

# Cookbook de protección de datos y uso responsable de plataformas de IA generativa

*Guía práctica para profesionales, usuarios y organizaciones en Argentina que utilizan plataformas de IA generativa*

Coautoras: Mariana Sánchez Caparrós - Maria Caraballo  
Colaboradora: Johanna Licciardi

## ÍNDICE TENTATIVO

<b>Introducción.....</b>	<b>3</b>
Objetivos de la guía.....	3
A quién está dirigida.....	3
Por qué es clave proteger los datos en la era de la IA generativa.....	4
<b>1. ¿Qué implica el tratamiento de datos personales en plataformas de IA generativa?.....</b>	<b>4</b>
Definición legal de dato personal y tratamiento (Ley 25.326).....	5
Características relevantes de la plataformas de IA generativa de cara a la protección de datos:.....	5
Datos que “viajan” en cada interacción: input, output, metadatos.....	6
Veámoslo con un ejemplo: un prompt aparentemente inocuo puede incluir datos personales.....	6
<b>2. Datos disponibles y datos de uso libre: acceso público y protección legal... 8</b>	<b>8</b>
Datos públicos y datos de acceso irrestricto.....	8
Marco legal argentino: límites al uso de datos personales disponibles en internet.	9
Veámoslo con un ejemplo: uso indebido de datos disponibles en bases abiertas.	9
<b>3. Riesgos para la privacidad cuando usamos plataformas de IA generativa... 10</b>	<b>10</b>
Recolección y entrenamiento con datos del usuario (ej. ChatGPT y Gemini).....	10
Usos comerciales adicionales, transferencias de datos y algunas advertencias a considerar.....	11
<b>4. Términos y condiciones: la “letra chica” que debemos leer..... 12</b>	<b>12</b>
Términos, condiciones y políticas de privacidad.....	12
Qué revisar en las políticas de privacidad de cada plataforma.....	12
Ejemplo comparado: ChatGPT gratuito/Plus/Pro (uso individual) vs. ChatGPT Enterprise (uso corporativo).....	13
Indicadores de alerta: qué cláusulas deberían preocuparnos.....	14
<b>5. Gobierno de Datos e Inteligencia Artificial..... 14</b>	<b>14</b>
¿Por qué es necesario un marco de Gobierno en IA generativa?.....	14

Decidir con IA propia no es lo mismo que usar herramientas externas.....	16
Gobernanza embebida: ejecución por default.....	17
<b>6. A modo de cierre: buenas prácticas para proteger nuestros datos al usar plataformas de IA generativa.....</b>	<b>17</b>
Otras alternativas seguras: licencias comerciales adecuadas, modelos locales, APIs herramientas sin conexión.....	19
<b>7. Checklist final: uso responsable de IA generativa.....</b>	<b>20</b>

## Introducción

### Objetivos de la guía

El objetivo de este *cookbook* es brindar una herramienta práctica y accesible para que profesionales, organismos públicos y usuarios en general comprendan los riesgos y obligaciones legales vinculados al uso de plataformas de inteligencia artificial generativa (IAgen) cuando están en juego datos personales.

Nos proponemos:

- Explicar de manera clara qué implica el tratamiento de datos personales en entornos de IA generativa de uso frecuente.
- Promover un uso responsable y seguro de plataformas como ChatGPT, Gemini, Copilot, entre otras.
- Difundir buenas prácticas que permitan cumplir con la Ley 25.326 de Protección de Datos Personales y minimizar los riesgos para la privacidad de las personas.
- Ofrecer ejemplos concretos que ayuden a identificar situaciones habituales de riesgo, muchas veces invisibles para el usuario no especializado.
- Fortalecer capacidades institucionales en materia de privacidad, especialmente en contextos sensibles como la justicia, la educación, la salud o la administración pública.

Esta guía no pretende desalentar el uso de herramientas de IA generativa, sino **acompañar su adopción con criterios de legalidad, ética y respeto por el derecho a la privacidad y protección de datos.**

### A quién está dirigida

Esta guía está especialmente pensada para:

- **Profesionales que utilizan IA en sus tareas diarias**, como personal judicial, docentes, investigadores, periodistas, médicos, abogados, técnicos o desarrolladores.
- **Agentes del sector público**, que implementan tecnologías en procesos institucionales y deben garantizar el cumplimiento de las normas de protección de datos.
- **Organizaciones que trabajan con información sensible o confidencial**, como ONGs, universidades, empresas prestadoras de servicios tecnológicos o de salud.

- **Usuarios individuales** que desean comprender mejor qué sucede con sus datos al interactuar con modelos de IA generativa y cómo pueden resguardar su privacidad.

Sin importar el nivel de conocimiento técnico o jurídico, el enfoque de este *cookbook* busca que cualquier persona pueda entender **por qué es importante proteger los datos personales y cómo hacerlo** en contextos concretos.

### **Por qué es clave proteger los datos en la era de la IA generativa**

La irrupción de la IA generativa cambió la forma en que interactuamos con las tecnologías. Hoy, con solo contar con un dispositivo electrónico y conexión a internet, es posible mantener un diálogo con una sistema de IA, pedirle que redacte textos, analice documentos, resuma expedientes, traduzca conversaciones o redacte correos electrónicos, entre muchas otras tareas.

