GIAJ 2.0

Guía Integral de Gobernanza y Aseguramiento Jurídico de la Inteligencia Artificial

Marco doctrinal, institucional, operativo y de mejora continua para el uso profesional, trazable, auditable y defendible de IA en el ámbito jurídico y judicial

Jorge Eduardo Peralta

Tracewarden

Versión 2.0 — Primera edición pública

Buenos Aires | 2026

Ficha del documento

Título	GIAJ 2.0 — Guía Integral de Gobernanza y Aseguramiento Jurídico de la Inteligencia Artificial
Autor	Jorge Eduardo Peralta
Entidad editora	Tracewarden — tracewarden.com
Versión	2.0 — Primera edición pública
Lugar y fecha	Buenos Aires, República Argentina — 2026
DOI	Pendiente de asignación
Licencia	Creative Commons Atribución–SinDerivadas 4.0 Internacional (CC BY-ND 4.0)
Marca	GIAJ® — marca registrada ante el INPI, República Argentina

Historial de versiones

Versión 1.0. Documento marco de circulación interna, base del trabajo de consultoría y formación de Tracewarden.

Versión 2.0 (Buenos Aires, 2026). Primera edición pública. Consolida el marco original e incorpora de manera transversal el criterio material de protección de datos personales alineado con la Ley 25.326 y la nota de alineación con ISO/IEC 42001:2023, sin alterar la arquitectura central de gobernanza, trazabilidad y responsabilidad profesional.

Licencia y uso de la marca

Cita sugerida

Peralta, J. E. (2026). GIAJ 2.0: Guía Integral de Gobernanza y Aseguramiento Jurídico de la Inteligencia Artificial (Versión 2.0). Tracewarden. https://tracewarden.com

Contenido

Presentación

La inteligencia artificial ya ingresó al trabajo jurídico. Ingresó a estudios, áreas legales, organismos públicos, tribunales, fiscalías, defensorías, espacios académicos, consultoras y estructuras administrativas. Ingresó, además, de una manera que no siempre fue reflexiva, ordenada ni profesional. En muchos casos entró por conveniencia, por presión de tiempo, por fascinación tecnológica, por moda o por simple disponibilidad técnica. Entró rápido. Y precisamente por eso, en una parte importante del ecosistema jurídico, entró mal.

Ese es el problema que este documento asume sin rodeos. GIAJ 2.0 no nace para celebrar la tecnología. Nace para ponerle estructura, límites, lenguaje institucional, exigencia profesional y capacidad de defensa futura. No fue concebido como un manual de entusiasmo, ni como una guía de herramientas, ni como un catálogo de prompts. Fue diseñado como una pieza de gobierno. Su función es ordenar, hacer defendible el uso de inteligencia artificial y evitar que abogados, estudios, organismos y actores judiciales queden expuestos a errores que podrían haberse evitado con criterio, diseño, control y disciplina.

La pregunta de fondo no es si la IA puede ser útil. Puede serlo. La pregunta seria es otra: cómo debe usarse para que su utilización pueda explicarse, justificarse, auditarse, corregirse y sostenerse frente a un cliente, frente a un tribunal, frente a una autoridad disciplinaria, frente a un órgano de control o frente a una revisión institucional futura.

GIAJ 2.0 responde a esa pregunta desde una doble lógica:

- la lógica de la responsabilidad jurídica indelegable;
- y la lógica de la gobernanza institucional del uso de IA.

Cómo leer este documento

GIAJ 2.0 fue diseñado para distintos niveles de lectura.

Lectura institucional breve. Presentación, Resumen Ejecutivo, Tesis Central, Principios Rectores y Fórmula de Posicionamiento.

Lectura de implementación. Arquitectura Integral, Contexto y Alcance, Liderazgo, Planificación, Soporte, Operación, Protocolo Operativo y Hoja de Implementación.

Lectura de control y auditoría. Trazabilidad, Evaluación del Desempeño, Auditoría, Revisión por Dirección, Gestión del Error, Mejora Continua, Registro GIAJ y anexos operativos.

Lectura académica o doctrinal. Fundamento Doctrinal, Humildad Epistémica, Riesgos de Segunda Generación, IA y Garantías, Propiedad Intelectual y Gobernanza Pública.

Esta estructura busca evitar dos defectos frecuentes: el documento abstracto que no sirve para operar y el protocolo operativo que no logra explicar por qué existe. GIAJ 2.0 intenta unir ambos planos: fundamento y ejecución.

Resumen ejecutivo

GIAJ 2.0 es la Guía Integral de Gobernanza y Aseguramiento Jurídico de la Inteligencia Artificial. Es un documento marco pensado para el ecosistema jurídico argentino y adaptable a estudios jurídicos, departamentos legales, organismos públicos, instituciones académicas, equipos de compliance, entornos judiciales y estructuras de transformación digital con impacto jurídico.

Su tesis central sigue siendo simple y no admite ambigüedades: la inteligencia artificial puede asistir tareas, acelerar procesos, sugerir estructuras y ampliar capacidad operativa, pero no absorbe ni reemplaza la responsabilidad profesional, jurídica, ética ni organizacional de quien decide, firma, presenta, comunica o actúa en base a sus resultados.

La versión 2.0 agrega una segunda tesis complementaria: toda organización que desarrolla, contrata, integra o utiliza IA en procesos jurídicos o judiciales necesita un sistema de gestión capaz de definir contexto, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua.

