MW Working Papers

N° 02 · Junio 2026

Uso seguro de Inteligencia Artificial en un estudio jurídico

Marco de gobernanza, anonimización y trazabilidad implementado en Martínez & Wehbe & Asociados

Por

Dr. Justiniano Martínez

CEO

Dr. Fernando Lascano

Socio · Área Empresas

Dra. Mercedes Gómez Chapman

Directora · Área Laboral

MARTÍNEZ & WEHBE & ASOCIADOS

Estudio Jurídico · Fundado en 2014

martinezwehbe.com · Córdoba, Argentina

Resumen

Este documento describe el marco de gobernanza, anonimización y trazabilidad implementado por Martínez & Wehbe & Asociados para el uso de Inteligencia Artificial generativa en operaciones jurídicas. Abarca dieciocho agentes IA en producción, integrados con cinco proveedores externos y conectados al sistema interno del estudio que administra los expedientes y la base de clientes.

El marco se construye sobre tres capas independientes: (i) una capa jurídica que adapta el marco normativo argentino (Ley 25.326, Resolución AAIP 161/2023, Código de Ética del Colegio de Abogados de Córdoba, Ley 5805, Artículo 156 del Código Penal, Código Civil y Comercial, Ley 11.723) al contexto operativo del estudio; (ii) una capa de gobernanza con roles definidos, política de revisión cuatrimestral, régimen sancionatorio interno y matriz de mínimo acceso para los agentes; y (iii) una capa técnica que implementa anonimización local de datos personales antes de cualquier llamada a proveedor externo, audit log estructurado de las llamadas, política de retención de registros y guardas defensivas contra activaciones accidentales.

El paper también documenta los riesgos abiertos que el estudio reconoce y el plan de mitigación trimestral en curso. Se publica con doble propósito: rendir cuentas a los clientes y servir de referencia para la comunidad jurídica argentina que enfrenta los mismos desafíos.

Sección

Introducción

Por qué este paper

La irrupción de la inteligencia artificial generativa en la práctica profesional jurídica ha sido vertiginosa. En menos de tres años, los grandes modelos de lenguaje han pasado de ser una curiosidad técnica a una herramienta cotidiana en los estudios de abogados de todo el mundo. La velocidad de adopción ha superado, sin embargo, la velocidad con la que la profesión ha reflexionado sobre las consecuencias jurídicas, deontológicas y operativas de esa adopción.

Martínez & Wehbe & Asociados ha decidido construir una infraestructura propia de agentes IA para su operación interna. Esa decisión, tomada en 2026, conllevó la responsabilidad de pensar formalmente cómo proteger la información de los clientes, el secreto profesional y los datos personales que el estudio administra desde su fundación en 2014. Este paper documenta el marco implementado.

A quién va dirigido

Este documento se dirige a tres audiencias diferenciadas, con propósitos distintos en cada caso:

- **A los clientes y prospectos del estudio**: como rendición de cuentas formal del tratamiento que damos a su información. La confianza profesional exige transparencia sobre cómo se procesan los datos confidenciales que cada cliente nos entrega.
- **Al Colegio de Abogados de Córdoba y a la comunidad jurídica argentina**: como contribución a la doctrina deontológica naciente sobre el uso de IA en abogacía. Otros estudios enfrentan los mismos dilemas; compartir el marco propio acelera la convergencia hacia estándares profesionales sólidos.
- **A la Agencia de Acceso a la Información Pública y demás autoridades regulatorias**: como referencia documental del cumplimiento del régimen argentino de protección de datos personales en una organización profesional regulada.

Qué cubre y qué no cubre

Este paper cubre la arquitectura de agentes IA en producción al cierre de junio de 2026, el marco de gobernanza vigente, las medidas técnicas y organizativas implementadas, y los riesgos abiertos que el estudio ha identificado y planea cerrar. No cubre los contenidos sustantivos de los asuntos profesionales del estudio, ni datos identificables de clientes individuales. Tampoco constituye dictamen jurídico sobre el régimen general de protección de datos en Argentina, materia sobre la cual existe literatura especializada extensa.

Estructura

El paper se organiza en doce secciones. La sección 2 reseña el marco normativo argentino aplicable. La sección 3 describe la arquitectura de los dieciocho agentes IA. Las secciones 4 a 8 desarrollan las medidas implementadas en cada una de las tres capas (jurídica, gobernanza, técnica). La sección 9 ilustra un caso de uso real anonimizado. La sección 10 documenta los riesgos abiertos. La sección 11 describe el régimen de auditoría y revisión continua. La sección 12 cierra con una invitación al diálogo.

Sección

Marco normativo aplicable

El uso de inteligencia artificial en un estudio jurídico argentino activa simultáneamente varios cuerpos normativos. Algunos son específicos del tratamiento de datos personales; otros son específicos de la profesión de abogado; otros son disposiciones generales del Código Civil y Comercial o del Código Penal. La conjunción es densa y no admite un cumplimiento parcial.

Régimen de protección de datos personales

Ley 25.326 (Protección de Datos Personales). Norma general que define el régimen de tratamiento, las obligaciones del responsable, los derechos del titular y el régimen sancionatorio. Los datos de clientes de un estudio jurídico encuadran en la definición de «datos personales» del Art. 2. En ciertos casos (situación patrimonial, familia, salud en accidentes de trabajo) encuadran también en la categoría de «datos sensibles» del Art. 7, con un estándar de protección más alto.

Resolución AAIP 161/2023 (Recomendaciones para el uso de Inteligencia Artificial). Documento de soft law emitido por la Agencia de Acceso a la Información Pública que establece principios de transparencia algorítmica, evaluación de impacto en protección de datos (DPIA), y mecanismos de explicabilidad para sistemas de IA que procesan datos personales.

Resolución AAIP 126/2024 (Régimen Sancionatorio). Vigente desde junio de 2024. Clasifica las infracciones en leves, graves y muy graves, con multas escalonadas y posibilidad de clausura. Es la norma que materializa el costo económico del incumplimiento.