Pero esta accesibilidad tiene un costo: cada vez que compartimos información con un modelo de IA, dejamos rastros que pueden incluir datos personales propios o de terceros. Nombres, direcciones, opiniones políticas, antecedentes laborales, enfermedades y otros padecimientos, e, incluso, imágenes, pueden quedar incorporadas en plataformas que no siempre ofrecen garantías de confidencialidad, ni control sobre el destino de esos datos.

Adicionalmente, aunque muchas personas, creen que si una sentencia o una resolución está publicada en internet ya puede usarse libremente, eso no es así. **El hecho de que un dato personal esté disponible en la web no significa que pueda tratarse sin límites.**

La Ley 25.326 protege todos los datos personales, aún los de acceso público, si se los trata en un contexto que afecte la privacidad o implique una finalidad distinta a la prevista al momento de su publicación.

Además, muchas de las plataformas de IA generativa son desarrolladas por empresas radicadas en el exterior, lo que introduce el problema adicional de la transferencia internacional de datos. La legislación argentina establece condiciones especiales para que estos flujos transfronterizos sean válidos y seguros.

En este contexto, **el uso responsable de la IA generativa no es solo una buena práctica, sino una obligación legal y ética.** Comprender cómo se recolectan, procesan, almacenan y comparten los datos personales en estas plataformas es clave para garantizar la protección de derechos y prevenir situaciones de vulnerabilidad digital.

Este *cookbook* se propone ser una brújula para navegar ese nuevo territorio.

### **1. ¿Qué implica el tratamiento de datos personales en plataformas de IA generativa?**

## Definición legal de dato personal y tratamiento (Ley 25.326)

La Ley 25.326<sup>1</sup> de Protección de los Datos Personales define como **dato personal** a toda información de cualquier tipo referida a personas físicas o de jurídicas determinadas o determinables<sup>2</sup>. Esto incluye nombres, domicilios, DNI, correos electrónicos, opiniones personales, datos laborales, entre otros. También contempla como **datos sensibles** a aquellos que revelan origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, información sobre salud o vida sexual<sup>3</sup>.

Por su parte, se entiende por **tratamiento de datos** a las "[O]peraciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias..."<sup>4</sup>.

Esto significa que **toda interacción con una plataforma de IA que implique cargar, ingresar o referenciar datos personales constituye un tratamiento de datos** y, por lo tanto, **debe cumplir con los principios y obligaciones previstos en la ley**, como el **consentimiento** del titular, la **finalidad** legítima, la **seguridad** de los datos y la **confidencialidad**.

### Características relevantes de la plataformas de IA generativa de cara a la protección de datos:

Las plataformas de IA generativa (como ChatGPT, Gemini, Copilot o Claude) presentan las siguientes características:

- **Multipropósito:** no están diseñadas para una tarea cerrada, sino que generan texto, imagen, código, video o sonido según la instrucción dada por el usuario, lo que incrementa la incertidumbre sobre el uso posterior de los datos ingresados.
- **Procesamiento en la nube y por terceros:** en general funcionan en servidores externos (normalmente ubicados en el extranjero), lo que implica una transferencia internacional de datos que debe estar habilitada por la Ley

---

<sup>1</sup> Ver <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>

<sup>2</sup> Ver art. 2 de la ley, en <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>

<sup>3</sup> Ver art. 2 de la ley, en <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>

<sup>4</sup> Ver art. 2 de la ley, en <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>

25.326 (art. 12)<sup>5</sup>.

- **Reutilización de la información:** algunas plataformas pueden utilizar los datos ingresados por el usuario para entrenar o mejorar sus modelos, así como para otros fines comerciales, salvo que se configure lo contrario o se use una versión empresarial con garantías específicas.

En virtud de ello, el usuario pierde el control sobre los datos ingresados si no se toman medidas preventivas.

### **Datos que “viajan” en cada interacción: input, output, metadatos**

Cuando usamos una herramienta de IA generativa, no solo se expone el contenido textual que le proporcionamos (input), sino también:

- **Los archivos que se cargan y su contenido:** documentos, PDFs, planillas, imágenes, audios.
- **El contenido que produce la IA (output):** puede reflejar, repetir o incluso inferir datos personales no ingresados explícitamente.
- **Los metadatos:** información técnica asociada a la interacción (ubicación, hora, ID de usuario, dirección IP, historial de consultas previas, etc.).

Toda esa información puede ser **recolectada, almacenada, analizada y eventualmente compartida con terceros si así lo permiten los términos y condiciones** de la plataforma.

### **Veámoslo con un ejemplo: un prompt aparentemente inocuo puede incluir datos personales**

Supongamos que una abogada laboralista utiliza una plataforma de IA generativa para mejorar la redacción de un escrito judicial y formula el siguiente mensaje:

*"Te adjunto una contestación de demanda que redacté para un cliente. Por favor, revisala y sugerime mejoras en la argumentación. Se trata de una causa por despido indirecto en la que el actor, Juan Carlos D., alega haber sido forzado a renunciar tras varios meses sin cobrar. Mi cliente es el titular de una ferretería en Avellaneda. Adjunto el archivo para que puedas trabajar con el contenido."*

El archivo contiene el escrito completo de la contestación de demanda, en el que figuran:

---

<sup>5</sup> Ver art. 12 de la ley, en <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>

- Nombre completo del actor, el empleador y sus respectivos domicilios.
- Detalles laborales (puesto, salario, fecha de ingreso y cese, CUIL).
- Hechos personales y circunstancias que podrían afectar la reputación de las partes.