Por eso, GIAJ 2.0 no se limita a recomendar prudencia. Va más lejos. Propone una arquitectura integral compuesta por:

- principios doctrinales;
- criterios de admisibilidad;
- clasificación de tareas y riesgos;
- reglas de gobierno institucional;
- exigencias de trazabilidad;
- niveles de supervisión humana;
- gobernanza de datos;
- evaluación de impacto jurídico-institucional;
- protocolos de validación y auditoría;
- mecanismos de respuesta a incidentes y mejora continua;
- y una hoja de implementación gradual.

En el contexto argentino, esa arquitectura tampoco puede desligarse del tratamiento de datos personales. Cuando la operación con IA alcance información de personas físicas, la gobernanza debe leerse de manera materialmente compatible con los principios de licitud, finalidad, calidad, seguridad, confidencialidad y circulación restringida que informan la Ley 25.326 de Protección de Datos Personales y su reglamentación, sin desplazar el deber profesional propio del trabajo jurídico.

El documento parte de una constatación práctica: en el trabajo jurídico, el riesgo principal de la IA no es solamente que se equivoque, sino que el profesional o la organización confundan una salida plausible con una conclusión fundada, o que carezcan luego de evidencia suficiente para demostrar que controlaron, verificaron y gobernaron razonablemente ese uso.

GIAJ 2.0 cumple seis funciones simultáneas:

1. Doctrinal: fija una posición conceptual seria sobre IA y responsabilidad jurídica.

2. Institucional: ofrece una base común para políticas internas, protocolos, formación y gobierno organizacional.
3. Operativa: ordena tareas, roles, controles, criterios mínimos de uso y circuitos de aprobación.
4. Probatoria: fortalece la posibilidad de demostrar diligencia, revisión, custodia y trazabilidad.
5. Auditora: permite medir, revisar, corregir y mejorar el sistema de uso de IA.
6. Estratégica: posiciona a quien adopta este marco como actor serio frente al uso desordenado de IA en el derecho y la justicia.

I. Naturaleza, función y alcance de GIAJ 2.0

1. Qué es GIAJ 2.0

GIAJ 2.0 es una arquitectura institucional de gobernanza aplicada al uso de inteligencia artificial en el ámbito jurídico y judicial. Está redactado en lenguaje profesional pero accesible. Busca ser suficientemente sólido para sostener una posición doctrinal seria y, al mismo tiempo, suficientemente claro para ser entendido por abogados, funcionarios, directivos, docentes y usuarios no técnicos.

Su diseño responde a una necesidad concreta del mercado jurídico contemporáneo: el sector ya no necesita únicamente saber qué puede hacer la IA, sino principalmente qué no debe hacer, bajo qué condiciones puede emplearse, cómo debe controlarse, cómo debe documentarse ese control y cómo debe mejorarse con el tiempo.

2. Qué no es GIAJ 2.0

GIAJ 2.0 no es:

- un instructivo de prompts;
- un recetario de productividad;
- una autorización general para automatizar sin límites;
- un documento técnico reservado a especialistas en software;
- una defensa ingenua de la innovación;
- una promesa de eliminación del criterio jurídico humano;
- una política vacía de marketing institucional;
- ni una mera adaptación cosmética de estándares externos.

3. A quién está dirigido

Este documento fue pensado para:

- estudios jurídicos individuales o colectivos;
- departamentos legales de empresas;
- organismos públicos y entes de control;
- fiscalías, defensorías, oficinas judiciales y estructuras de administración de justicia;

- consultoras legales, de compliance y de transformación digital;
- instituciones educativas y programas de formación jurídica;
- actores del sistema judicial;
- responsables de innovación, modernización o transformación digital con impacto sobre procesos jurídicos.

4. Qué problema busca resolver

GIAJ 2.0 busca resolver un problema de esta época: la entrada acelerada de sistemas de IA al trabajo jurídico sin un marco suficientemente serio de custodia, validación, límites, legitimidad y defensa futura del proceso. No pretende bloquear el uso de la tecnología. Pretende impedir su incorporación irresponsable.

II. La tesis central de GIAJ 2.0

La tesis central puede formularse así:

> **La inteligencia artificial puede participar en la producción de trabajo jurídico, pero mientras exista decisión humana, firma humana, presentación humana o deber humano frente al cliente, la responsabilidad no se delega.**

Esa tesis tiene consecuencias concretas.

Primera consecuencia: el output de IA nunca debe recibir estatus automático de verdad jurídica, suficiencia técnica o aptitud procesal.

Segunda consecuencia: cuanto más cerca esté la herramienta del núcleo decisional —estrategia, interpretación, recomendación, redacción final, firma, prueba, persecución penal, determinación de riesgo o comunicación sensible— mayor debe ser la intensidad del control humano y menor el margen para automatismos opacos.

Tercera consecuencia: no alcanza con revisar el contenido. También debe poder reconstruirse el proceso. En derecho no solo importa el resultado. Importa cómo se llegó a él.

Cuarta consecuencia: la organización que usa IA sin reglas internas, sin clasificación de riesgos, sin política de datos, sin responsables y sin trazabilidad mínima no está innovando; está acumulando exposición.

Quinta consecuencia: en el ámbito judicial y público, además de diligencia profesional, también está en juego la legitimidad institucional del uso de la herramienta.