Disposición AAIP 60/2016 (Transferencia Internacional de Datos). Regula el traslado de datos personales a países que no han sido declarados con nivel adecuado de protección. Estados Unidos no integra esa lista, lo cual impacta directamente sobre el uso de proveedores de IA con servidores en territorio norteamericano (Anthropic, OpenAI, Google, ElevenLabs).

Régimen local de gobernanza algorítmica en el ámbito judicial provincial

Acuerdo Reglamentario N.° 1939, Serie «A», del Tribunal Superior de Justicia de Córdoba (14 de mayo de 2026). Es el primer marco normativo formal de gobernanza algorítmica del Poder Judicial provincial. Regula el sistema Jurisemia —sistema oficial de jurisprudencia con asistencia de inteligencia artificial— y establece ocho principios rectores aplicables al uso de IA en la administración de justicia provincial: legalidad; finalidad y proporcionalidad; protección reforzada de categorías especiales de datos personales; supervisión humana efectiva sobre todos los procesos asistidos por IA; progresividad y gradualidad; rendición de cuentas y trazabilidad; proporcionalidad entre transparencia y protección de derechos; equidad en el acceso.

Define además un mecanismo de control escalonado por roles —ninguna salida del sistema se publica sin dos instancias humanas de revisión—, exige soberanía técnica plena (servidores propios del Poder Judicial provincial, no terceros), y prevé validación externa por colegios profesionales. Aunque la norma no es aplicable directamente al sector privado, fija el estándar local de «lo que se espera» en materia de IA jurídica cordobesa y constituye una referencia obligada para cualquier estudio que opere en la provincia. La Sección 11 desarrolla el cruce concreto entre el régimen del Estudio y el régimen del Tribunal Superior.

Régimen profesional del abogado

Ley 5805 de la Provincia de Córdoba (Ejercicio de la Profesión de Abogado y Colegiación Obligatoria). El Artículo 19 inciso 7 establece el deber de secreto profesional como obligación legal del abogado. No es disponible unilateralmente: requiere consentimiento del cliente o autorización judicial expresa para su levantamiento.

Código de Ética del Colegio de Abogados de Córdoba. Desarrolla el alcance del deber de reserva profesional. Establece la responsabilidad del abogado por la conducta profesional propia y por la de los colaboradores y dependientes que actúan en su nombre.

Guía CPACF para el uso de Inteligencia Artificial en abogacía (2025). Documento orientativo del Colegio Público de Abogados de la Capital Federal que recomienda informar al cliente cuando el abogado utiliza herramientas de IA, mantener supervisión humana sobre decisiones jurídicas relevantes y verificar la información generada por sistemas automatizados antes de incorporarla a un dictamen.

Disposiciones generales del Código Penal y Civil

Artículo 156 del Código Penal. Tipifica la violación de secretos profesionales con pena de hasta dos años de prisión e inhabilitación profesional especial. Es el corolario penal del deber de reserva. Se activa cuando el secreto se revela «sin justa causa» a un tercero —incluido, potencialmente, un proveedor extranjero de servicios de IA al que se envíen datos cubiertos por el secreto sin contar con un acuerdo contractual que asegure equivalente protección.

Artículo 53 del Código Civil y Comercial de la Nación. Reconoce a la voz como atributo de la personalidad, sujeto a protección equivalente a la imagen y al honor. Aplicable a la práctica de clonación de voz (voice cloning), tecnología que el estudio utiliza para algunas comunicaciones internas y cuyo régimen específico se aborda en secciones posteriores.

Artículo 902 del Código Civil y Comercial. Establece que la mayor previsibilidad de las consecuencias exige mayor diligencia. Aplicado a un estudio jurídico que implementa IA: el grado de previsión exigible es superior al de un particular que utiliza las mismas herramientas, porque la aptitud técnica y profesional del estudio es superior.

Ley 11.723 (Régimen Legal de la Propiedad Intelectual). Aplicable a dos cuestiones distintas: (i) la titularidad de los outputs generados por IA (dictámenes, contratos, comunicaciones), materia doctrinariamente abierta porque la ley exige autoría humana para reconocer derechos de autor; y (ii) la clonación de voz sin consentimiento del titular, encuadrable en el Art. 71 con sanciones civiles y penales.

Síntesis

Síntesis

Las normas reseñadas no operan en compartimentos estancos: el incumplimiento de la Ley 25.326 puede activar simultáneamente el régimen profesional (porque hay datos cubiertos por secreto) y el penal (porque la revelación a un tercero sin justa causa configura el tipo del Art. 156). Esta conjunción es la que justifica el grado de detalle del marco que describimos en las secciones siguientes.

SECCIÓN

Arquitectura de agentes IA del estudio

Inventario general

Al cierre de junio de 2026, Martínez & Wehbe opera dieciocho agentes IA en distintos roles de la operación. La arquitectura es modular: cada agente tiene un alcance funcional definido, un canal de salida específico y un conjunto delimitado de fuentes de datos a las que puede acceder. La modularidad permite aplicar la matriz de mínimo acceso (que se describe en la sección 8) sin sacrificar la capacidad operativa.

Categoría	Función	Cantidad
Orquestadores	Coordinación de tareas, dirección de los demás agentes, atención a empleados del estudio y a clientes externos por canales digitales.	3
Comerciales	Análisis del pipeline comercial, enriquecimiento de prospectos, generación de propuestas, gestión del CRM.	2
Operativos	Operaciones internas, kanban del equipo, monitoreo de actividades, finanzas y tesorería.	3
Contenido y marketing	Pipeline editorial del estudio, publicación en redes sociales, generación de imágenes.	2
Compliance	Revisión de contenidos antes de publicación, verificación de cumplimiento de copys.	1
Investigación	Búsqueda en fuentes públicas, recopilación de información, síntesis de jurisprudencia.	1
Técnicos	Codificación, code review, auditorías de seguridad técnica, orquestación paralela de sprints.	5
Personales	Asistencia personal al CEO, coaching y soporte de decisiones estratégicas.	1

Proveedores externos integrados

Los dieciocho agentes utilizan cinco proveedores externos de inteligencia artificial, cada uno con un propósito específico:

Proveedor	Servicio utilizado	Tipo de payload

Anthropic	Modelos generativos (familia Claude) para procesamiento de lenguaje, generación de texto, análisis de documentos.	Texto.
OpenAI	Transcripción de audio (Whisper, configurable). Generación de embeddings para memoria semántica.	Audio y texto, opt-in.
Google	Generación de imágenes para piezas gráficas (Gemini Flash Image).	Prompts visuales en inglés, sin datos personales.
ElevenLabs	Síntesis de voz para respuestas auditivas (text-to-speech).	Texto a sintetizar.
Firecrawl	Búsqueda y extracción en fuentes públicas (SAIJ, InfoLEG, Boletín Oficial).	Consultas legales públicas.

