



Uso responsable y confidencial de la IA

Qué puede salir de tu escritorio, qué nunca, y cómo se documenta lo que hiciste

Esta es la sección que conviene imprimir y dejar a la vista. Las guías anteriores son técnica; esta es responsabilidad. La buena noticia es que no hay que aprender deberes nuevos: los que ya te obligaban siguen siendo los mismos, y esta guía solo los traduce al momento en que abres una herramienta y pegas un documento.

Sirve para cualquier persona que maneje información de terceros —abogados, despachos, áreas jurídicas, consultores, servidores públicos— y termina con dos entregables listos para copiar: una política interna de una página y una cláusula modelo para tu contrato de servicios.

Dato	Detalle
Serie	Justicia Inteligente · Guías prácticas de IA — guía 5 de 6
Para quién	Quien maneja información de terceros, con o sin formación jurídica
Complementa	La guía 4 desarrolla el método de verificación; esta, el régimen de la información
Advertencia	Es divulgación, no asesoría. Verifica la norma vigente en el Diario Oficial antes de aplicarla a un caso
Actualizada	Septiembre de 2026

1. Tres deberes que ya te obligaban

Antes de cualquier tecnicismo, la idea que ordena todo: **la inteligencia artificial no creó deberes nuevos, solo hizo más fácil incumplir los que ya existían.** Son tres y conviene tenerlos en ese orden.

Deber	Qué significa frente a una IA
Confidencialidad	Lo que te confiaron no sale de tu ámbito de control. Pegar un documento en una herramienta de terceros es sacarlo, aunque nadie lo lea del otro lado.
Protección de datos	Los datos personales que tratas no son tuyos: son de las personas. Su tratamiento necesita base, finalidad y medidas de seguridad, y eso no cambia porque el destino sea un modelo.
Veracidad y verificación	Lo que afirmas debe ser cierto y estar comprobado. Es el deber que produjo las sanciones documentadas en la guía 4.

Si una decisión te genera duda, la pregunta útil no es «¿esto está prohibido?», sino «¿podría explicar esta decisión, con estas tres palabras en la mano, delante de mi cliente o de un tribunal?».

2. El marco mexicano, en una página

El 20 de marzo de 2025 se publicó en el Diario Oficial de la Federación la nueva **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, junto con las leyes generales de transparencia y de datos en posesión de sujetos obligados. Con la desaparición del INAI, las funciones de autoridad garante pasaron a la Secretaría Anticorrupción y Buen Gobierno, y se homologaron reglas y procedimientos entre particulares y sujetos obligados.

Lo que le interesa a quien usa IA no es el organigrama, sino cómo aterrizan los principios de siempre.

Principio o deber	Cómo aterriza al usar una herramienta de IA
Finalidad	Los datos se tratan para lo que se recabaron. Si tu cliente te dio su expediente para defenderlo, esa es la finalidad: no incluye alimentar un sistema de terceros sin más.
Proporcionalidad	Solo los datos necesarios para esa finalidad. Subir el expediente completo cuando basta un fragmento es desproporcionado y, además, empeora el resultado.
Información	El aviso de privacidad debe reflejar lo que realmente haces. Si usas herramientas de IA en el tratamiento, ahí debe decirse.
Consentimiento	Los datos sensibles —salud, origen, creencias, datos de menores, entre otros— exigen un estándar reforzado. La regla práctica: no salen.
Seguridad y confidencialidad	Medidas razonables contra accesos no autorizados. Una cuenta personal compartida por todo el despacho no las cumple.
Responsabilidad	Respondes por el tratamiento aunque lo haga un tercero por ti. El proveedor de IA no asume tu responsabilidad; la conservas íntegra.

A esto se suman los criterios judiciales mexicanos ya comentados: los cuatro principios mínimos del Segundo Tribunal Colegiado en Materia Civil del Segundo Circuito —proporcionalidad y seguridad, protección de datos, transparencia y explicabilidad, supervisión humana— y, en materia penal, el desarrollo del **amparo directo 241/2025** del Primer Tribunal Colegiado en Materia Penal del Segundo Circuito sobre la diferencia entre IA auxiliar y IA sustituta, y sobre el deber de declarar el uso, la fase y la metodología.