Aunque la intención de la profesional es simplemente mejorar la redacción del escrito, lo que está haciendo —sin una revisión previa ni anonimización del documento— es exponer datos personales de múltiples personas ante una plataforma que, según su propia política de privacidad:

1. **Puede conservar el contenido ingresado** (texto y archivos) y utilizarlo para múltiples finalidades, incluso con posterioridad al cierre de la sesión.
2. **Puede procesarlo fuera de la Argentina**, en servidores ubicados en terceros países, lo que implica una transferencia internacional de datos que sólo cumpliría con la legislación local si el país receptor ofrece un nivel de protección adecuado o se aplican las excepciones previstas por el artículo 12 de la Ley 25.326.
3. **Puede utilizar la información (input, output y metadatos) para mejorar sus modelos de IA**, entrenarlos o desarrollar nuevas funcionalidades, salvo que el usuario haya realizado una configuración específica de exclusión (opt-out).
4. **Puede usar los datos con fines comerciales adicionales**, como analizar el modo en que se utilizan los servicios, mejorar productos existentes, desarrollar nuevos servicios, prevenir fraudes, cumplir obligaciones legales o realizar transmisiones de negocio.
5. **Puede compartir los datos con terceros**, incluyendo proveedores de servicios tecnológicos, autoridades gubernamentales, entidades afiliadas, administradores de cuentas empresariales y, eventualmente, terceros que participen en operaciones estratégicas (fusiones, adquisiciones, reorganizaciones)<sup>6</sup>.

Este tipo de situación, común en el uso profesional cotidiano de herramientas de IA, supone un tratamiento de datos personales que podría resultar incompatible con la normativa argentina si no se cuenta con una base legal válida (consentimiento,

---

<sup>6</sup> “Sam Altman advierte: las conversaciones con ChatGPT no están protegidas por secreto profesional”, Infobae, <https://www.infobae.com/tecno/2025/07/28/sam-altman-advierte-las-conversaciones-con-chatgpt-no-estan-protegidas-por-secreto-profesional/>, acceso el 24/9/2025.

interés estatal legítimo, etc.) o si no se adoptan medidas adecuadas de seguridad y anonimización.

La clave es entender que adjuntar un documento que contiene datos personales sin anonimizar **equivale a compartirlo con un tercero no autorizado**, salvo que se demuestre que la plataforma ofrece garantías equivalentes a las exigidas por la Ley 25.326 y su reglamentación.

Por ello, toda carga de archivos o interacción con IA generativa debe hacerse con una **lógica de privacidad por defecto y desde el diseño**, lo que implica:

- No cargar datos personales o sensibles sin anonimizar.
- Revisar la política de privacidad y condiciones del servicio antes de usarlo.
- Preferir herramientas con garantías contractuales adecuadas o versiones empresariales con retención cero.
- Consultar al Delegado de Protección de Datos o a las áreas legales y técnicas de la organización.

## **2. Datos disponibles y datos de uso libre: acceso público y protección legal**

### **Datos públicos y datos de acceso irrestricto**

En el lenguaje cotidiano, se suele pensar que si un dato está publicado en internet, cualquiera puede utilizarlo libremente. Sin embargo, un “dato de acceso irrestricto” es aquel que, por decisión normativa expresa, puede ser consultado y reutilizado libremente por cualquier persona, sin autorización previa y sin restricciones derivadas de derechos de terceros. Ejemplos típicos son:

- Estadísticas agregadas sin información identificable.
- Normativa publicada en boletines oficiales.

Ahora bien, **la simple accesibilidad técnica a datos personales** —como que una sentencia judicial sin anonimizar esté publicada en una web de acceso público— **no habilita su uso irrestricto**.

Esa información continúa protegida por la normativa de protección de datos personales, y el hecho de que esté disponible en línea no altera ni la finalidad legítima para la cual fue difundida (por ejemplo, garantizar la publicidad de los actos de gobierno), ni las garantías que rigen su tratamiento cuando éstos exceden la finalidad para la cual fueron colectados<sup>7</sup>.

---

<sup>7</sup> Para ampliar ver Peyrano, Guillermo A, “El acceso a la información pública y las restricciones emergentes del carácter de los datos archivados

## Marco legal argentino: límites al uso de datos personales disponibles en internet

Bajo la Ley 25.326<sup>8</sup>, el hecho de que un dato personal esté en un portal público o que se pueda acceder mediante buscadores **no elimina su carácter protegido** si:

- Permite identificar, directa o indirectamente, a una persona.
- No existe una norma que habilite su reutilización para fines distintos a los que motivaron su publicación (ej. procesamiento en una plataforma de IA propiedad de un tercero que se reserva el derecho de darle otros usos).
- Su tratamiento implica una cesión a terceros (ej. una plataforma de IA generativa), lo que requiere consentimiento o una base legal válida.

En este punto:

- El **art. 4** de la ley 25.326 exige que el tratamiento sea lícito y adecuado a la finalidad para la que se recolectaron los datos.
- El **art. 11** regula la cesión a terceros, imponiendo consentimiento informado salvo excepciones limitadas (p. ej., ejercicio de funciones propias del Estado).
- El **art. 12** establece condiciones estrictas para **transferencias internacionales de datos**, prohibiendo enviar datos a países sin nivel de protección adecuado salvo excepciones taxativas.