Sistemas internos conectados

Adicionalmente, los agentes están conectados al sistema interno del estudio (Sistema MW, alojado en infraestructura propia con base de datos Supabase) que administra el CRM, los expedientes y la base de clientes; y a herramientas operativas (Google Workspace, WhatsApp Business, repositorio de código).

> **Volumen de datos en juego**. Al cierre de junio de 2026, el Estudio acumula doce años de operación profesional desde su fundación en 2014. El sistema MW administra registros de aproximadamente 4.169 clientes históricos, 230 prospectos activos en el CRM y un volumen acumulado de actividades, comunicaciones y documentos que se cuenta en cientos de miles. La protección de ese volumen es el objeto del marco que describimos a continuación.

SECCIÓN

Las tres capas de protección

El marco implementado en Martínez & Wehbe se construye sobre tres capas independientes que protegen los datos por mecanismos distintos. Las capas son redundantes por diseño: si una falla, las otras dos cubren. Esta sección describe la lógica del esquema completo; las secciones siguientes profundizan cada capa.

Figura 1. *Esquema de las tres capas de protección. Cada capa opera de forma independiente; la falla de una no compromete a las otras.*

Capa 1 — Jurídica

La capa jurídica es el marco normativo interno del estudio. Está construida sobre tres políticas maestras escritas y revisadas internamente por los socios:

- **Política de Gobernanza de IA**. Establece los principios rectores del uso de IA en el estudio, define roles (CAIO, DPO, Socio Responsable), describe el proceso de toma de decisiones sobre incorporación de nuevos agentes o proveedores, fija el régimen de revisión periódica y enumera el régimen sancionatorio interno por incumplimiento.
- **Política de Datos Personales y Confidencialidad**. Quince capítulos, sesenta y un artículos. Adapta el marco de Ley 25.326 al contexto operativo del estudio; clasifica los datos en cuatro niveles; define el régimen de tratamiento por categoría; establece la política de retención de logs; describe el procedimiento de incidentes con notificación a la AAIP en setenta y dos horas; y formula la cláusula tipo a incorporar al contrato de honorarios.

- **Política de Uso de Proveedores IA Externos**. Lista blanca de proveedores autorizados; requisitos contractuales mínimos por proveedor (DPA, SCC, ZDR); payload permitido por proveedor en función del régimen contractual; técnicas de anonimización requeridas para cada flujo; y guardas (switch flags) que bloquean activaciones accidentales.

> Las tres políticas fueron redactadas internamente por el equipo del estudio, revisadas por los socios y firmadas por el CEO. La decisión de no contratar consultoría externa fue deliberada y se fundamenta en que Martínez & Wehbe ES un estudio jurídico: la capacidad técnico-jurídica existía internamente.

Capa 2 — Gobernanza

La capa de gobernanza traduce las políticas a estructura organizativa concreta. Tres roles formales asumen la responsabilidad del cumplimiento:

- **Chief AI Officer (CAIO)**. Designado en cabeza del CEO de manera provisional, con previsión de descentralización a un socio específico cuando la complejidad lo requiera. Coordina la operación del marco, decide sobre incorporación de nuevos agentes y nuevos proveedores, firma las decisiones de gobierno.
- **Data Protection Officer interno (DPO)**. Designado en cabeza de un socio del Área Empresas. Atiende los derechos de titulares de datos personales, gestiona la relación con la AAIP, supervisa el cumplimiento de la política de datos.
- **Socio Responsable por cuenta**. Cada cliente tiene asignado un socio del estudio que responde por el cumplimiento del marco en relación con esa cuenta específica.

Adicionalmente, la capa de gobernanza incluye un régimen de revisión cuatrimestral en el que el Comité de Gobernanza IA (los tres roles más una representación del equipo profesional) examina los incidentes del trimestre, evalúa la pertinencia de incorporar nuevos agentes o proveedores, revisa la matriz de riesgos y actualiza las políticas cuando corresponde.

Capa 3 — Técnica

La capa técnica es la que materializa las dos anteriores en código y configuración. Incluye:

- **Anonimización local de datos personales antes de cualquier llamada a proveedor externo**. Es el principio rector del marco. Se desarrolla en detalle en la sección siguiente.
- **Audit log estructurado de las llamadas externas**. Cada vez que un agente llama a un proveedor IA, se registra metadata (proveedor, archivo origen, tamaño del payload, presencia de PII detectada) sin almacenar el contenido. Esto habilita auditorías posteriores sin comprometer los datos originales.

- **Política de retención de registros**. Todos los registros operativos —conversaciones, logs de actividad, traces de observabilidad— tienen un período de retención definido. Pasado ese período, los archivos se eliminan automáticamente por proceso programado.
- **Permisos NTFS reforzados** sobre los directorios sensibles del filesystem; los archivos `.env` con credenciales están en `.gitignore`; existen guardas defensivas en código (kill-switches) que bloquean activaciones accidentales de funciones de riesgo elevado.
- **Audit de operaciones en base de datos**. Toda lectura y escritura sobre tablas sensibles de la base de datos del estudio (clientes, prospectos, asuntos, facturas) queda registrada en una tabla de auditoría con el identificador del agente que la realizó, la cantidad de filas afectadas y el filtro aplicado.