3. Qué pasa realmente con lo que escribes

Antes de decidir qué subir conviene saber a dónde va. Tres preguntas resuelven el noventa por ciento: quién puede leerlo, cuánto tiempo se conserva, y si sirve para entrenar modelos.

Tipo de cuenta	Qué aplica
Individual (Free, Pro, Max)	Tú decides si tus conversaciones se usan para entrenar modelos nuevos. Desactivado, se conserva el periodo de treinta días; activado, la retención sube a cinco años. Se configura en Configuración → Privacidad .
De trabajo (Team, Enterprise)	Quedan fuera de ese entrenamiento, con administración central, control de accesos y, en Enterprise, retención personalizada y registros de auditoría.
Educativa y gubernamental	Claude for Education y Claude Gov también quedan fuera del entrenamiento con datos de usuario.

Las demás plataformas tienen ajustes equivalentes con otros nombres: en ChatGPT, la opción de mejorar el modelo para todos, dentro de controles de datos; en Gemini, la actividad de aplicaciones y su periodo de conservación. La conclusión operativa es la misma en todas: **el ajuste existe, viene con una decisión pendiente, y revisarlo toma dos minutos una sola vez.**

ALTO AHÍ

Desactivar el entrenamiento no convierte a la herramienta en un espacio confidencial. Sigue siendo un tercero que procesa y conserva información por un tiempo. Es una medida de mitigación, no una autorización para subir lo que sea.

4. El semáforo del dato

La decisión de qué subir no se toma documento por documento, se toma una vez y se convierte en reflejo. Este es el criterio.

EL SEMÁFORO



Qué sube, cómo sube y qué no sube nunca

De abajo hacia arriba aumenta la exposición. La franja de en medio es donde ocurre casi todo el trabajo real, y es la que hay que volver automática.

SUBE TAL CUAL

sin riesgo

Material público

Normas, criterios publicados, doctrina

Texto propio

Tus formatos y tus escritos modelo

Supuestos hipotéticos

Casos que tú inventas para practicar

SUBE ANONIMIZADO

la franja de trabajo

Resoluciones y escritos

Sin nombres, domicilios ni expediente

Contratos

Partes por su posición, montos redondeados

Declaraciones

Testigo uno, testigo dos

SOLO CON BASE

autorización y cuenta adecuada

Datos identificables necesarios

Cuando la tarea no funciona sin ellos

Volumen de expedientes

Cuenta de equipo y acceso mínimo

NO SUBE

ni anonimizado

Datos sensibles

Salud, creencias, origen, biométricos

Datos de menores

Incluidas iniciales y edades exactas

Identificadores oficiales

CURP, RFC, cuentas, identificaciones

Material bajo reserva

Y lo que tu institución prohíba

LA REGLA La responsabilidad no se transfiere al proveedor: viaja contigo en todas las franjas.

5. Anonimizar bien: cuatro reglas

Anonimizar no es tachar nombres. Es asegurarse de que el documento ya no permita llegar a la persona.

1. **Sustituye de forma consistente.** El actor es siempre «el actor», no a veces «A.» y a veces su inicial real. La inconsistencia reintroduce identificadores.
2. **Cuida las combinaciones.** Un dato inocuo más otro identifica: profesión, municipio pequeño, fecha de un hecho y número de hijos pueden señalar a una sola persona aunque no haya un solo nombre.

3. **Revisa lo que no es texto.** Encabezados, sellos, metadatos del archivo, nombres de archivo y firmas escaneadas llevan datos que nadie revisó. Renombra el archivo antes de subirlo.
4. **Haz la prueba de reidentificación.** Léelo como si fueras un tercero curioso: ¿podrías averiguar de quién se trata con lo que quedó? Si la respuesta es sí, falta trabajo.

Antes de trabajar, revisa este documento y dime qué datos podrían identificar a una persona, incluyendo combinaciones de datos que por separado parecen inocuos. No los uses en tu respuesta: solo enlista dónde están y con qué los sustituirías.

Ese prompt se corre sobre el documento ya despersonalizado por ti, como segunda revisión. No al revés: la primera pasada la haces tú, porque subir para que te diga qué anonimizar ya es haberlo subido.