La segunda tesis de GIAJ 2.0 es la siguiente:

> **Toda organización que usa IA en funciones jurídicas o judiciales necesita un sistema de gestión que permita definir contexto, asignar liderazgo, planificar riesgos y objetivos, dar soporte, operar con controles, evaluar resultados y mejorar de forma continua.**

Dicho sin rodeos: ya no alcanza con usar IA con cuidado. Hay que poder demostrar que la organización sabe gobernarla.

III. Fundamento doctrinal: por qué el derecho no puede tratar a la IA como un simple atajo

El trabajo jurídico no es mera producción de texto. Es interpretación situada, toma de posición responsable, evaluación de hechos, identificación de relevancia normativa, administración del riesgo, tutela de intereses ajenos, protección de derechos y decisión profesional bajo estándares de diligencia.

Un sistema generativo puede construir frases plausibles, reorganizar material, imitar estilos y producir respuestas con apariencia de solvencia. Pero no asume secreto profesional, no responde disciplinariamente, no comparece ante un tribunal, no soporta sanción patrimonial, no es sujeto de deberes de lealtad procesal y no carga con las consecuencias institucionales de una presentación defectuosa.

Eso marca una diferencia decisiva entre asistencia cognitiva y responsabilidad jurídica. La IA puede intervenir en la primera. La segunda sigue siendo humana e institucional. Por eso GIAJ 2.0 adopta cinco premisas doctrinales fuertes.

1. Premisa de no sustitución

La IA no sustituye al profesional ni al órgano competente. Como máximo, lo asiste.

2. Premisa de opacidad relativa

Aunque la herramienta sea útil, su funcionamiento no siempre es plenamente inteligible para el usuario jurídico. Esa opacidad obliga a elevar el estándar de prudencia y no a bajarlo.

3. Premisa de falibilidad estructural

La generación probabilística puede producir errores convincentes. La apariencia de coherencia no garantiza fidelidad normativa, fáctica ni probatoria.

4. Premisa de responsabilidad concentrada

Aunque la producción sea híbrida, la responsabilidad jurídica permanece concentrada en la persona o institución que decide usar, adoptar, comunicar o presentar el resultado.

5. Premisa de legitimidad institucional

En funciones públicas, judiciales o de alto impacto, no alcanza con que la herramienta sea útil. También debe poder justificarse su uso desde la legalidad, la proporcionalidad, el control humano, la razonabilidad del procedimiento y la rendición de cuentas.

Consecuencia institucional de estas premisas

En el ámbito jurídico, usar IA nunca puede equivaler a externalizar el deber profesional. A lo sumo permite redistribuir parte del esfuerzo operativo. Pero la obligación de estudiar, comprender, controlar, justificar, documentar y responder permanece en quien ejerce la función jurídica o dirige la organización que la ejerce.

Dicho de forma más directa: la IA puede acelerar el trabajo; no puede absorber el deber.

IV. Humildad epistémica como disciplina profesional

GIAJ 2.0 incorpora como eje doctrinal la humildad epistémica. No como consigna blanda, sino como regla metodológica.

Humildad epistémica significa que toda salida de IA debe ser tratada como hipótesis preliminar hasta que una verificación suficiente la vuelva utilizable. Significa asumir que el sistema puede sonar seguro sin estarlo, que puede completar vacíos con aparente naturalidad, que puede confundir precedentes, sintetizar mal una norma, deformar una relación fáctica o construir una seguridad verbal que el caso no merece.

En el campo jurídico, la soberbia tecnológica es particularmente peligrosa. Porque la forma puede engañar. Un texto bien escrito puede estar mal. Una cita plausible puede no existir. Una conclusión elegante puede ser procesalmente ruinosa. Por eso la humildad epistémica no es un rasgo psicológico. Es una disciplina profesional.

Sus traducciones operativas son claras:

- no confiar en la forma por encima de la fuente;
- no usar outputs sin contraste independiente;
- no equiparar velocidad con suficiencia;
- no disimular con seguridad verbal lo que todavía no fue verificado;
- no presentar revisión superficial como control sustantivo;
- no convertir la herramienta en sustituto silencioso del criterio.

V. Glosario mínimo de uso institucional

IA jurídica

Uso de sistemas de inteligencia artificial en tareas vinculadas directa o indirectamente con trabajo jurídico, judicial, regulatorio, de compliance, contractual, académico o institucional.

Gobernanza

Conjunto de reglas, responsables, límites, controles y mecanismos de revisión destinados a ordenar el uso de IA dentro de una organización.

Aseguramiento jurídico

Conjunto de medidas destinadas a garantizar que el uso de IA no degrade deberes profesionales, estándares de diligencia, legalidad, prueba, defensa futura ni legitimidad institucional.

Supervisión humana efectiva

Revisión sustantiva, responsable y suficiente del proceso y del resultado, realizada por una persona con competencia real y capacidad de corregir, detener o invalidar el uso de IA.

Trazabilidad reconstructiva

Capacidad de reconstruir razonablemente qué herramienta se usó, con qué finalidad, sobre qué insumos, bajo qué criterios, con qué revisión y con qué decisión final.

Evaluación de impacto jurídico-institucional

Análisis previo o posterior de un sistema o caso de uso de IA para determinar su posible efecto sobre derechos, deberes profesionales, legalidad, prueba, confidencialidad, sesgo, debido proceso, legitimidad y responsabilidad organizacional.