## Veámoslo con un ejemplo: uso indebido de datos disponibles en bases abiertas

**Sentencias judiciales no anonimizadas:** el principio de publicidad procesal habilita el acceso a sentencias publicadas en la web, pero no habilita automáticamente a su procesamiento con cualquier herramienta de IA generativa, si ello conlleva usos para fines ajenos al proceso.

Por ejemplo, una persona que prepara un recurso judicial podría volcar en una plataforma de IA generativa el texto completo de una sentencia no anonimizada—que contiene nombres, domicilios o datos sensibles— para pedir un resumen o análisis. Aunque el objetivo sea personal y legítimo, al usar una herramienta que almacena o procesa la información en servidores de terceros (incluso en el extranjero), si los términos y condiciones de la plataforma contemplan posibles usos comerciales de ese contenido, se estaría realizando un tratamiento de datos

---

["https://www.sajj.gob.ar/doctrina/dasa050098-peyrano-acceso\\_informacion\\_publica\\_las.htm#:~:text=%2D%20Tales%20a%20modo%20de%20ejemplo.la%20perseguida%20con%20la%20registraci%C3%B3n](https://www.sajj.gob.ar/doctrina/dasa050098-peyrano-acceso_informacion_publica_las.htm#:~:text=%2D%20Tales%20a%20modo%20de%20ejemplo.la%20perseguida%20con%20la%20registraci%C3%B3n).

<sup>8</sup> Cfr. arts. 4, 5, 6, 11 y 12 de la Ley 25.326.

personales no autorizado, con riesgo de vulnerar la privacidad de las personas mencionadas y de incumplir la normativa vigente.

En otras palabras, si los términos y condiciones de la herramienta habilitan el almacenamiento o reutilización esa información para entrenar modelos o para otros fines comerciales, se estaría incurriendo en un tratamiento no autorizado de datos personales, comprometiendo no sólo la confidencialidad del expediente sino también la responsabilidad institucional del magistrado.

### 3. Riesgos para la privacidad cuando usamos plataformas de IA generativa

El uso de plataformas de IA generativa como **ChatGPT (OpenAI)**, **Grok (XAI)** o **Gemini (Google)** bajo licencias de usuario individual, plantea riesgos específicos para la privacidad que los usuarios deben conocer.

Estos riesgos derivan, principalmente, de la **recolección y tratamiento de datos personales**, su **uso para fines distintos al inicialmente previsto** (como entrenamiento de modelos o fines comerciales), y la **posible transferencia internacional de datos** a países con diferentes niveles de protección.

#### Recolección y entrenamiento con datos del usuario (ej. ChatGPT y Gemini)

Tanto OpenAI<sup>9</sup> como Google<sup>10</sup>, bajo licencias no comerciales (ej. licencias Plus y Pro de OpenAI), recogen información de las interacciones de los usuarios:

- **ChatGPT:** salvo en versiones empresariales (Enterprise, Team, API), la política de OpenAI permite recolectar **los prompts, archivos subidos y las respuestas generadas**, así como información técnica (IP, dispositivo, cookies). Estos datos pueden usarse para entrenar modelos, aunque existe la opción de excluirse (“opt out”), y mejorar servicios, entre otros posibles usos comerciales.
- **Gemini (Google):** por defecto, guarda la actividad del usuario y puede usar **conversaciones, archivos, imágenes, audios y pantallas compartidas** para mejorar servicios y entrenar sus modelos.

**Riesgo principal:** al subir información protegida (ej. una historia clínica o un expediente judicial), esos datos podrían ser almacenados y analizados por la empresa para fines que exceden finalidad original para la que fueron colectados.

---

<sup>9</sup> Ver en <https://openai.com/es-ES/policias/row-privacy-policy/>, acceso el 18/8/2025.

<sup>10</sup>

Ver

en

[https://support.google.com/gemini/answer/13594961?hl=es&visit\\_id=638911106617658115-1419311114&p=e\\_history\\_pn&rd=1#privacy\\_notice](https://support.google.com/gemini/answer/13594961?hl=es&visit_id=638911106617658115-1419311114&p=e_history_pn&rd=1#privacy_notice), acceso el 18/8/2025.

## Usos comerciales adicionales, transferencias de datos y algunas advertencias a considerar

En general, las licencias de usuario individual de plataformas de IA generativa, como ChatGPT o Gemini, contemplan la posibilidad de compartir datos con **proveedores de servicios externos** (cloud, soporte técnico, analítica, publicidad). A modo de ejemplo:

- Google aclara que puede utilizar la información para **personalizar anuncios y servicios**, aunque restringe el uso de categorías sensibles (salud, religión, orientación sexual).
- OpenAI prevé que los datos puedan compartirse con **afiliados, contratistas y autoridades gubernamentales** en ciertos supuestos.

Además, en la práctica, el procesamiento se realiza en **servidores fuera de la Argentina**. Esto supone una **transferencia internacional de datos** bajo el art. 12 de la Ley 25.326, lo que obliga a tener presente que:

- La regla es que solo pueden transferirse datos a países con “nivel adecuado” (p. ej. UE, Uruguay, Israel para datos automatizados, etc.).
- Si no lo son (como EE.UU. salvo mecanismos contractuales), se requiere consentimiento expreso del titular o cláusulas contractuales modelo aprobadas por la AAIP.

