resolución N° 161/2023, 2023. Disponible en: https://www.argentina.gob.ar/normativa/nacional/norma-389231/texto [Fecha de consulta: 2 de octubre de 2026].

ARGENTINA. AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA (AAIP). *Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable*, 2025. Disponible en: https://www.argentina.gob.ar/sites/default/files/guia_ai-final-2025.pdf [Fecha de consulta: 2 de octubre de 2026].

Normativa provincial (Mendoza)

MENDOZA (Provincia). Ley N° 9.625, Sistema de Administración Pública Digital de la Provincia de Mendoza. *Boletín Oficial de la Provincia de Mendoza*. Disponible en: https://boe.mendoza.gov.ar/publico/pdf_pedido/0c4b4c5e1a4eec73c35dd33d19e6dd8972c113b034 [Fecha de consulta: 2 de octubre de 2026].

MENDOZA (Provincia). Ley N° 9.726, Ley de Ciberseguridad. *Boletín Oficial de la Provincia de Mendoza*. Disponible en: https://boe.mendoza.gov.ar/publico/pdf_pedido/2ca2e0a960c54303b4071b193e8a3b30131ab86d35 [Fecha de consulta: 2 de octubre de 2026].

Información para citar este artículo

Gómez, Sandra , "Compliance e inteligencia artificial: la tecnología cambia, el deber se mantiene," *Mendoza Legal - Colegio de Abogados y Procuradores 1° Circunscripción Judicial - Mendoza*, https://mendozalegal.com/omeka/items/show/1794.