No conformidad

Desvío respecto de la política, los procedimientos, los criterios de riesgo, las reglas de operación o los controles establecidos por la organización.

CAPA jurídico-institucional

Sistema de acciones correctivas y preventivas destinado a responder a errores, incidentes, hallazgos de auditoría o debilidades estructurales del sistema de gestión de IA.

VI. Los catorce principios rectores de GIAJ 2.0

1. Centralidad humana de la decisión

La decisión relevante debe permanecer bajo control humano efectivo.

2. Responsabilidad indelegable

Mientras exista firma humana, presentación humana o deber humano, la responsabilidad no se delega.

3. Humildad epistémica

Toda salida de IA es hipótesis preliminar hasta verificación suficiente.

4. Verificación sustantiva

La revisión debe recaer sobre fuentes, hechos, contexto, razonamiento y consecuencia jurídica.

5. Proporcionalidad según riesgo

A mayor impacto, mayor exigencia de control, revisión, documentación y autorización.

6. Trazabilidad reconstructiva

El proceso debe poder reconstruirse de forma razonable si luego es cuestionado.

7. Gobernanza organizacional

El uso de IA exige reglas, responsables, política, formación, auditoría y mejora.

8. Minimización y custodia del dato

Solo debe utilizarse la información necesaria y bajo condiciones compatibles con secreto profesional, confidencialidad y protección de datos.

En la práctica argentina, este principio debe interpretarse además en armonía con la Ley 25.326: no todo dato útil puede cargarse, circular o reutilizarse sin necesidad, finalidad compatible y resguardo suficiente.

9. Transparencia funcional

Debe poder explicarse para qué se usa la herramienta, con qué alcance y bajo qué intervención humana.

10. Auditabilidad

La organización debe poder revisar periódicamente el sistema, detectar desvíos y producir evidencia de diligencia.

11. Corrección institucional del error

Todo incidente relevante debe generar respuesta, documentación, corrección y aprendizaje.

12. Mejora continua

La gobernanza de IA no es un acto único. Es un ciclo de revisión, ajuste y maduración.

13. Legitimidad institucional

En funciones públicas o judiciales, el uso de IA debe ser compatible con legalidad, razonabilidad, proporcionalidad y control.

14. Defensa futura del proceso

La organización debe actuar como si un tercero fuera a pedir mañana explicaciones completas sobre cómo se usó la IA hoy.

VII. Arquitectura integral del modelo GIAJ 2.0

GIAJ 2.0 se estructura sobre siete capas:

1. Capa doctrinal: tesis, premisas y principios.
2. Capa institucional: política, liderazgo, alcance, roles y apetito de riesgo.
3. Capa operativa: admisibilidad, clasificación de tareas, flujos de aprobación, supervisión y trazabilidad.
4. Capa de datos y evidencia: gobernanza de datos, documentación, registros y custodia.
5. Capa de control y auditoría: indicadores, monitoreo, revisión y auditoría interna.
6. Capa de respuesta y mejora: incidentes, no conformidades, acciones correctivas, preventivas y lecciones aprendidas.
7. Capa estratégica: posicionamiento, reputación, legitimidad y preparación frente a regulaciones futuras.

Esta arquitectura busca que el uso de IA sea:

– profesionalmente defensible;

- institucionalmente gobernable;
- operativamente usable;
- jurídicamente explicable;
- y estratégicamente sostenible.

VIII. Contexto, alcance y partes interesadas del sistema

1. Contexto organizacional

Toda adopción seria de IA debe comenzar por una definición expresa de contexto. La organización tiene que saber dónde está usando IA, para qué, con qué procesos impactados, con qué dependencia tecnológica y con qué tipo de riesgo jurídico o institucional.

2. Alcance

El alcance no debe definirse solo por tecnología. Debe definirse por proceso afectado. Entre otros:

- investigación jurídica;
- redacción y revisión documental;
- clasificación, búsqueda y síntesis;
- trabajo contractual;
- atención y soporte a usuarios;
- gestión judicial;
- compliance y monitoreo regulatorio;
- análisis de riesgo;
- formación y producción académica;
- apoyo a decisiones administrativas o jurisdiccionales.

3. Partes interesadas

La organización debe identificar, según corresponda:

- clientes;
- abogados y equipos internos;
- jueces, fiscales, defensores y funcionarios;
- usuarios o administrados;
- proveedores de tecnología;
- colegios profesionales;
- autoridades regulatorias;
- órganos de control;
- áreas de auditoría o compliance;
- comunidad académica;
- ciudadanía, cuando el uso tenga proyección pública.

4. Criterio de alcance responsable

No todo caso de uso merece el mismo trato. Debe distinguirse entre:

- uso auxiliar de bajo impacto;
- uso sensible con impacto profesional relevante;
- uso de alto impacto sobre derechos, decisiones, prueba, acceso a justicia, persecución penal o actuación estatal.

IX. Liderazgo, política institucional y gobierno directivo

1. Liderazgo real

La gobernanza de IA fracasa cuando se terceriza silenciosamente hacia usuarios dispersos. La dirección debe asumir un rol visible: definir política, aprobar criterios de riesgo, asignar recursos, crear responsables y revisar periódicamente el desempeño del sistema.