Cuando el usuario sube información que no es propia (por ejemplo, la **historia clínica de un paciente**, el **legajo de un empleado**, o una **sentencia judicial con nombres completos**), se encuentra frente a una situación que obliga a considerar los siguientes elementos con relación a:

### 1. La titularidad de esos datos.

Según la Ley 25.326, el **consentimiento debe ser prestado por el titular del dato** para que el tratamiento sea lícito, salvo excepciones expresas (ej. cumplimiento de funciones estatales).

### 2. La finalidad original del tratamiento cuando esta no coincide con los usos previstos en los términos y condiciones de la plataforma.

Que un dato esté en un expediente judicial, en un legajo administrativo o en una base pública **no habilita su reutilización con fines comerciales** por un tercero, como entrenamiento de modelos, analítica de negocio o personalización de anuncios.

### 3. La posible cesión o transferencia del dato.

Cuando esos datos son procesados para finalidades propias (mejora de

servicios, marketing, entrenamiento), se convierten en una **cesión no autorizada**. El usuario que los subió sin consentimiento puede quedar expuesto a responsabilidad por haberlos transferido sin base legal válida.

**En suma:** el usuario puede desconocer que al usar estas plataformas está autorizando indirectamente, no solo la transferencia internacional de datos, sino también su **uso para fines comerciales incompatibles** con la finalidad original de recolección del dato. Esto es particularmente grave tratándose de **datos de terceros que nunca prestaron consentimiento**, lo que puede generar infracciones a la Ley 25.326, responsabilidades administrativas ante la AAIP y, en algunos casos, responsabilidad civil por daños.

#### **4. Términos y condiciones: la “letra chica” que debemos leer**

##### **Términos, condiciones y políticas de privacidad**

Cuando usamos plataformas de IA generativa, los **términos y condiciones (T&C) y las políticas de privacidad** son los documentos que regulan cómo se tratarán los datos que compartimos a través de las conversaciones que mantenemos con la IA. Y aunque muchas veces se aceptan sin leerlos, allí se define si el contenido que subimos puede ser usado para entrenar modelos, cuánto tiempo se conserva, si puede compartirse con terceros y si hay transferencias internacionales de datos.

En Argentina, la **Ley 25.326 de Protección de Datos Personales** establece que todo tratamiento de datos debe tener base legal (consentimiento, contrato, obligación legal, etc.) y que las transferencias internacionales solo son válidas si el país receptor garantiza un “nivel adecuado” de protección o si se firman cláusulas contractuales aprobadas por la AAIP.

Por eso, **conocer la letra chica no es un detalle:** puede marcar la diferencia entre un uso seguro o una vulneración de la privacidad. Usualmente, **las licencias de uso individual y las licencias de uso corporativo** que ofrecen las plataformas suelen presentar diferencias importantes en cuanto al tratamiento y protección de los datos recolectados de la interacción del usuario con la IA. **Es importante conocer esas diferencias para hacer una elección adecuada.**

##### **Qué revisar en las políticas de privacidad de cada plataforma**

Al elegir una plataforma de IA generativa conviene fijarse en:

- **Recolección de datos:** qué información colecta (inputs, archivos, historial de uso, metadatos).
- **Uso de los datos:** si se usan para entrenar modelos, mejorar servicios o fines comerciales.

- Tiempo de retención: cuánto se guardan los datos y dónde.
- Acceso de terceros: si se comparten con proveedores, afiliados o autoridades.
- Transferencias internacionales: si los datos se procesan fuera de Argentina y en qué condiciones legales.
- Derechos del usuario: posibilidad de pedir acceso, rectificación, eliminación o exclusión de usos como el entrenamiento.

**Ejemplo comparado: ChatGPT gratuito/Plus/Pro (uso individual) vs. ChatGPT Enterprise (uso corporativo)**

Aspecto	ChatGPT Free / Plus / Pro (uso individual)	ChatGPT Team / Enterprise (uso corporativo)
Acceso	<a href="https://openai.com/es-ES/policies/ro-privacy-policy/">https://openai.com/es-ES/policies/ro-privacy-policy/</a>	<a href="https://openai.com/es-ES/enterprise-privacy/">https://openai.com/es-ES/enterprise-privacy/</a>
Recolección de datos	OpenAI guarda inputs, archivos subidos, outputs y metadatos de uso.	Los datos son propiedad del cliente; OpenAI no los usa para entrenar modelos.
Uso para entrenamiento	Sí, por defecto. El usuario puede hacer <i>opt-out</i> (configuración de privacidad).	No se utilizan para entrenamiento ni mejora de modelos.
Uso comercial	OpenAI se reserva el derecho de utilizar los datos para “fines comerciales legítimos”, como desarrollo de nuevos servicios, transmisiones de negocios y compartición con terceros.	Se limita el uso comercial: OpenAI no puede explotar datos de clientes Enterprise más allá de lo necesario para la prestación del servicio y soporte técnico.
Retención	Tiempo indeterminado; se conserva mientras sea “necesario” para fines comerciales y legales.	El cliente controla retención y eliminación de datos (Enterprise ofrece incluso “retención cero”).
Acceso de terceros	Puede compartirse con proveedores de servicios, afiliados, autoridades y en fusiones/ventas.	Acceso restringido a empleados autorizados por soporte o

		seguridad; contratistas sujetos a confidencialidad.
<b>Seguridad</b>	Encriptación básica, cookies y analítica.	Cifrado AES-256 y TLS 1.2+, SAML SSO, controles avanzados de acceso.