SECCIÓN

Anonimización local: el principio rector

> **Regla firme del estudio**. La detección y redacción de datos personales tiene que ocurrir cien por ciento local. Nunca se utiliza un modelo de lenguaje externo (Anthropic, OpenAI, Google, ElevenLabs u otros) para «anonimizar» datos antes de mandarlos al mismo proveedor.

Por qué la regla

Hacer una llamada a un modelo externo para detectar datos personales en un texto que después se va a procesar con el mismo proveedor es lógicamente contradictorio. Los datos crudos viajan al proveedor durante el paso de detección. Nada cambia respecto del riesgo: si el dato cubierto por secreto profesional sale del estudio, la posibilidad de configurar el tipo del Art. 156 del Código Penal se mantiene idéntica.

El mismo razonamiento aplica a cualquier proveedor externo: si la detección requiere que el texto crudo salga del estudio, el riesgo legal queda igual. La anonimización tiene que ser local por construcción, no por contrato.

Arquitectura — Tres capas de anonimización

La detección de datos personales se ejecuta en tres capas, ordenadas de menor a mayor costo computacional. Las capas son acumulativas: el texto pasa por todas las que estén habilitadas, en orden.

Capa 1 · Expresiones regulares deterministas

1 Patrones precisos para mails, teléfonos argentinos, JID de WhatsApp, CUIT y CUIL, DNI con palabra clave de contexto, números de expediente, carátulas, blocklist de nombres del equipo. ≈ 0 ms

Capa 2 · Reconocimiento de entidades (NER) en español

2 Modelo de lenguaje pequeño (spaCy modelo en español pequeño) corriendo local en la máquina del estudio. Detecta nombres propios de clientes, organizaciones y lugares que las regex no capturan. ≈ 6 ms

Capa 3 · Modelo de lenguaje local (Ollama, opcional)

3 Llama 3.2 o Qwen 2.5 corriendo local para casos ambiguos que las dos capas anteriores no resuelven. Cero datos van afuera. Pendiente de evaluación en el tercer trimestre de 2026. ≈ 1 s

Figura 2. *Pila de anonimización local. La cobertura combinada de las dos primeras capas se estima en torno al noventa por ciento para texto jurídico argentino estándar.*

Implementación

Las dos primeras capas están implementadas y operando en producción. El módulo de filtrado de PII aplica las expresiones regulares en menos de un milisegundo por texto. El módulo NER corre como subproceso Python persistente (lanzado una vez por sesión, mantiene el modelo en memoria, recibe peticiones por canal de entrada estándar). La latencia agregada por la pila completa es del orden de seis milisegundos por texto en estado estacionario.

Cobertura medida

Treinta y dos casos de prueba para Capa 1 (regex), doce casos adicionales para Capa 2 (NER). En todos ellos, el texto crudo no sobrevive sin redactar. Cuando un dato es detectado por las dos capas (caso de un nombre propio que también satisface una regex), se prefiere la sobre-redacción a la sub-redacción.

Caso negativo — Qué no permite la regla

La regla excluye explícitamente:

- Usar un modelo externo (Anthropic, OpenAI, Google) para «detectar» PII en texto crudo.
- Usar un modelo externo para «redactar» PII en texto crudo.
- Enviar transcripciones de reuniones con clientes a un modelo externo «para que extraiga pain points y después nos diga qué nombres redactar».

> **Excepciones autorizadas**. Una sola, documentada y firmada por el CEO y el DPO. Cuando el estudio cuente con contrato Enterprise + DPA firmado con el proveedor externo, y el cliente cuyos datos se procesan haya prestado consentimiento informado explícito (cláusula del contrato de honorarios), está permitido enviar datos identificables al proveedor para servicios distintos de «anonimización».

SECCIÓN

Trazabilidad y auditoría operativa

Audit log de llamadas externas

Cada llamada a un proveedor externo desde cualquier agente queda registrada en un archivo de log estructurado. El registro contiene metadata operativa pero no contenido. Un ejemplo:

```
{
  "ts": "2026-06-13T19:40:12.345Z",
  "provider": "anthropic",
  "endpoint": "messages.create",
  "caller": "src/wa-group-classifier.ts",
  "model": "claude-haiku-4-5",
  "payload_bytes": 312,
  "has_pii": false,
  "status_code": 200,
  "error": null
}
```

Figura 3. *Ejemplo de entrada del audit log. Solo metadata operativa; el contenido del prompt y de la respuesta no se almacena.*

El campo **has_pii** es la salida del módulo de detección de la sección anterior. Una entrada con **has_pii: true** no significa que se haya enviado información identificable al proveedor: significa que se detectó PII en el texto antes de procesarlo. Si la política aplicable requiere anonimización, el texto que llega al proveedor fue redactado antes. La distinción es central: el audit log permite verificar a posteriori que el principio rector se aplicó correctamente.

Audit de operaciones en base de datos

Toda operación de lectura o escritura sobre tablas marcadas como sensibles (clientes, prospectos del CRM, asuntos, actividades, facturas, pagos, comisiones, liquidaciones) queda registrada en la tabla `erp_audit_log` con cuatro campos clave:

Campo	Significado
agent_id	Identificador del agente que originó la operación.
operacion_tipo	SELECT, INSERT, UPDATE o DELETE.
filtros_aplicados	Cláusula WHERE de la consulta, sin valores específicos.
rows_returned	Cantidad de filas afectadas. Útil para detectar consultas anómalamente amplias.

Esto permite reconstruir, ante cualquier disputa o investigación, qué agente consultó qué información y cuándo. Es la base material de la rendición de cuentas.

Observabilidad de calls al SDK

Adicionalmente, el sistema de observabilidad (Arize Phoenix corriendo en contenedor local) captura traces de todas las llamadas al SDK de IA. La configuración aplicada para esta instalación oculta los inputs y outputs completos —solo se ven el nombre del modelo, los tokens, la latencia y los errores—. De ese modo, los traces de Phoenix nunca contienen el contenido sensible del prompt ni de la respuesta, sino solo la metadata necesaria para diagnosticar problemas de rendimiento.