6. Explicabilidad: la frase que debes poder escribir

La transparencia dejó de ser una virtud opcional. En el criterio penal del Segundo Circuito aparece como deber de declarar el uso de la herramienta, la fase en que intervino y la metodología seguida. Trasladado a cualquier despacho o área jurídica, significa que **debes poder escribir una frase**, en cualquier momento, sobre cualquier trabajo que entregaste.

En este asunto se utilizó [herramienta] durante la fase de [análisis / organización del material / redacción del borrador].
El material se cargó [anonimizado / despersonalizado].
La revisión de citas, hechos y razonamiento la realizó [nombre], y el resultado se auditó contra [lista de verificación].

Dónde vive esa frase

- **Nota interna por asunto.** Dos renglones en tu expediente de trabajo. Es el registro que te salva la conversación incómoda.
- **Frente al cliente.** En el contrato de servicios, por adelantado, no cuando ya pasó algo.
- **Frente al tribunal.** Si te lo preguntan, la respuesta debe existir antes de la pregunta.

UN MATIZ IMPORTANTE

Declarar el uso no equivale a confesar una debilidad. Un escrito verificado pieza por pieza, con su metodología explicada, es más defendible que uno del que nadie sabe cómo se hizo. La opacidad es lo que genera sospecha, no la herramienta.

7. Los riesgos propios del modo agéntico

Cuando la herramienta deja de conversar y empieza a actuar sobre carpetas y servicios conectados, aparecen riesgos que no existen en el chat.

Riesgo	Defensa práctica
Inyección de prompt	Un documento, un correo o una página pueden contener instrucciones ocultas dirigidas al agente. Requiere dos condiciones: que lea contenido fuera de tu frontera de confianza y que pueda ejecutar acciones dañinas. Ataca las dos: conecta solo la carpeta del asunto y usa aprobación manual con material de contraparte o de origen desconocido.
Exceso de acceso	Conecta la carpeta del asunto, nunca el disco completo, y jamás carpetas con credenciales, información financiera o documentación de otros clientes.
Tareas programadas	Corren sin nadie mirando. Úsalas solo para material propio y revisa sus resultados con la misma severidad que los demás.
Conectores	Cada integración amplía la superficie. Autoriza las que necesitas para la tarea y revoca las que dejaste de usar.
Vigilancia del patrón	Más útil que auditar cada acción aislada: pregúntate si está haciendo lo que le pediste. Las desviaciones se notan en el patrón, no en el detalle.

8. Si ya subiste algo que no debías

Pasa, y lo peor que se puede hacer es nada. El protocolo es corto.

1. **Contén.** No sigas trabajando en ese hilo ni generes más material derivado.
2. **Elimina.** Borra la conversación y el archivo cargado. Revisa también la memoria de la herramienta y borra lo que haya retenido.

3. **Verifica los ajustes.** Comprueba si el entrenamiento estaba activado, porque de eso depende el periodo de retención aplicable.
4. **Documenta.** Anota qué se subió, cuándo, en qué cuenta y qué hiciste. Sin ese registro no puedes evaluar nada después.
5. **Evalúa el deber de informar.** Si hubo datos personales de terceros involucrados, valora si procede notificar al titular o a quien corresponda conforme a la normativa aplicable y a tu política interna.
6. **Corrige la causa.** Casi siempre es una de tres: prisa, ausencia de protocolo, o una cuenta equivocada. Arregla esa.

9. Tu política interna, en una página

Este es el verdadero entregable de la guía. Cópialo, adáptalo a tu realidad y compártelo con tu equipo. Si trabajas solo, sigue sirviendo: es el documento que te obliga a ti.

POLÍTICA DE USO DE INTELIGENCIA ARTIFICIAL

[Nombre del despacho o área] · [Fecha]

1. HERRAMIENTAS AUTORIZADAS

Solo las de esta lista, en las cuentas del despacho:

[herramienta / tipo de cuenta / quién la administra]

2. QUÉ NO SE SUBE NUNCA

Datos sensibles, datos de menores, identificadores oficiales, material bajo reserva y expedientes completos sin anonimizar.