2. Política institucional de IA

Toda organización madura debería tener una política breve y clara que establezca:

- finalidad del uso de IA;
- principios obligatorios;
- usos permitidos, restringidos y prohibidos;
- exigencia de revisión humana;
- reglas de confidencialidad y datos;
- criterios de trazabilidad;
- gestión del error;
- obligación de formación;
- y mecanismos de reporte.

Cuando la organización trate datos personales en flujos asistidos por IA, esa política debería conectar expresamente las reglas internas de uso con los principios de protección de datos personales de la Ley 25.326, definiendo finalidades, perfiles de acceso, criterios de seguridad, conservación, anonimización cuando corresponda y límites de reutilización.

3. Gobierno y responsabilidades mínimas

Responsable político o directivo. Aprueba política, alcance, recursos y revisión periódica.

Responsable de implementación. Coordina el sistema, mantiene matrices, procedimientos y despliegue.

Responsable jurídico de revisión. Valida criterios, revisa usos sensibles y define exigencias de control jurídico.

Responsable de datos y fuentes. Supervisa confidencialidad, clasificación, minimización y custodia.

Usuarios autorizados. Operan dentro de reglas, registran usos cuando corresponda y respetan restricciones.

Instancia de auditoría o revisión periódica. Evalúa cumplimiento, desempeño, incidentes y mejora.

X. Planificación: riesgos, objetivos y gestión del cambio

1. Metodología de riesgo

Toda organización que use IA debe identificar riesgos al menos en estas categorías:

- error normativo;
- cita inexistente o no verificable;
- alucinación fáctica;
- sesgo o trato desigual;
- pérdida de secreto profesional o confidencialidad;
- contaminación de prueba o evidencia;
- automatización improcedente;
- opacidad del proveedor;
- degradación del criterio profesional;
- daño reputacional;
- incumplimiento contractual o regulatorio;
- dependencia tecnológica no gobernada.

2. Objetivos del sistema

La organización debe fijar objetivos medibles, por ejemplo:

- porcentaje de usos registrados en procesos sensibles;
- porcentaje de personal formado por rol;
- porcentaje de casos de uso con evaluación previa;
- tiempo de cierre de incidentes;
- porcentaje de proveedores evaluados;
- número de auditorías realizadas;
- porcentaje de revisión sustantiva documentada.

3. Gestión del cambio

Todo cambio relevante debe gatillar revisión. Entre otros:

- cambio de proveedor;
- cambio de versión o modelo;
- cambio de finalidad;
- incorporación de nuevas bases de datos;

- integración con sistemas internos;
- ampliación de usuarios;
- nuevo colectivo afectado;
- cambio regulatorio o jurisprudencial significativo.

XI. Soporte organizacional

1. Recursos

No alcanza con pedir prudencia. Deben existir horas, responsables, presupuesto, plantillas, repositorios, soporte técnico y tiempo real de revisión.

2. Competencias por rol

No todos necesitan saber lo mismo. Debe haber una matriz de competencias diferenciada para:

- usuario operativo;
- revisor jurídico;
- líder de implementación;
- responsable de datos;
- auditor interno;
- dirección.

3. Formación

La formación debe cubrir, como mínimo:

- límites y riesgos de la IA generativa;
- verificación de fuentes y citas;
- clasificación de tareas;
- secreto profesional y datos;
- principios básicos de protección de datos personales y criterios de compatibilidad práctica con la Ley 25.326;
- trazabilidad y registro;
- sesgos y control humano;
- incidentes y reporte;
- criterios específicos según área penal, contenciosa, administrativa, académica o pública.

4. Comunicación

Debe existir una estrategia mínima de comunicación:

- interna, para reglas, cambios, alertas y formación;
- externa, para transparencia funcional, explicaciones al cliente y respuesta ante incidentes.

5. Información documentada

Toda organización madura debería controlar al menos:

- política;
- procedimientos;
- matrices de riesgo;
- registros de casos de uso;
- auditorías;
- incidentes;
- evidencia de capacitación;
- revisiones por dirección.

XII. Operación: del principio a la práctica

1. Criterio de admisibilidad

Antes de usar IA en una tarea, deberían responderse cinco preguntas:

1. ¿La tarea admite asistencia tecnológica sin vaciar el deber profesional?
2. ¿El dato puede exponerse en el entorno elegido?
3. ¿La herramienta es compatible con el nivel de riesgo del proceso?
4. ¿Puede reconstruirse el proceso si más adelante alguien lo cuestiona?
5. ¿Hay una persona claramente identificable que asuma la revisión final?

Si alguna respuesta es negativa, el uso debe restringirse, rediseñarse o descartarse.

En particular, la segunda pregunta no puede resolverse de manera intuitiva ni por mera comodidad operativa: si intervienen datos personales, la decisión debe ser compatible con la finalidad del tratamiento, la necesidad concreta de uso, la sensibilidad de la información, el nivel de seguridad del entorno y el estándar de confidencialidad exigible según la Ley 25.326 y el secreto profesional.

2. Clasificación de tareas

Tareas normalmente admisibles con control básico

- lluvia de ideas;
- organización preliminar de materiales;
- reformulación expresiva no sensible;
- resúmenes exploratorios sobre material ya verificado;
- apoyo en diseño de estructura de documentos.

Tareas admisibles con control reforzado

- síntesis jurídica orientativa;
- propuestas de redacción contractual;
- detección preliminar de problemas normativos;

- clasificación documental en entornos controlados;
- asistencia en formación o investigación interna.