Retención de los logs

Los archivos de log tienen un período de retención definido por política:

- **Conversaciones de agentes**: treinta días para conversaciones operativas. Noventa días para conversaciones con contexto jurídico relevante.
- **Audit log de calls externas**: trescientos sesenta y cinco días. Pasado ese plazo, archivo comprimido para retención prolongada.
- **Audit de base de datos**: retención según política de Supabase Auth (siete años, alineado al deber profesional de conservación de antecedentes).
- **Traces de Phoenix**: treinta días.

La rotación se ejecuta por procesos automatizados diarios. La eliminación es definitiva y el procedimiento queda registrado a su vez en un log de rotación, para evidenciar a posteriori que la política se aplicó.

SECCIÓN

Datos personales y secreto profesional

Clasificación en cuatro niveles

La Política de Datos Personales del estudio clasifica toda la información tratada en cuatro niveles, ordenados de menor a mayor sensibilidad. Cada nivel tiene un régimen de tratamiento diferenciado:

Figura 4. *Pirámide de clasificación de datos. El régimen del Nivel 4 es el más estricto y se aborda separadamente del régimen general de Ley 25.326.*

Régimen por nivel

Nivel	Régimen aplicable
N1 Público	Sin restricción. Puede enviarse a cualquier proveedor sin anonimización.
N2 Interno	No divulgable a terceros sin autorización. Puede enviarse a proveedores con cláusula contractual de confidencialidad.
N3 Confidencial	Anonimización obligatoria antes de transferencia internacional. Requiere consentimiento del titular según el caso. Retención limitada al plazo necesario para la finalidad declarada.

N4 Secreto profesional	Prohibido enviar a proveedor IA sin contrato Enterprise + Data Processing Agreement + Zero Data Retention + anonimización + consentimiento explícito del cliente.

Transferencia internacional

Los proveedores externos integrados (Anthropic, OpenAI, Google, ElevenLabs, Firecrawl) tienen su infraestructura primaria en Estados Unidos. Estados Unidos no integra la lista de países declarados por la Argentina con nivel adecuado de protección de datos (Disposición AAIP 60/2016 y actualizaciones).

La consecuencia operativa es directa: para que datos personales argentinos puedan procesarse legalmente en infraestructura norteamericana, se requiere alguna de las siguientes bases legales:

- Consentimiento informado expreso y escrito del titular para la transferencia.
- Cláusulas contractuales modelo que aseguren equivalente protección.
- Contrato específico (DPA) con garantías documentadas de cumplimiento.

En la práctica, esto se traduce en el principio que rige la Capa Técnica: **anonimizar antes de enviar**. Los datos que efectivamente salen del estudio están redactados; los placeholders (`<NOMBRE>`, `<EMAIL>`, `<CUIT>`, `<EXPTE>`, `<NOMBRE>`, `<ORG>`, `<LUGAR>`) reemplazan al dato real. La cláusula contractual del estudio con el cliente complementa con consentimiento informado.

Datos sensibles del Art. 7 Ley 25.326

Cuando los datos tratados encuadran en la categoría de «datos sensibles» del Artículo 7 (situación patrimonial, situación familiar, datos de salud, ideología, religión), el estándar de consentimiento es más estricto: debe ser libre, expreso, escrito y específico para esa finalidad. El estudio mantiene un agente con función estrictamente personal (coaching del CEO) cuyo régimen documental se aborda con tratamiento especial porque la conversación incluye categorías de datos sensibles del propio CEO.

Sección

Disclosure al cliente y consentimiento informado

El deber de informar

Las directrices del CPACF para uso de Inteligencia Artificial en abogacía (2025) establecen que el abogado debe informar al cliente si utiliza herramientas de IA. La Resolución AAIP 161/2023 desarrolla el principio de transparencia algorítmica. Ambas convergen en una conclusión simple: el cliente tiene derecho a saber cuándo y cómo la IA participa en la prestación del servicio que contrata.

Implementación en Martínez & Wehbe

El estudio implementa tres mecanismos complementarios de disclosure:

- **Identificación al primer contacto externo**. Cuando un agente IA establece contacto con una persona externa al estudio (típicamente, vía WhatsApp), se identifica al primer mensaje como «asistente digital del Estudio Martínez & Wehbe & Asociados», no como abogado del estudio. Si la persona requiere asesoramiento, se la deriva a un correo institucional del estudio donde un profesional humano la atiende.
- **Nota al pie en documentos**. Todo documento generado con asistencia de IA y entregado al cliente lleva una nota al pie que aclara la naturaleza del proceso. La revisión profesional humana del documento queda explicitada y firmada.
- **Cláusula en el contrato de honorarios**. El template de contrato de honorarios del estudio incluye una cláusula específica que informa al cliente del uso de herramientas de IA en la operación del estudio, identifica los proveedores externos involucrados, declara las medidas de protección implementadas y solicita el consentimiento informado del cliente para el tratamiento.

Cláusula tipo

A continuación se reproduce el texto literal de la cláusula que se incorpora a los nuevos contratos de honorarios. Para los clientes preexistentes a su entrada en vigor, el estudio publica una nota de regularización del backlog con plazo de oposición de treinta días.

> *El Estudio utiliza herramientas de inteligencia artificial generativa para asistir en la operación profesional. Estas herramientas operan bajo un marco interno de gobernanza, anonimización y trazabilidad que el Estudio mantiene actualizado y disponible para consulta del cliente. Los datos personales del cliente que requieran tratamiento por estos sistemas son anonimizados localmente antes de cualquier transferencia a proveedores externos, salvo que medie consentimiento informado*

expreso para la transferencia identificable o que la operación se realice bajo un contrato Enterprise con garantías equivalentes. El cliente puede solicitar en cualquier momento información sobre el régimen de tratamiento aplicable a sus datos, así como ejercer los derechos de acceso, rectificación y supresión previstos por la Ley 25.326. El Estudio asume el deber de informar al cliente cualquier incidente de seguridad que pueda afectar sus datos personales conforme al procedimiento previsto por la Resolución AAIP 126/2024.

— Cláusula incorporada al contrato de honorarios MW (2026)

Sección

Caso de uso anonimizado

Para ilustrar cómo opera el marco en la práctica, esta sección describe el flujo completo de un mensaje recibido por WhatsApp por uno de los agentes orquestadores. Los datos están anonimizados.

