Palatino

GUÍA DE USO SEGURO · DESPACHOS LEGALES

El marco de uso seguro de *IA* para despachos

Qué puede y qué no puede entrar en una IA, en qué entorno y con qué control. Uso gobernado alineado con el RGPD y el Reglamento de IA de la UE.

3 reglas maestras · **Checklist de 6 puntos** · **10 minutos de lectura**

Construimos el futuro humano del trabajo.

INTRODUCCIÓN

El riesgo *invisible* de usar IA sin gobierno

La mayoría de los despachos ya usan IA. La mayoría no sabe dónde acaba el dato cuando alguien pega el correo de un cliente, un borrador de contrato o las notas de un expediente en una herramienta de consumo.

No es un problema de tecnología. Es secreto profesional, es RGPD y, llegado el caso, responsabilidad. La IA no es el riesgo: usarla sin saber qué dato sale del despacho, sí lo es.

Con esta guía sabrás:

- **Qué puede y qué no puede entrar en una IA.** Un criterio común para todo el equipo, de seniors a juniors.
- **En qué entorno tratar cada tipo de dato.** La diferencia entre una herramienta de consumo y un entorno gobernado.
- **Cómo reducir el riesgo en segundos.** Tres reglas y una checklist que aplicas antes de cada prompt.

Borrador no es *decisión*.

La IA prepara. El despacho revisa, valida y firma. Siempre.

Esta guía es informativa y no constituye asesoramiento jurídico. Ante cualquier duda sobre un caso concreto, valídalo con tu DPO o asesor especializado.

FUNDAMENTOS

Las 3 reglas *maestras*

Tres reglas fijas. El ochenta por ciento del riesgo eliminado cuando se aplican con consistencia.

La IA produce borradores, nunca decisiones

01

Todo lo que sale —una cláusula, un resumen de expediente, una respuesta a cliente— es un punto de partida que revisas, corriges y firmas. Bajo el Reglamento de IA, toda salida con efecto jurídico exige control humano. La firma es del abogado, no de la herramienta.

El entorno importa tanto como el prompt

02

No es lo mismo una herramienta de consumo que un entorno corporativo con tu licencia y un contrato de encargado del tratamiento. La protección real depende de tu configuración y tus contratos, no de que el proveedor sea conocido. Verifícalo con IT y con la documentación vigente del proveedor.

Ante duda regulatoria, se escala. No se improvisa

03

Si no tienes claro si puedes introducir un dato, qué base de licitud aplica o si encaja en una categoría especial, la respuesta no es seguir con cautela. Es parar y consultar con tu DPO o compliance. Esta regla evita los incidentes que nacen de decidir en lo jurídico como si fuera técnico.

EL REFLEJO CLAVE

Clasifica un dato en *3 segundos*

Antes de pegar nada en una IA, clasifica. Son tres categorías. El tiempo que tardas es proporcional a lo que te ahorras si hay un incidente.

A Dato interno sin personas

Procedimientos del despacho, plantillas, documentación interna que no identifica a nadie.

Ejemplo. *el texto base de tu modelo de contrato de arrendamiento, sin datos del inquilino.*

→ **Adelante, en entorno gobernado. Revisa el resultado.**

B Dato personal de cliente o tercero

Nombre, DNI, datos de contacto, económicos o del caso que identifiquen a una persona física.

Ejemplo. *el hilo de correo del cliente sobre su litigio, con su nombre y los datos de la contraparte.*

→ **Solo en entorno gobernado y con el dato mínimo. Nunca en herramienta de consumo.**

C Categoría especial o dato sensible

Salud, datos penales, ideología, afiliación sindical, biometría, origen racial, creencias, orientación sexual.

Ejemplo. *el informe médico de un caso laboral; los antecedentes penales en un expediente de extranjería.*

→ **Para. Consulta con DPO o compliance antes de cualquier tratamiento. Sin excepción.**

EL HÁBITO QUE MÁS PROTEGE

El dato que no introduces no se puede *filtrar*

El error más frecuente no es el tipo de dato: es la cantidad. Quien pega de más, expone de más.