Tareas de alto riesgo o severamente restringidas

- redacción final de escritos sin revisión sustantiva;
- recomendaciones jurídicas personalizadas sin validación humana competente;
- determinación automatizada de estrategia procesal;
- uso sobre datos sensibles o reservados en entornos no aprobados;
- evaluación automatizada con impacto sobre derechos;
- decisiones penales o cuasi sancionatorias sin control humano robusto.

3. Señales de alerta

Debe detenerse el proceso y escalarse revisión cuando aparezcan, entre otras, estas señales:

- citas no verificables;
- exceso de seguridad verbal sin fuente;
- razonamiento elegante pero jurídicamente impreciso;
- uso de datos sensibles sin aprobación;
- presión de tiempo que degrade revisión;
- dependencia creciente del output sin comprensión del caso;
- ampliación silenciosa de usos no aprobados.

4. Gobernanza de datos

La gobernanza de datos es uno de los puntos ciegos que más daño puede causar.

En el ecosistema jurídico argentino, esta materia no debe tratarse como un apéndice menor de compliance. Cuando la información involucre datos personales, la organización debe operar con un criterio materialmente compatible con la Ley 25.326: usar solo lo necesario, limitar finalidades, restringir accesos, reforzar seguridad, preservar confidencialidad y evitar reutilizaciones incompatibles con el motivo por el cual el dato fue obtenido, confiado o incorporado al expediente o al asunto.

Debe existir, como mínimo:

- clasificación del dato;
- criterio de minimización;
- criterio de finalidad y compatibilidad de uso;
- medidas de seguridad proporcionales al tipo de dato, al entorno y al nivel de exposición;
- anonimización o seudonimización cuando corresponda;
- prohibición de carga de información especialmente protegida en entornos no autorizados;
- registro de proveedores y condiciones de tratamiento;
- reglas para secretos profesionales, documentos reservados y evidencia.

5. Supervisión humana efectiva

Supervisión básica. Control de coherencia general y adecuación formal en tareas de bajo riesgo.

Supervisión reforzada. Contraste de fuentes, contexto, hechos, razonamiento y ajuste jurídico en tareas de riesgo medio.

Supervisión decisional. Revisión profunda, con validación competente, en tareas de alto impacto o cercanas a la decisión relevante.

Revisar no es mirar por arriba. Revisar es estudiar si lo producido puede ser sostenido profesionalmente.

6. Trazabilidad

Trazabilidad mínima

- herramienta utilizada;
- fecha;
- finalidad;
- usuario;
- decisión final humana.

Trazabilidad reforzada

Además de lo anterior:

- insumos utilizados;
- criterios de revisión;
- fuentes validadas;
- ajustes relevantes;
- incidentes detectados;
- versión o proveedor;
- aprobación o restricción del caso de uso.

7. Evaluación de impacto jurídico-institucional

Toda organización debería contar con un formulario o matriz para evaluar, al menos:

- finalidad del uso;
- población o sujetos afectados;
- nivel de autonomía;
- impacto sobre derechos o deberes;
- datos comprometidos;
- riesgo de sesgo;
- necesidad de control humano reforzado;
- exigencia de explicación;
- necesidad de aprobación específica;

- compatibilidad con legalidad, debido proceso y legitimidad institucional;
- compatibilidad con protección de datos personales, deber de confidencialidad y resguardos alineados con la Ley 25.326.

8. Gestión operativa del cambio

Todo cambio relevante en un sistema o caso de uso debe activar revisión previa, y en ciertos casos nueva evaluación de impacto.

XIII. Evaluación del desempeño, auditoría y revisión por dirección

1. Indicadores mínimos

La organización debería medir al menos:

- incidentes por tipo;
- porcentaje de usos sensibles registrados;
- casos con revisión insuficiente detectada;
- proveedores evaluados;
- tiempo de corrección;
- capacitación completada por rol;
- hallazgos de auditoría;
- porcentaje de acciones correctivas cerradas.

2. Auditoría interna

Debe existir revisión periódica del sistema. Esa auditoría puede incluir:

- muestreo de casos de uso;
- verificación documental;
- revisión de trazabilidad;
- cumplimiento de política;
- análisis de permisos y accesos;
- control de proveedores;
- análisis de incidentes y reincidencias.

3. Revisión por dirección

La dirección debe revisar periódicamente:

- desempeño del sistema;
- incidentes relevantes;
- brechas de recursos;
- cambios normativos o institucionales;
- necesidad de modificar política, alcance o controles;

– decisiones estratégicas de continuidad, restricción o expansión del uso de IA.

XIV. Gestión del error, no conformidades y mejora continua

1. Gestión del error

El error no debe tratarse solo como falla individual. Debe analizarse también como síntoma de debilidad de proceso.

2. No conformidades

Toda desviación respecto de política, procedimientos, criterios de riesgo o reglas de operación debe registrarse, evaluarse y corregirse.

3. CAPA jurídico-institucional

La respuesta madura a incidentes exige:

– identificación del problema;
– contención inmediata;
– análisis de causa raíz;
– acción correctiva;
– acción preventiva;
– responsable;
– plazo;
– verificación de cierre.

4. Lecciones aprendidas

Todo incidente relevante debe dejar una enseñanza operativa: modificación de plantillas, cambio de control, restricción de uso, refuerzo de capacitación o rediseño del proceso.

5. Mejora continua

La mejora continua es la diferencia entre una política decorativa y un sistema vivo.

