

GUÍA GRATUITA

🕒 6 min de lectura

IA sin miedo: privacidad y seguridad para principiantes

Qué es seguro compartir, qué no, y qué configurar hoy para trabajar con tranquilidad

01

Semáforo de datos

02

Configuración en 20 minutos

03

Política para tu equipo



Tienes razón en tener dudas. Si vas a pegar información de tu negocio en una herramienta de IA, lo responsable es preguntarte a dónde va esa información. Es una pregunta sana, no paranoia.

Pero hay dos extremos que no ayudan. Uno es no usar IA por miedo a todo. El otro es pegar cualquier cosa sin pensar. Esta guía busca el punto medio: entender qué pasa con lo que escribes, decidir qué compartes y dejar configurada tu herramienta en unos veinte minutos.

Primero, lo que no está pasando

Un mito común: “la IA me está escuchando o me espía”. Las herramientas de chat trabajan con lo que tú les escribes, les subes o les autorizas a leer. No es magia ni vigilancia oculta. El riesgo real es más simple y más controlable: **lo que compartes puede quedar guardado en los servidores de la empresa que da el servicio**, bajo sus propias políticas.

Por eso la pregunta útil no es “¿me espía?”, sino “¿qué le estoy dando y qué hace la empresa con eso?”.

Qué pasa cuando envías un mensaje

1. Tu texto, tus archivos y tus imágenes viajan a los servidores del proveedor para generar la respuesta.
2. Según tu plan y tu configuración, esa conversación puede guardarse en tu historial y, en algunos casos, usarse para mejorar los modelos.
3. Los planes para empresas suelen tener condiciones distintas a los planes personales, pero eso depende de cada proveedor y cada contrato.

IMPORTANTE

Las políticas cambian. Lo que escribo aquí es el criterio general. Antes de compartir información delicada, lee la política de privacidad vigente de la herramienta que usas y, si es para tu empresa, revisa qué ofrece su plan de negocios.

El semáforo de la información

Una forma simple de decidir qué pegar en una herramienta de IA es clasificar la información en tres colores.

Color	Qué es	Ejemplos	Qué hacer
Verde	Información pública o genérica	Textos que ya publicaste, ideas, borradores, preguntas generales	Pégala con libertad
Amarillo	Información interna del negocio, sin datos personales	Procesos, listas de precios, planes, minutas	Úsala revisando la configuración de tu herramienta
Rojo	Información personal, financiera o confidencial	Contraseñas, tarjetas, datos bancarios, expedientes de clientes o empleados, contratos con nombres, información médica	No la compartas, o anonimízala primero



Cómo anonimizar antes de pegar

Muchas veces no necesitas que la IA vea los datos reales: solo necesitas que entienda la estructura. Sustituye los datos identificables por etiquetas.

Antes	Después
Juan Pérez, RFC XXXX, debe \$84,000 desde marzo	Cliente A, debe una cantidad importante desde hace tres meses
Contrato con Grupo Ejemplo S.A. de C.V.	Contrato con Empresa X
Correo de mari@empresa.com	Correo de una clienta

PROMPT PARA ANONIMIZAR UN TEXTO

Voy a pegar un texto. Sustituye todos los nombres de personas, empresas, teléfonos, correos, direcciones y cifras exactas por etiquetas genéricas (Persona A, Empresa X, Monto 1). No cambies nada más. Devuélveme también una tabla con qué etiqueta reemplazó a qué dato, para que yo pueda revertirlo.

Ojo: si usas la propia IA para anonimizar, ya le estás enviando el dato original. Para información realmente delicada, es mejor anonimizar tú mismo, con buscar y reemplazar, antes de pegar.



Configura tu herramienta en 20 minutos

Los nombres exactos de los menús cambian entre ChatGPT, Claude y Gemini, y cambian con el tiempo. Busca en la configuración de tu cuenta las secciones que se llaman parecido a estas:

Qué buscar	Para qué sirve	Qué decidir
Privacidad o datos (“mejorar el modelo”, “entrenamiento”)	Controla si tus conversaciones pueden usarse para mejorar el sistema	Actívalo o desactívalo conscientemente. Si trabajas con información de clientes, considera desactivarlo
Historial de conversaciones	Determina qué se guarda y por cuánto tiempo	Borra lo que no necesites conservar
Chat temporal o modo incógnito	Conversaciones que no se guardan en tu historial ni alimentan la memoria	Úsalo para temas más delicados
Memoria	Lo que la herramienta recuerda de ti entre conversaciones	Revisa qué guardó y elimina lo que no quieras
Conectores y aplicaciones	Permisos para leer tu correo, archivos o calendario	Dale el permiso mínimo necesario: lectura si solo necesita leer
Sesiones y dispositivos	Dónde tienes iniciada la cuenta	Cierra sesiones que no reconozcas y activa la verificación en dos pasos



Los conectores y agentes: más poder, más cuidado

Cuando conectas la IA a tu correo, tus archivos o tus anuncios, deja de ser solo un chat y puede actuar. Eso es muy útil, y también exige más criterio.

- **Da el permiso mínimo.** Si solo necesita leer, no le des permiso de enviar.

- **Prefiere borradores a envíos.** Que prepare, y tú aprietas el botón.
- **Revisa antes de aprobar acciones que mueven dinero o salen a un cliente.**
- **Desconecta lo que no uses.** Un permiso olvidado sigue abierto.

Otras amenazas que conviene conocer



Suplantación con voz o video generados

Hoy es posible imitar una voz o un rostro con pocos segundos de material. Si alguien te llama pidiendo una transferencia urgente, aunque suene idéntico a un familiar o a un socio, verifica por otro canal. Una medida muy práctica: acordar una palabra clave con tu familia y con tu equipo de finanzas que solo ustedes conozcan.

Correos y mensajes cada vez más convincentes

La IA también ayuda a quien escribe fraudes, así que los errores de ortografía ya no son una señal confiable. Fíjate en lo que sí es: urgencia inusual, solicitud de datos o pagos, y enlaces o cuentas que no coinciden con las de siempre.

Textos de fuentes no confiables

Si le pides a un agente que lea páginas, correos o documentos de terceros, ese contenido puede traer instrucciones escondidas dirigidas a la IA. Es una técnica conocida como inyección de instrucciones. Si la herramienta tiene permiso de actuar, no le pidas ejecutar acciones importantes basándose en contenido que no controlas sin revisar antes.



Política mínima de IA para tu equipo

Si tienes colaboradores, tiene más sentido poner por escrito lo básico que confiar en que cada quien lo adivine. Esta plantilla cabe en una hoja:

PLANTILLA (edítala según tu empresa)

1. Herramientas autorizadas: _____.
2. Nunca se comparte: contraseñas, datos bancarios, expedientes de clientes o empleados, contratos con datos identificables.
3. Antes de pegar información de clientes: se anonimiza.
4. Todo lo que la IA genere y salga a un cliente lo revisa una persona.
5. Cuentas de trabajo para uso laboral; cuentas personales para uso personal.
6. Si tienes dudas sobre si algo se puede compartir, pregunta a _____ antes.

Checklist de 10 minutos

1. Revisé si mis conversaciones se usan para entrenar el modelo y decidí conscientemente.
2. Borré del historial lo que no necesito.
3. Revisé qué recuerda la memoria de mi herramienta.
4. Repasé los conectores que tengo activos y quité los que no uso.
5. Activé la verificación en dos pasos en mi cuenta.
6. Acordé una palabra clave con mi familia y mi equipo.
7. Sé qué información está en rojo y no la pego.

Con eso cubres lo más importante. El resto es criterio, y el criterio se construye con la práctica.

IA sin miedo, en una captura

- 1** **El riesgo real:** lo que compartes queda en servidores ajenos, con sus propias políticas.
- 2** **Semáforo.** Verde: público. Amarillo: interno sin datos personales. Rojo: no lo compartas, o anonimízalo.
- 3** **Anonimiza** nombres, correos y cifras exactas antes de pegar.
- 4** **Configura:** entrenamiento, historial, memoria, conectores y verificación en dos pasos.
- 5** **Permisos mínimos.** Que prepare borradores; tú envías.
- 6** **Verifica por otro canal** cualquier pedido urgente de dinero, aunque la voz suene igual. Acuerda una palabra clave.
- 7** **Pon por escrito** una política de una hoja para tu equipo.

Usar IA con criterio es más seguro que no usarla o usarla a ciegas.

SÍGUEME PARA MÁS GUÍAS GRATIS

@luis.rene.ia luisrene.com

Luis RenéIA