## Indicadores de alerta: qué cláusulas deberían preocuparnos

Cuando leas una política de privacidad, prestá especial atención a:

1. “Podemos usar tus datos para mejorar nuestros servicios, incluyendo entrenamiento de modelos” → significa que tus inputs no son privados y hay un riesgo de uso no previsto originariamente.
2. “Podemos compartir tus datos con afiliados, proveedores o autoridades competentes” → riesgo de cesión amplia y uso no previsto originariamente.
3. “Conservaremos tus datos mientras sea necesario para fines comerciales legítimos” → ausencia de plazo concreto y habilitación para usos de negocio no previstos originalmente.
4. “Tus datos pueden ser transferidos y procesados en otras jurisdicciones” → implica transferencias internacionales que, en Argentina, requieren garantías adicionales.
5. “Nos reservamos el derecho de modificar la política en cualquier momento” → puede cambiar el nivel de protección sin previo aviso.

## 5. Gobierno de Datos e Inteligencia Artificial

### ¿Por qué es necesario un marco de Gobierno en IA generativa?

Como se ha señalado a lo largo de este texto, el uso de inteligencia artificial generativa abre posibilidades inéditas, pero también expone riesgos concretos para la privacidad y el manejo de datos sensibles<sup>11</sup>.

Esto se vuelve aún más evidente en ámbitos críticos como instituciones públicas, donde **una mala práctica puede comprometer derechos fundamentales o erosionar la confianza**. Frente a este escenario, no alcanza con aplicar recomendaciones aisladas, se necesita un marco de Gobierno de Datos e

<sup>11</sup> Ley 25.326 — Protección de Datos Personales (Argentina). Marco general de licitud del tratamiento, calidad de datos, consentimiento informado y transferencias internacionales (arts. 4, 5, 6, 11 y 12).

Inteligencia Artificial (IA) que ordene, controle y habilite<sup>12</sup> el uso responsable de estas tecnologías, asegurando que la innovación no se traduzca en vulneración de derechos.

El Gobierno de Datos e IA no se limita a cumplir con una ley o con una política de privacidad. Se trata de un marco organizacional que establece cómo se deben gestionar los datos y los modelos de manera integral: desde la recolección y el almacenamiento hasta la forma en que se comparten, auditan y reutilizan. Es el mecanismo que permite garantizar que los proyectos de IA realmente aporten valor, reduciendo riesgos legales, éticos y reputacionales, y promoviendo un uso transparente y confiable.

A diferencia de las prácticas individuales, el Gobierno de Datos e IA, **desplaza la responsabilidad de la persona usuaria hacia la organización en su conjunto.**

No basta con que un juez, un investigador o un empleado público “tenga cuidado”<sup>13</sup> al usar IA generativa, porque estaríamos dependiendo de la proactividad de cada persona para capacitarse<sup>14</sup> y formarse en estas temáticas. Se requieren reglas, procesos y roles, con responsabilidades bien definidas que aseguren un uso legítimo, seguro y ético.

Así, el foco pasa de la gestión individual del riesgo a una responsabilidad institucional y colectiva, donde cada parte asume un rol específico en la **protección de los datos y en la integridad de los resultados.**

Un marco de Gobierno sólido también es clave para generar confianza. La ciudadanía espera que las instituciones que administran información sensible —como expedientes judiciales o historias clínicas— actúen con responsabilidad y transparencia. La confianza se fortalece cuando se aplican medidas de gobernanza claras: auditorías, protocolos de anonimización, trazabilidad de datos y criterios éticos en la elección de proveedores y plataformas. **Sin confianza, incluso la mejor tecnología puede verse cuestionada o rechazada socialmente.**

En este sentido, el Gobierno de Datos e Inteligencia Artificial es la brújula que guía el uso de IA generativa y tradicional, en entornos institucionales. Permite aprovechar su potencial transformador, sin comprometer la privacidad, la seguridad ni la dignidad de las personas. Es, al mismo tiempo, un **marco de cumplimiento**

---

<sup>12</sup> OCDE (2019), “Principios sobre Inteligencia Artificial” — y UNESCO (2021), “Recomendación sobre la Ética de la IA”. Estándares internacionales: enfoque basado en riesgos, transparencia/explicabilidad, supervisión humana y gobernanza responsable. Sirven para anclar que el Gobierno de Datos e IA es un marco organizacional y no solo cumplimiento legal.

<sup>13</sup> UNESCO, Recomendación sobre la Ética de la IA (2021). Estándar global que subraya supervisión humana, protección de derechos y proporcionalidad en el despliegue de IA por instituciones públicas.

<sup>14</sup> Ley 27.275 — Acceso a la Información Pública (Argentina).

Consagra la máxima divulgación con excepciones proporcionales, incluyendo protección de datos personales. Refuerza la idea de responsabilidad institucional: transparencia sí, pero con resguardos.

**normativo, una herramienta de gestión de riesgos y una garantía ética** para que la adopción de IA sea sostenible, escalable y legítima <sup>15</sup>en el tiempo.