XV. Aplicación según tipo de organización

1. Estudios jurídicos

Necesitan foco en secreto profesional, control de calidad, trazabilidad mínima, uso restringido en escritos y relación con el cliente.

2. Departamentos legales y compliance

Necesitan foco en contratos, políticas internas, proveedores, riesgos regulatorios, matrices de uso y evidencia de diligencia.

3. Organismos públicos

Necesitan foco en legalidad, motivación, transparencia funcional, rendición de cuentas, debido procedimiento y legitimidad institucional.

4. Sistema judicial

Necesita foco en independencia, debido proceso, proporcionalidad, prueba, control humano reforzado, no automatización decisional opaca y capacidad de explicación.

5. Instituciones académicas

Necesitan foco en integridad, formación rigurosa, transparencia metodológica, evaluación honesta y procedencia de materiales.

XVI. IA, sistema de justicia, proceso penal y garantías

El campo penal exige un estándar reforzado. Cuando la IA toca investigación, persecución, selección de casos, análisis de riesgo, valoración de información, apoyo a decisiones cautelares o gestión de evidencia, el problema ya no es solo de productividad. Es de garantías.

Por eso, toda adopción en esta materia debería examinar expresamente:

- riesgo de sesgo;
- proporcionalidad del uso;
- afectación sobre presunción de inocencia;
- control de legalidad;
- necesidad de intervención humana competente;
- explicabilidad suficiente;
- trazabilidad de criterios;
- compatibilidad con debido proceso y defensa.

La regla de prudencia aquí debe ser más severa: cuanto mayor sea la incidencia sobre derechos, libertad, prueba o coerción estatal, menor debe ser el margen para automatismos y mayor la exigencia de documentación y revisión.

XVII. Propiedad intelectual, procedencia de materiales y reutilización de outputs

La adopción madura de IA no puede ignorar la cuestión de la procedencia. Toda organización debería analizar, según su contexto:

- origen de materiales cargados al sistema;
- licencias o restricciones de uso;
- condiciones del proveedor;
- reutilización de contenidos generados;

- riesgo de incorporar expresiones, estructuras o materiales de terceros sin control suficiente;
- necesidad de transparencia sobre participación de IA en ciertos productos.

No se trata solo de evitar litigios. Se trata de evitar contaminación documental y pérdida de seriedad metodológica.

XVIII. Relación con el cliente y transparencia funcional

La relación con el cliente exige sobriedad y claridad. No toda participación de IA debe informarse de la misma manera, pero toda organización debería poder explicar su política general cuando ello sea relevante para confianza, diligencia, confidencialidad o alcance del servicio.

La transparencia funcional no exige exhibir todo el proceso técnico. Exige que la organización pueda explicar razonablemente:

- qué controles usa;
- qué no delega;
- cómo protege la información;
- cómo valida lo que presenta;
- y cómo responde si ocurre un incidente.

XIX. Adaptación al contexto argentino y bonaerense

GIAJ 2.0 fue pensado para convivir con el sistema normativo argentino y con particular sensibilidad hacia la Provincia de Buenos Aires. Eso implica atender, entre otros, a:

- deberes profesionales y éticos del abogado;
- secreto profesional;
- deber de diligencia;
- reglas procesales y carga argumental;
- exigencias de motivación y prueba;
- responsabilidades estatales y administrativas;
- trazabilidad y defensa futura en expedientes y actuaciones.

La adaptación local no significa provincialismo estrecho. Significa capacidad de aterrizar principios globales a un ecosistema jurídico concreto.

XX. Modelos de madurez organizacional GIAJ

Nivel 1. Uso espontáneo. No hay política, ni límites, ni registros. El uso depende de cada persona.

Nivel 2. Uso tolerado. Existen advertencias generales, pero no un sistema de control real.

Nivel 3. Uso ordenado. Hay política, clasificación básica, formación mínima y revisión más o menos estable.

Nivel 4. Uso gobernado. Hay roles, matrices, trazabilidad, evaluación de impacto, auditoría e incidentes gestionados.

Nivel 5. Uso institucionalmente maduro. Existe sistema de gestión consolidado, revisión directiva, mejora continua y capacidad real de explicación, defensa y adaptación regulatoria.

XXI. Paquete mínimo documental de una organización madura

1. Política institucional de IA.
2. Matriz de casos de uso permitidos, restringidos y prohibidos.
3. Metodología de evaluación de riesgo.
4. Formulario de evaluación de impacto jurídico-institucional.
5. Registro de sistemas, proveedores, versiones y responsables.
6. Protocolo de incidentes, no conformidades y CAPA.
7. Plan anual de formación y matriz de competencias.
8. Programa de auditoría interna y revisión por dirección.
9. Reglas de transparencia funcional.
10. Repositorio de evidencia de diligencia y trazabilidad.

XXII. Protocolo operativo mínimo GIAJ 2.0

1. Identificar la tarea.
2. Clasificar su riesgo.
3. Verificar si el dato puede usarse en el entorno elegido.
4. Evaluar si se requiere aprobación previa.
5. Ejecutar bajo criterio de minimización.
6. Revisar con intensidad acorde al riesgo.
7. Validar fuentes, hechos, contexto y conclusión.
8. Registrar trazabilidad cuando corresponda.
9. Corregir o descartar el output si no es defendible.
10. Escalar incidentes, errores o dudas relevantes.
11. Conservar evidencia mínima.
12. Retroalimentar el sistema con hallazgos y mejoras.