Para resumir un párrafo de un contrato no necesitas pegar las cien páginas con los datos de todas las partes. Para proponer el tono de una respuesta a cliente no necesitas el historial completo del asunto.

La minimización no es un principio abstracto del RGPD (art. 5.1.c): es la forma más práctica de reducir el riesgo. Por cada dato que no introduces, hay un dato que no puede filtrarse, no puede usarse para entrenamiento, no puede aparecer en un incidente.

LA REGLA OPERATIVA

- Introduce el fragmento mínimo que necesita la tarea, nunca el documento entero.
- Si puedes anonimizar o pseudonimizar sin perder utilidad, hazlo.
- Si la tarea no requiere dato personal, no incluyas ninguno.

Menos dato es *menos exposición*.

ANTES DE CADA PROMPT

Checklist *previa* de uso

Aplícala antes de introducir cualquier contenido en una IA. Son menos de treinta segundos.

1

¿Sé en qué entorno estoy trabajando?

Confirma que la herramienta está en el entorno corporativo gobernado, con contrato de encargado del tratamiento activo. Si no lo sabes con certeza, consulta con IT.

2

¿He clasificado el dato que voy a introducir?

Categoría A, B o C. Si es C, para. Si es B, continúa solo en entorno gobernado y con el dato mínimo.

3

¿Estoy introduciendo más dato del necesario?

Recorta. Si puedes hacer la tarea con un fragmento, usa solo el fragmento. Elimina nombre y DNI si no son necesarios.

4

¿La salida va a salir del despacho o tiene efecto jurídico?

Si es un correo a cliente, un escrito o una propuesta, trátalo como borrador que exige revisión y validación antes de usar.

5

¿Tengo dudas sobre si esto es correcto?

Escala a DPO o compliance. No decidas solo sobre terreno incierto.

6

¿Voy a revisar y validar el resultado antes de usarlo?

Si la respuesta es no —por urgencia o por delegarlo a quien no revisará—, este no es el momento de usar la IA para esta tarea.

Por tipo de *dato*

Tipo de dato	Nivel	Entorno admitido	Control mínimo
Procedimientos y plantillas internas sin personas	**Bajo**	Cualquier entorno gobernado	Revisión del output
Datos personales de cliente (nombre, caso, situación)	**Medio**	Solo entorno gobernado con contrato de encargado	Minimización + revisión
Datos personales de terceros en el expediente	**Medio**	Solo entorno gobernado	Minimización + revisión
Datos económicos o financieros del cliente	**Medio-alto**	Solo entorno gobernado	Minimización + revisión + validación
Datos de salud, penales, ideología u otras categorías especiales	**Alto**	Consultar con DPO antes de cualquier uso	Validación previa obligatoria

Cómo leer el nivel

El nivel orienta la cautela, no sustituye el criterio. Cualquier caso que combine varias categorías, o que tengas dudas de clasificar, sube de nivel por defecto y se consulta. La regla 3 manda: ante duda regulatoria, se escala al DPO.

Sobre el entorno corporativo. Que una herramienta pertenezca a un proveedor conocido no garantiza por sí solo la protección del dato. Verifica con tu equipo de IT y con la documentación vigente del proveedor qué datos se tratan, con qué fines y bajo qué contrato.