Escenario

Un cliente del estudio envía un mensaje a la cuenta de WhatsApp institucional con la siguiente consulta: «Hola, ¿cómo está? Tengo una duda sobre el expediente número 4523/2024 que tienen ustedes. Necesito saber si hay novedad de la audiencia.»

Flujo paso a paso

Paso 1 — Recepción. El daemon de WhatsApp recibe el mensaje a través del puente local. El mensaje se persiste en un archivo de log diario con permisos NTFS restringidos al usuario del sistema, fuera del repositorio de código.

Paso 2 — Pre-clasificación. Un agente clasificador (modelo de bajo costo) determina si el mensaje proviene del equipo del estudio, de un cliente conocido o de un externo. El criterio se aplica sobre el JID del remitente, no sobre el contenido. La decisión se loguea en el audit trail con `has_pii: false` porque solo se procesó el identificador del canal.

Paso 3 — Anonimización local. Antes de cualquier llamada al modelo generativo, el texto del mensaje pasa por la pila de tres capas. La regex captura el número de expediente. El NER detecta el nombre propio si lo hubiera. El texto que llega al siguiente paso es: «Hola, ¿cómo está? Tengo una duda sobre el expediente `<EXPTE>` que tienen ustedes. Necesito saber si hay novedad de la audiencia.»

Paso 4 — Procesamiento. El agente orquestador determina que la consulta requiere intervención humana. No accede a la base de datos para responder qué dice el expediente; redacta una respuesta institucional derivando al correo del estudio.

Paso 5 — Respuesta. El agente responde: «Hola, soy el asistente digital del Estudio Martínez & Wehbe. Por consultas sobre su expediente le pido que escriba a contacto@martinezwehbe.com indicando su nombre completo y su número de expediente; un profesional del estudio le atenderá.»

Paso 6 — Auditoría. La operación queda registrada en cuatro lugares simultáneamente: el log de conversaciones (retención 30 días), el audit trail de calls externas (retención 365 días, sin contenido), el audit de base de datos (no aplica porque no se consultó la BD), y los traces de Phoenix (sin contenido por configuración).

Nótese que en ningún paso del flujo el número de expediente real, el nombre del cliente real, ni el contenido sustantivo del asunto sale del entorno local del estudio. Lo que se procesa con el modelo generativo externo es texto redactado; lo que se persiste localmente está protegido por NTFS y por la política de retención.

Sección

Riesgos abiertos y plan de cierre

Posición del estudio frente al riesgo

Ningún marco de protección es perfecto el día de su entrada en vigor. La autenticidad del marco se mide por la capacidad de identificar abiertamente sus puntos débiles y comprometerse al cierre con plazos concretos. A continuación reseñamos los riesgos abiertos al cierre de junio de 2026, con el plan de mitigación correspondiente.

Riesgos en proceso de cierre

Riesgo identificado	Plan de mitigación en curso	Plazo
Configuración contractual con el proveedor principal de modelos generativos requiere upgrade a contrato Enterprise con DPA específico.	Decisión en curso entre tres alternativas (upgrade total, mantenimiento de plan actual con anonimización exhaustiva, esquema mixto por flujos).	3er trimestre 2026.
Verificación documental del régimen contractual de la tecnología de síntesis de voz utilizada en respuestas auditivas internas.	Verificación pendiente del origen del voice ID en el panel del proveedor.	3er trimestre 2026.
Inscripción del estudio como Responsable de Bases de Datos Personales ante el Registro Nacional de la AAIP, conforme al Art. 21 Ley 25.326.	Dossier técnico preparado. Inscripción en sede TAD en curso.	Junio 2026.
Evaluación de Impacto en Protección de Datos (DPIA) formal sobre los flujos de mayor riesgo, conforme Resolución AAIP 161/2023.	Programada con autoría compartida de los socios y el área de gobernanza interna.	3er trimestre 2026.
Pipeline de anonimización integrado al cien por cien-	Capas 1 y 2 implementadas (treinta y dos casos cu-	4to trimestre 2026.

to de los flujos identificados.	biertos por regex, doce casos adicionales por NER). Capa 3 (LLM local) pendiente de evaluación.	
Soberanía técnica del procesamiento: tratamiento en servidores bajo jurisdicción argentina o latinoamericana, en línea con el estándar fijado por el TSJ Córdoba para su sistema Jurisemia (Acuerdo Reglamentario 1939/2026).	Evaluación de proveedores con infraestructura en jurisdicciones de protección equivalente. En el corto plazo, la anonimización local antes de la transferencia opera como mitigación funcional. En el mediano plazo, evaluación de modelos open source corriendo on-premise para los flujos de mayor sensibilidad.	4to trimestre 2026 - 2027.
Validación externa del presente marco por la Comisión de Tecnología del Colegio de Abogados de Córdoba.	Presentación del whitepaper y solicitud de revisión externa, en línea con la práctica seguida por el TSJ Córdoba al validar Jurisemia con el Colegio de Abogados y la FECACOR.	3er trimestre 2026.

Riesgos que el estudio considera cubiertos al cierre de junio de 2026

- Detección de credenciales hardcodeadas en código histórico (cuatro credenciales identificadas, rotadas en paneles, removidas del working tree).
- Configuración del sistema de observabilidad sin exposición de payload sensible.
- Audit log centralizado de llamadas externas a APIs IA.
- Audit trail de operaciones SELECT en base de datos de producción.
- Política de retención de conversaciones de agentes (treinta días, NTFS).
- Filtro de PII en el proceso de consolidación nocturna de memoria.
- Guardas contra activaciones accidentales de transcripción cloud.

Compromiso de actualización

El presente paper documenta el estado al cierre de junio de 2026. El Comité de Gobernanza IA actualiza esta lista en cada revisión cuatrimestral. Los riesgos cerrados en cada trimestre se publican en el sitio institucional del estudio.