XXIII. Formación y cultura organizacional

No hay gobernanza real sin cultura organizacional. La organización que declara prudencia pero premia velocidad ciega está incubando errores. La cultura que GIAJ 2.0 propone se resume así:

- mejor una demora explicable que una presentación ruinosa;
- mejor un rechazo preventivo que una automatización improcedente;
- mejor una revisión incómoda que una falsa seguridad;
- mejor una política exigente que una innovación imposible de defender.

XXIV. Indicadores mínimos para evaluar si GIAJ 2.0 está funcionando

- porcentaje de personal formado;
- porcentaje de casos de uso clasificados;
- porcentaje de usos sensibles con trazabilidad completa;
- número de incidentes por trimestre;
- tiempo medio de cierre de acciones correctivas;
- porcentaje de auditorías ejecutadas;
- cantidad de hallazgos recurrentes;
- grado de madurez organizacional alcanzado.

XXV. Hoja de implementación en cinco etapas

Etapa 1. Diagnóstico. Mapa de usos actuales, proveedores, riesgos, datos y actores.

Etapa 2. Diseño. Definición de política, alcance, roles, matrices y criterios de control.

Etapa 3. Implementación. Capacitación, despliegue de procedimientos, registros y pilotos.

Etapa 4. Auditoría inicial. Revisión de desvíos, incidentes, vacíos documentales y fallas de supervisión.

Etapa 5. Consolidación. Mejora continua, revisión por dirección, madurez y preparación regulatoria.

XXVI. Riesgos de segunda generación

Una organización puede superar los errores más burdos y aun así quedar expuesta a riesgos más sofisticados.

1. Dependencia opaca de proveedores

Se usa una herramienta cuya lógica, límites o cambios no son comprendidos.

2. Degradación del criterio profesional

El equipo empieza a pensar menos porque la herramienta responde más.

3. Pérdida de memoria del proceso

Se conserva el resultado, pero no el camino ni la revisión que lo volvió utilizable.

4. Normalización del atajo

Lo excepcional se vuelve rutina y la revisión se vacía.

5. Simulación de gobernanza

Existen documentos, pero no operación real, auditoría ni mejora.

XXVII. Fórmula de posicionamiento

La inteligencia artificial ya entró al trabajo jurídico, pero entró mal. La respuesta seria no es prohibirla ni celebrarla sin límites. La respuesta seria es gobernarla.

> **GIAJ 2.0 expresa esa posición: no alcanza con usar IA; hay que poder defender cómo se usó. Eso exige trazabilidad, validación, documentación, política, responsabilidad, mejora y criterio jurídico.**

XXVIII. Manifiesto GIAJ 2.0

1. La inteligencia artificial puede asistir trabajo jurídico, pero no reemplaza la responsabilidad del profesional o de la institución.
2. La decisión relevante debe permanecer bajo control humano efectivo.
3. Todo output algorítmico es una hipótesis hasta que una verificación suficiente lo vuelva utilizable.
4. La velocidad nunca equivale por sí sola a calidad jurídica.
5. La apariencia de coherencia no sustituye a la fuente, al contexto ni al criterio.
6. La innovación sin gobernanza es una forma de exposición profesional.
7. La trazabilidad es memoria defensiva de la diligencia.
8. La custodia del dato forma parte del núcleo del deber profesional.
9. La revisión humana solo vale si es sustantiva.
10. La organización que usa IA sin política, sin límites, sin registro y sin mejora no está modernizando: está acumulando riesgo.
11. En funciones públicas o judiciales, la legitimidad del uso importa tanto como su utilidad.
12. La autoridad profesional futura dependerá, en parte, de poder demostrar cómo se trabajó con IA.
13. Mientras exista firma humana, debe existir responsabilidad humana y custodia humana.

14. La buena gobernanza de IA no es una moda: es una condición de seriedad institucional.

XXIX. Cierre

GIAJ 2.0 no propone una relación ingenua con la inteligencia artificial. Tampoco una relación temerosa. Propone una relación seria.

Seria significa: usar cuando corresponde, restringir cuando hace falta, prohibir cuando el riesgo supera la utilidad, documentar lo que importa, revisar lo que duele, corregir lo que falla y mejorar antes de que la regulación o el conflicto obliguen a hacerlo.

Ese es el sentido de este documento. No es un elogio de la IA. Es un marco para que su uso, cuando exista, pueda sostenerse.

Anexo. Nota de alineación con ISO/IEC 42001

Sin reducirse a una traslación mecánica de estándares externos ni implicar certificación alguna, GIAJ 2.0 fue concebido de manera materialmente compatible con la lógica de sistema de gestión de IA de ISO/IEC 42001:2023. Esa compatibilidad se expresa en la exigencia de contexto, liderazgo, planificación, soporte, operación, evaluación del desempeño, auditoría, revisión por dirección y mejora continua.

La referencia a ISO/IEC 42001 no desplaza el enfoque jurídico del documento. Lo refuerza. GIAJ 2.0 toma esa lógica organizacional y la adapta al ecosistema jurídico argentino, donde la gobernanza de IA debe integrarse además con trazabilidad probatoria, secreto profesional, deber de revisión humana, control de datos personales, defensa futura del proceso y responsabilidad profesional indelegable.