### **Decidir con IA propia no es lo mismo que usar herramientas externas**

El uso de inteligencia artificial generativa en el ámbito judicial y administrativo plantea un dilema central: ¿qué cambia cuando el Estado decide usar un modelo propio para tomar decisiones frente a cuando alguien utiliza una herramienta de terceros como ChatGPT? Ambos escenarios parecen similares, pero los riesgos de gobernanza son distintos y deben abordarse con criterios específicos.

#### **Caso 1: Modelos de IA generativa aplicados a decisiones judiciales o administrativas.**

Cuando una institución pública incorpora un modelo de IA generativa<sup>16</sup> para apoyar resoluciones o actos administrativos, el foco del gobierno debe estar en la legitimidad institucional. Esto implica asegurar la trazabilidad de los datos de entrenamiento, la explicabilidad de las respuestas, la existencia de mecanismos de auditoría y revisión humana y, sobre todo, la soberanía de los datos: que la información procesada se aloje en entornos bajo control estatal. Aquí, el riesgo principal es que la IA condicione o justifique decisiones que afectan derechos, por lo que se requieren los más altos estándares de transparencia, imparcialidad y responsabilidad.

#### **Caso 2: Uso de herramientas de terceros como ChatGPT, Gemini, Copilot, Claude o Perplexity, que funcionan en la nube y bajo políticas comerciales externas.**

En este caso, cuando se utiliza una plataforma externa para procesar expedientes, redactar escritos o analizar información, el riesgo de gobernanza se traslada a la gestión de los datos ingresados. La prioridad debe ser evitar que se expongan datos personales o sensibles, revisar si los términos de servicio permiten reutilizar la información para entrenamiento de los modelos, y evaluar si se producen transferencias internacionales que podrían vulnerar la normativa argentina. Aquí, además, aparece una responsabilidad directa de los funcionarios: al subir una sentencia, resolución, etc, o cualquier acto administrativo a una plataforma que permita su consumo público, están exponiendo datos personales de las partes que luego pueden ser utilizados, almacenados o redistribuidos por cualquier persona o entidad fuera todo control. En este escenario, el problema no es solo la fuga o explotación comercial de datos, sino también la posible responsabilidad institucional y personal por haber entregado información pública en condiciones que vulneran la privacidad y los derechos de terceros.

---

<sup>15</sup> Reglamento (UE) 2024/1689 — “AI Act”.Enfoque basado en riesgo, obligaciones de gestión, trazabilidad y transparencia para sistemas de IA. Referencia internacional para sostener un Gobierno de IA que sea sostenible, escalable y legítimo.

<sup>16</sup> AAIP, Guía para una IA responsable (2024).Recomendaciones para integrar transparencia y protección de datos personales en proyectos de IA de organismos públicos y privados (evaluación de impacto, minimización y anonimización)

## Gobernanza embebida: ejecución por *default*

El gobierno de datos e IA no debe entenderse como una carga manual, sino como un **sistema automatizado de garantías**. Conviene integrarlo en *pipelines* institucionales que combinen herramientas de proveedores y soluciones *open source*: antes de publicar una sentencia o resolución, el flujo extrae el texto, **detecta y anonimiza** datos personales, limpia metadatos e imágenes, **bloquea la publicación** si persiste información sensible y genera un **registro auditable**. Todo queda orquestado desde el gestor documental o el *CI/CD*, ya sea en entornos propios (*on-premises*) o en nube soberana. Así, la privacidad y la ética dejan de depender de acciones individuales porque quedan **integradas** al proceso.

La automatización, además, habilita **controles preventivos** y de **cumplimiento continuo**: alertas cuando un expediente contiene información sensible; **data contracts** que definen de antemano qué datos pueden usarse y bajo qué condiciones; y **auditorías en tiempo real** sobre lo que se carga en modelos de terceros. De este modo, la gobernanza se convierte en una **infraestructura viva** que acompaña la innovación con seguridad, transparencia y eficiencia, manteniendo la confianza pública sin frenar la adopción tecnológica.

Este capítulo, deja una premisa nítida: **transparencia sin exposición, ética operativa y gobernanza embebida por defecto**. En las instituciones, **decidir con IA propia** exige trazabilidad, explicabilidad y soberanía de datos; **usar herramientas externas** demanda frenar la fuga de información y controlar estrictamente los términos de uso. Cuando normas, ética y automatización convergen, la gobernanza deja de ser una política para convertirse en **infraestructura**<sup>17</sup>: reglas que se ejecutan por diseño, se auditan sin fricción y escalan con el proceso.

**En síntesis: lo correcto, automatizado y a escala.**

## 6. A modo de cierre: buenas prácticas para proteger nuestros datos al usar plataformas de IA generativa

El uso de plataformas de IA generativa (IAGen) implica un riesgo potencial para la privacidad, ya que muchas de ellas recolectan, procesan y almacenan la información ingresada —incluyendo datos personales— para distintos fines, como mejorar sus modelos o con otros propósitos comerciales.

La **Ley 25.326** protege estos datos incluso si están disponibles en línea, y su tratamiento requiere base legal o consentimiento del titular.

### Buenas prácticas:

---

<sup>17</sup> OCDE, Principios de IA (2019). Promueven transparencia, responsabilidad y robustez; respaldan la noción de gobernanza como infraestructura de confianza.