Sección

Cruce con el régimen del Tribunal Superior de Justicia de Córdoba

Por qué este cruce importa

El 14 de mayo de 2026, el Tribunal Superior de Justicia de Córdoba aprobó el Acuerdo Reglamentario N.° 1939, Serie «A», que regula formalmente la gobernanza algorítmica del sistema Jurisemia. Es el primer marco normativo provincial específico sobre uso de inteligencia artificial en el ámbito judicial. Aunque su alcance jurídico se limita a las dependencias del Poder Judicial provincial, define el estándar regulatorio local de referencia: la altura de exigencia que un Tribunal Superior considera adecuada en su propia operación con IA.

Para un estudio jurídico cordobés que adopta IA en operaciones internas, ese estándar es ineludible. No por aplicación directa, sino porque cualquier lector calificado —Colegio de Abogados, AAIP, contrapartes técnicas— va a comparar el marco del estudio contra el del Tribunal. Esta sección hace ese cruce explícitamente: dónde estamos alineados, dónde reforzamos a partir del nuevo estándar y dónde el régimen del Estudio se diferencia abiertamente del régimen judicial, con la justificación correspondiente.

Cuadro comparativo

Principio o requisito del AR 1939	Régimen de Martínez & Wehbe	Estado
Supervisión humana efectiva. La decisión final sobre publicación, clasificación o anonimización no puede ser adoptada de manera exclusivamente automatizada (Considerando VII y Art. 5).	El régimen del Estudio asume el mismo principio. Todo output entregado al cliente lleva revisión y firma humana. Los agentes IA no pueden emitir dictamen ni instrumento profesional sin paso humano de aprobación.	**Alineado**
Control escalonado por roles. Mínimo dos instancias de revisión humana antes de cualquier publicación (gestor de carga y supervisor, Art. 5).	Cubierto parcialmente para outputs públicos (revisión por agente Compliance + revisión humana por socio responsable). Se formaliza en el régimen interno como requisito explícito de dos pasos	**Refuerzo**

	antes del envío a cliente o publicación externa.	
Trazabilidad completa de todas las acciones sobre cada documento, instrumentada operativamente por una plataforma con registro auditable (Art. 5 y plataforma Nexo).	Audit log centralizado de calls externas y audit trail de operaciones sobre la base de datos están implementados. La trazabilidad documento por documento (cada dictamen, contrato o comunicación profesional) se incorpora como criterio operativo y se documenta en el sistema interno del estudio.	**Refuerzo**
Anonimización de datos personales antes del procesamiento, con protección reforzada para categorías especiales (Art. 2 inc. c y Considerando VIII).	Pila de tres capas locales (regex, NER en español, LLM local opcional). El secreto profesional opera además como cuarto nivel de la clasificación interna, con régimen propio. La cobertura combinada medida es del orden del noventa por ciento.	**Alineado**
Soberanía técnica del procesamiento. Almacenamiento y procesamiento exclusivamente en servidores bajo control del Poder Judicial; participación de terceros sólo con autorización formal (Considerando XI y Art. 9).	No alineado. Los proveedores de modelos generativos del Estudio (Anthropic, OpenAI, Google) operan en infraestructura propia, no del Estudio. La mitigación funcional es la anonimización local antes de la transferencia internacional, complementada con régimen contractual sobre el tratamiento. El cierre completo de esta brecha está identificado como objetivo de mediano plazo (ver Sección 10).	**Diferencia honesta**
Validación externa por colegios profesionales. El sistema fue validado por el Colegio de Abogados de Córdoba y por la FECACOR antes de su consoli-	El Estudio se compromete a presentar este whitepaper a la Comisión de Tecnología del Colegio de Abogados de Córdoba para revisión externa durante el tercer trimes-	**Compromiso**

dación normativa (Considerando VI).	tre de 2026. La validación externa es el cierre natural del proceso interno descrito en este documento.	
Roles institucionales operativos: administrador, supervisor, gestor de carga (Art. 8).	El Estudio define tres roles análogos: CAIO (Chief AI Officer), DPO interno (Responsable de Protección de Datos) y Socio Responsable por cuenta. Adicionalmente, el agente Compliance funciona como filtro automatizado previo a la revisión humana final.	**Alineado**
Capacitación obligatoria y reconocimiento institucional del personal afectado a la operación del sistema (Art. 8 y 11).	El régimen del Estudio prevé revisión cuatrimestral y formación continua del equipo profesional. La inducción específica al equipo sobre el marco interno se documenta como parte del proceso de incorporación de cualquier socio o asociado al área Empresas.	**Alineado**

Lectura del cuadro

De los ocho ejes comparados, el Estudio se encuentra alineado con el estándar del Tribunal Superior en cinco; presenta refuerzos formales en dos ejes (control escalonado y trazabilidad documental, en proceso de formalización); y diferenciación honesta en uno (soberanía técnica). El compromiso de validación externa por el Colegio de Abogados de Córdoba sigue la práctica del propio TSJ con FECACOR.

> **Observación deliberada sobre la diferencia honesta.** El Estudio reconoce abiertamente que la soberanía técnica plena —servidores bajo jurisdicción argentina, infraestructura propia para modelos generativos— no es alcanzable hoy con la oferta tecnológica disponible para una organización profesional del tamaño del Estudio. El compromiso es seguir evaluando el mercado de modelos open source corriendo on-premise y, cuando la madurez técnica lo permita, migrar los flujos de mayor sensibilidad. La anonimización local antes de la transferencia internacional opera mientras tanto como mitigación funcional sustantiva, no meramente formal.

Sección

Auditoría y revisión continua

Régimen de revisión cuatrimestral

El Comité de Gobernanza IA se reúne cada cuatro meses. La reunión sigue una agenda estándar:

1. Revisión de los incidentes operativos del trimestre, agrupados por categoría (acceso indebido, leak de PII, fallo de proveedor, error de clasificación).
2. Evaluación de las solicitudes de incorporación de nuevos agentes o nuevos proveedores externos, con dictamen del DPO sobre el régimen de tratamiento de datos aplicable.
3. Actualización de la matriz de riesgos: cuáles cerraron, cuáles abrieron, cuáles cambiaron de prioridad.
4. Revisión del cumplimiento de la política de retención (auditoría de archivos eliminados).
5. Aprobación de modificaciones a las tres políticas maestras si corresponde.
6. Definición del plan operativo del trimestre siguiente.