3. QUÉ SE SUBE ANONIMIZADO

Todo lo demás que provenga de un asunto: nombres por posición procesal, sin domicilios, sin RFC ni CURP, sin número de expediente y con el archivo renombrado.

4. AUTORIZACIÓN DEL CLIENTE

Se recaba en el contrato de servicios, por adelantado.

5. VERIFICACIÓN OBLIGATORIA

Ninguna cita entra a un escrito sin abrirse en su fuente oficial. Cada afirmación de hecho remite a su constancia. Responsable de la revisión final: [nombre o cargo].

6. REGISTRO

Cada asunto lleva una nota interna: qué herramienta se usó, en qué fase y quién revisó el resultado.

7. LO QUE NO SE DELEGA

La estrategia, la ponderación de la prueba, el consejo al cliente y la decisión de presentar.

8. INCIDENTES

Se reportan a [nombre o cargo] el mismo día, por escrito.

Cláusula modelo para el contrato de servicios

Redacción orientativa; ajústala a tu práctica y a la normativa aplicable antes de usarla.

USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL. El prestador podrá auxiliarse de herramientas de inteligencia artificial en las fases de organización de material, análisis y elaboración de borradores, bajo las siguientes condiciones: (i) la información del cliente se tratará de forma despersonalizada siempre que la tarea lo permita; (ii) no se emplearán datos personales sensibles ni de menores; (iii) toda cita, dato y afirmación será verificada por el prestador en su fuente antes de utilizarse; (iv) la estrategia, la valoración jurídica y la decisión sobre los escritos que se presenten corresponden exclusivamente al prestador, quien conserva íntegra su responsabilidad profesional; y (v) el prestador informará al cliente, a solicitud de éste, qué herramienta se utilizó y en qué fase intervino.

10. Antes de cargar cualquier cosa

- ☐ Revisé el ajuste de entrenamiento y retención de mi cuenta.
- ☐ Estoy en la cuenta correcta: la del despacho, no la personal.
- ☐ El documento está anonimizado y pasó la prueba de reidentificación.
- ☐ Renombré el archivo y revisé encabezados, sellos y metadatos.
- ☐ No hay datos sensibles, de menores ni identificadores oficiales.
- ☐ Subo solo lo que la tarea necesita, no el expediente completo.
- ☐ Tengo la autorización del cliente, o no la necesito porque está despersonalizado.
- ☐ Puedo escribir la frase de explicabilidad sobre este trabajo.

La confidencialidad no se pierde por usar una herramienta nueva: se pierde por no haber decidido antes qué podía salir de tu escritorio.

11. La serie y el contacto

Guía	Título	De qué trata
1	Primeros pasos con la inteligencia artificial	De cero a tu primera sesión útil.
2	Guía práctica de Claude	Planes, modelos, proyectos, memoria, Cowork y habilidades.
3	Cómo redactar mejores instrucciones	Describir bien, verificar y construir tu biblioteca.
4	IA para profesionales del derecho	Riesgo por tarea, verificación en tres capas y explicabilidad.
5	Uso responsable y confidencial de la IA	Esta guía: deberes, marco de datos personales, semáforo del dato y política interna.
6	Fluidez en IA	Ruta de aprendizaje con el marco de las cuatro D y los programas oficiales.

Si algo de esta guía te sirvió, compártela con tu equipo. El usuario es el mismo en las cuatro redes: **@soyangelolvera** —Instagram, Facebook, TikTok y X—.

Correo: soyangelolveravillafan@gmail.com · **Trayectoria y publicaciones:** www.soyangelolvera.com

Puedes usar esta guía, adaptarla y compartirla con tu equipo. La referencia a la legislación mexicana corresponde a la publicada el 20 de marzo de 2025 y a la información pública disponible en septiembre de 2026; verifica el texto vigente en el Diario Oficial de la Federación antes de aplicarlo a un caso concreto. Este material es divulgación y no constituye asesoría jurídica ni postura institucional del órgano en el que laboro.

La justicia que no se entiende, no puede exigirse ni defenderse — y eso empieza por explicarla bien.

Ángel Olvera Villafán · Justicia Inteligente

@soyangelolvera — Instagram · Facebook · TikTok · X

soyangelolveravillafan@gmail.com · www.soyangelolvera.com