Por tipo de *tarea*

Tarea	Nivel	Control recomendado
Resumir un hilo de correo interno sin datos de cliente	**Bajo**	Revisión del output
Triar y priorizar la bandeja de entrada	**Bajo-medio**	Solo fragmentos; sin expediente completo
Redactar borrador de comunicación interna	**Bajo**	Revisar antes de distribuir
Resumir o mapear un contrato con datos de partes	**Medio**	Entorno gobernado; minimizar; verificar hallazgos contra el original
Comparar versiones de un contrato	**Medio**	Entorno gobernado; verificar diferencias contra los originales
Borrador de acta de reunión con cliente	**Medio**	Transparencia/consentimiento previo; revisar atribuciones
Analizar datos de gestión interna (horas, asuntos)	**Medio**	Datos agregados; no analizar a personas para decidir sobre ellas sin compliance
Buscar o citar jurisprudencia o normativa	**Medio-alto**	Verificar toda cita contra la fuente; nunca usar sin verificar
Tratar datos de categoría especial (salud, penal)	**Alto**	Consultar con DPO antes de iniciar
Generar una decisión jurídica final o un dictamen	**No aplica**	La IA no decide; el abogado concluye, redacta y firma

CUANDO ALGO SALE MAL

Ante un *incidente*

Una exposición accidental de datos personales a una herramienta no autorizada puede constituir una violación de seguridad bajo el RGPD y activar obligaciones de notificación.

SEÑALES DE ALERTA

- Se introdujo un expediente o correo de cliente en una herramienta de consumo no autorizada.
- Se usó una herramienta sin verificar si hay contrato de encargado del tratamiento.
- La IA devolvió información que parece de otros usuarios o fuentes externas.
- Se envió a un cliente un documento generado con IA sin revisar, con un error material.

PASOS INMEDIATOS

1. No borrar ni alterar nada. Documenta qué herramienta, qué dato, cuándo y quién.
2. Comunica el incidente a tu DPO o responsable de protección de datos el mismo día.
3. No notifiques fuera ni avises al cliente por tu cuenta: esa decisión es del responsable del tratamiento y del DPO.

De la norma a la práctica

RGPD (UE 2016/679)

Base de licitud validada por tu DPO en cada caso de uso. Minimización (art. 5.1.c), plazos de conservación y contrato de encargado del tratamiento con el proveedor (art. 28) son exigencias directas. Sin ese contrato, el tratamiento probablemente carece de cobertura suficiente.

Reglamento de IA (UE 2024/1689)

Control humano sobre toda salida con efecto jurídico: la firma es del abogado. Transparencia frente al interesado cuando un sistema de IA interviene de forma relevante. Analizar a personas para decidir sobre ellas puede activar obligaciones adicionales: se consulta antes.

Palatino

EL SIGUIENTE PASO

Vosotros decidís. Nosotros *construimos*

Este marco te protege en el uso diario. Una cosa es que cada persona aplique las reglas por su cuenta; otra es que el despacho tenga un sistema que las incorpore por diseño: procesos definidos, controles integrados y criterio común. Esa es la diferencia entre depender de que cada uno se acuerde y tener una forma de trabajar que funciona aunque cambien las personas.

Menos de 8 semanas a producción. Del diagnóstico al primer proceso automatizado funcionando.

Ingenieros dedicados, sin rotación. El mismo equipo que diseña tu sistema lo construye.

100 % foco en el trabajo humano. Automatizamos lo repetitivo; el criterio jurídico sigue siendo del despacho.

Reserva tu diagnóstico de automatización

Una conversación sobre tu despacho y tus procesos. Identificamos los tres que más horas te devolverían y su nivel de riesgo. Sin presentaciones genéricas.

hola@palatino.ai

Construimos el futuro humano del trabajo.

PARA PROFUNDIZAR

Fuentes *oficiales*

Reglamento General de Protección de Datos

Reglamento (UE) 2016/679

eur-lex.europa.eu/eli/reg/2016/679/oj

Reglamento de Inteligencia Artificial

Reglamento (UE) 2024/1689

eur-lex.europa.eu/eli/reg/2024/1689/oj

Esta guía tiene carácter informativo y orientativo. No constituye asesoramiento jurídico ni sustituye la decisión de tu DPO o asesor especializado. No afirma comportamientos concretos de licencias de proveedores: verifícalos con tu equipo de IT y con la documentación vigente. Para la aplicación a situaciones concretas de tu despacho, consulta con compliance.

hola@palatino.ai