Qué NO pegar en la IA y cómo anonimizar en 2 minutos

Semáforo de datos para usar IA sin exponer a tus clientes ni a tu empresa: qué puedes pegar, qué debes anonimizar antes y qué nunca se comparte.

Consulta este semáforo antes de pegar un texto, una tabla o un archivo en cualquier asistente de IA. Te toma dos minutos y evita exponer a tus clientes, a tu equipo o a ti.

El semáforo de datos

Color	Ejemplos	Qué haces
Verde	Dudas generales, textos sin nombres, información ya pública	Pégalo
Amarillo	Nombres, teléfonos, correos, ventas, contratos, calificaciones	Anonimiza antes
Rojo	Contraseñas, NIP, CVV, e.firma, INE, expedientes médicos, datos de menores	No lo pegues

Si dudas entre dos colores, elige el más estricto.

Anonimiza en 2 minutos

1. **Quita lo que no hace falta.** Borra columnas o párrafos que la IA no necesita para ayudarte.
2. **Sustituye identificadores.** Cambia nombres por etiquetas: Cliente A, Empleado 1, Proveedor X.
3. **Generaliza lo delicado.** «Colonia Del Valle» pasa a «zona sur»; «$48,350» pasa a «cerca de $50,000», si el dato exacto no importa.
4. **Elimina claves únicas.** RFC, CURP, número de cuenta, placas, folios, direcciones y teléfonos.
5. **Guarda tu tabla de equivalencias** fuera del chat para regresar los nombres reales al final.

Antes y después

```
Antes: María Fernanda López Ruiz (RFC LORM850312XX0) debe $12,400 de la
factura 884, vencida el 3 de marzo, y no contesta el WhatsApp 55 1234 5678.

Después: Cliente A debe cerca de $12,000 de una factura vencida hace más de
un mes y no responde mensajes.
```

La IA te ayuda igual a redactar el recordatorio de pago, y la persona real nunca salió de tu archivo.

Prompt de apoyo

```
Voy a compartirte un caso con datos sustituidos por etiquetas (Cliente A,
Empleado 1).
Conserva esas etiquetas tal cual en tu respuesta y no intentes adivinar a
quién corresponden.
Mi solicitud: [qué necesitas].
```

Revisa también la herramienta

- ☐ Sé si estoy en una cuenta personal o en la que autoriza mi trabajo.
- ☐ Revisé en la configuración si mis conversaciones se usan para entrenar el modelo y si puedo desactivarlo.
- ☐ Sé cómo borrar el historial o abrir un chat temporal.
- ☐ El archivo que subo no trae hojas ocultas, comentarios ni columnas con datos de más.

Errores comunes

- Creer que «nadie lo va a ver»: lo que pegas sale de tu control.
- Quitar el nombre y dejar el teléfono, el RFC o la dirección, que identifican igual.
- Subir el archivo completo cuando bastaban diez renglones.
- Olvidar que los datos de clientes y empleados siguen siendo tu responsabilidad: en México los protege la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, uses o no IA.

¿Quieres dominar el tema? El curso «Seguridad, privacidad y ética de la IA» lo enseña paso a paso, con ejercicios y certificado: https://klaroia.com/cursos/seguridad-etica-ia