Atención de derechos del titular

La Ley 25.326 reconoce a los titulares de datos personales cuatro derechos fundamentales: acceso, rectificación, supresión y oposición. El estudio implementa los siguientes procedimientos:

- **Solicitud de acceso**: el titular envía la solicitud al correo institucional del estudio o al DPO designado. Plazo de respuesta: diez días corridos. Se entrega un informe estructurado de los datos que el estudio mantiene sobre el solicitante.
- **Solicitud de rectificación**: similar procedimiento. Plazo de quince días. Se documenta el cambio en el audit log.
- **Solicitud de supresión**: el estudio analiza si la conservación del dato responde a una obligación legal (por ejemplo, conservación de antecedentes profesionales por siete años) y procede en consecuencia. Si la supresión es viable, se aplica también a los logs operativos y a las copias de respaldo.
- **Solicitud de oposición**: el titular puede oponerse al tratamiento de sus datos para finalidades específicas (típicamente, comunicaciones de marketing). Se aplica y se confirma por escrito.

Procedimiento de incidentes

Ante un incidente de seguridad de datos, el procedimiento es:

1. Identificación y contención inicial (primeras dos horas).

2. Notificación al CAIO y al DPO interno.
3. Análisis del alcance (datos afectados, titulares afectados, gravedad).
4. Notificación a la AAIP dentro de las setenta y dos horas, conforme al régimen reforzado por el DNU 70/2024 y la Resolución AAIP 126/2024.
5. Notificación a los titulares afectados cuando el riesgo lo justifique.
6. Documentación completa del incidente en el registro de incidentes interno.
7. Revisión post-mortem para identificar mejoras al marco.

Sección

Cierre

Una invitación al diálogo

La inteligencia artificial generativa está modificando aceleradamente la práctica jurídica argentina. Los estudios que decidan adoptarla con sofisticación tienen una ventaja competitiva real; los que la adopten con descuido se exponen a una responsabilidad jurídica y profesional considerable. Entre ambas alternativas, el marco que hemos descrito es una respuesta concreta: usar la herramienta, pero con guardas que protegen al cliente y al estudio.

Este paper se publica con la convicción de que la convergencia hacia estándares profesionales sólidos en materia de IA va a llevar tiempo y va a beneficiarse de la conversación entre estudios, del intercambio de experiencias y de la revisión crítica de marcos como el que aquí describimos. Quien encuentre fallas, lagunas o áreas de mejora está invitado a comunicárnoslas; quien quiera adoptar partes del marco para su propio estudio puede hacerlo libremente; quien quiera contratar el desarrollo de un marco análogo para su organización puede contactarnos por los canales habituales.

Compromiso de validación externa

El Estudio asume el compromiso de presentar este whitepaper, durante el tercer trimestre de 2026, a la Comisión de Tecnología del Colegio de Abogados de Córdoba para revisión externa. Esta presentación sigue la práctica institucional adoptada por el Tribunal Superior de Justicia de Córdoba al someter el sistema Jurisemia a la validación previa del Colegio de Abogados de Córdoba y de la Federación de Colegios de Abogados (FECACOR), conforme surge del Acuerdo Reglamentario 1939/2026. La validación externa por los pares profesionales operará como cierre natural del proceso interno descrito en este paper y como base para la primera revisión cuatrimestral del marco.

Contacto

Martínez & Wehbe & Asociados

Estudio Jurídico · Córdoba, Argentina

contacto@martinezwehbe.com

martinezwehbe.com

> Las consultas específicas sobre el marco descrito en este paper, propuestas de revisión, o pedidos de información adicional sobre algún aspecto puntual pueden

> dirigirse al Comité de Gobernanza IA del Estudio a través de las direcciones de contacto institucional.

Sección

Referencias

1. **Ley 25.326** — Protección de los Datos Personales. Honorable Congreso de la Nación Argentina.
2. **Ley 11.723** — Régimen Legal de la Propiedad Intelectual. Honorable Congreso de la Nación Argentina.
3. **Ley 5805** (Provincia de Córdoba) — Ejercicio de la Profesión de Abogado y Colegiación Obligatoria.
4. **Código Penal de la Nación**, Artículo 156 — Violación de Secretos Profesionales.
5. **Código Civil y Comercial de la Nación**, Artículos 53 (derecho a la imagen y la voz) y 902 (mayor diligencia exigible).
6. **Resolución AAIP 161/2023** — Recomendaciones para el uso de Inteligencia Artificial. Agencia de Acceso a la Información Pública.
7. **Resolución AAIP 126/2024** — Régimen Sancionatorio. Agencia de Acceso a la Información Pública.
8. **Disposición AAIP 60/2016** — Transferencia Internacional de Datos.
9. **Disposición DNPDP 2/2005** — Formulario FA.01, estructura del Registro Nacional de Bases de Datos.
10. **Resolución AAIP 132/2018** — Eliminación de la renovación anual de inscripciones.
11. **Guía para el uso de Inteligencia Artificial para Abogados** (2025). Colegio Público de Abogados de la Capital Federal (CPACF).
12. **Código de Ética** del Colegio de Abogados de Córdoba.
13. **Acuerdo Reglamentario N.° 1939, Serie «A»** (14/05/2026). Tribunal Superior de Justicia de la Provincia de Córdoba. Aprobación del sistema Jurisemia y establecimiento del régimen institucional aplicable al uso de inteligencia artificial en el ámbito del Poder Judicial provincial. Expediente SAC 10142344. Protocolo de Acuerdos Reglamentarios.
14. Reglamentos y directrices de los proveedores externos integrados (Terms of Service y Data Processing Addendums de Anthropic, OpenAI, Google, ElevenLabs y Firecrawl).
15. Doctrina argentina sobre confidencialidad cliente-abogado frente al uso de IA. Publicaciones en revistas jurídicas especializadas (2024-2026).