## 1. Evaluar la política de privacidad antes de usar la herramienta

- Identificar qué datos recolecta, para qué los usa, si los conserva, y si los transfiere internacionalmente.
- Ejemplo: en ChatGPT (versión gratuita y licencias Plus y Pro), los prompts y archivos pueden usarse para entrenar modelos y otros fines comerciales; en ChatGPT Enterprise, la empresa asegura que no se usan para entrenamiento y que el cliente controla la retención.

## 2. Aplicar el principio de minimización de datos

- Ingresar sólo la información estrictamente necesaria para la tarea.
- Ejemplo: si la IA debe resumir una sentencia, eliminar nombres y otros datos identificatorios antes de cargarla.

## 3. Limitar el uso de herramientas sin control institucional

- Organizaciones y organismos públicos deberían definir qué plataformas están autorizadas y bajo qué condiciones.
- Ejemplo: un tribunal puede permitir el uso de un modelo local para tareas internas, pero prohibir plataformas abiertas con expedientes no anonimizados.

## 4. Pre-publicación de sentencias (pipeline automático)

Al cerrar un fallo, el sistema extrae texto, detecta PII (nombres, DNI/CUIL, domicilios), anonimiza, limpia metadatos y **bloquea** la publicación si queda algo sensible. Se registra un **log** auditable (hash + sello de tiempo) con la versión original y la pública.

## 5. Pasarela DLP para IA externas (ChatGPT/Gemini/Copilot/Claude)

Antes de enviar un documento o *prompt*, un **proxy** revisa y **redacta** PII o **impide** el envío si hay información crítica; además, traza quién, cuándo y a qué plataforma intentó enviar.

## 6. Data contracts para expedientes

Cada tipo documental tiene un contrato con **campos permitidos/prohibidos**. Al entrar a un flujo (resumen, clasificación, búsqueda), un validador automático **rechaza** el documento si trae campos no permitidos o faltan redacciones obligatorias.

## 7. Alertas preventivas en tiempo real

Si el expediente contiene categorías sensibles (salud, menores, violencia de género), el sistema dispara una **alerta** y fuerza el modo “**solo interno**” hasta cumplir la anonimización.

## 8. Sandboxes locales para tareas de IA

Resúmenes o clasificaciones preliminares se ejecutan en un **entorno local sin internet**; solo la versión ya anonimizada puede salir a un servicio externo, con **trazabilidad** de las operaciones.

## 9. Panel de auditoría continua

Tablero que muestra qué documentos pasaron por qué **controles**, quién aprobó, qué se **redaccionó** y qué **reglas** están activas. Incluye un **interruptor de emergencia (kill-switch)**: ante un incidente, despublica versiones afectadas y bloquea envíos externos hasta resolver.

### Otras alternativas seguras: licencias comerciales adecuadas, modelos locales, APIs herramientas sin conexión

La elección de herramientas de IA generativa debe **priorizar aquellas que reduzcan o eliminen la exposición de datos personales a terceros y que permitan cumplir con la ley 25.326.**

#### Opciones recomendadas:

Alternativa	Nivel de riesgo	Requisitos legales	Casos de uso recomendados	Ventajas principales
<b>Licencias comerciales adecuadas</b>	Bajo (si el contrato es claro y se audita su cumplimiento)	Contratos alineados con ley 25.326; cláusulas que limiten tratamiento; control de retención y acceso.	Trabajo con datos personales o sensibles que requieren garantía contractual de no entrenamiento y uso limitado.	Mayor seguridad jurídica, soporte técnico, acuerdos de confidencialidad.

<b>Modelos locales</b>	Muy bajo (sin transferencia a terceros)	Cumplir con medidas de seguridad de la Ley 25.326; privacidad por diseño y por defecto.	Procesamiento de expedientes judiciales, análisis interno de datos sensibles, entrenamiento de modelos propios.	Control total sobre datos y entorno, sin transferencias internacionales.
<b>APIs privadas con acuerdos específicos</b>	Medio-bajo (depende de configuración y país de alojamiento)	Uso de Cláusulas Contractuales Modelo si el país no es adecuado; retención cero cuando sea posible.	Integraciones en sistemas internos que requieren IA potente pero con controles de privacidad reforzados.	Combina potencia de modelos avanzados con mayor control técnico y jurídico.
<b>Herramientas sin conexión</b>	Muy bajo (sin conexión externa)	Garantizar que no haya sincronización ni envío involuntario de datos; auditoría de software.	Anonimización, clasificación y análisis de datos en entornos desconectados.	Riesgo mínimo de fuga; ideal para preprocesar datos antes de usarlos en IA en línea.

## 7. Checklist final: uso responsable de IA generativa

Pregunta clave	Qué verificar	Cumplido
¿Uso datos personales?	Confirmar base legal o consentimiento del titular antes de tratarlos.	SI/NO
¿Leí la política de privacidad?	Verificar si recolecta datos, si los usa para entrenamiento y con quién los comparte.	SI/NO

<b>¿Hay transferencia internacional?</b>	Confirmar si el país receptor es “adecuado” según AAIP; si no, verificar cláusulas contractuales modelo o consentimiento expreso.	SI/NO
<b>¿Anonimicé la información?</b>	Aplicar anonimización o seudonimización antes de usar la IA siempre que sea posible.	SI/NO
<b>¿Tengo respaldo institucional?</b>	Usar la herramienta bajo autorización o protocolos oficiales para evitar responsabilidades personales o institucionales.	SI/NO