

Qué nunca pegar en una IA: reglas de privacidad y datos sensibles

Guía rápida para operar con IA sin exponer información confidencial de tu negocio o clientes

Lo riesgoso al adoptar herramientas de inteligencia artificial no es usar la tecnología: **es qué información se le proporciona**. Según la herramienta, el plan y la configuración, las conversaciones pueden quedar registradas o emplearse para entrenamiento. Esta guía resume los 7 tipos de datos prohibidos y las reglas de oro para proteger tu negocio.

Tabla de datos prohibidos: qué nunca ingresar

Tipo de dato	Ejemplos frecuentes	Qué hacer en su lugar
Contraseñas y accesos	Claves, tokens de API, códigos 2FA, credenciales de sistemas	Nunca. No existe versión segura ni uso justificado.
Datos de pago y bancarios	Números de tarjeta, CVV, cuentas, CBU/CVU de personas	Usar referencias genéricas («importe X», «cuenta bancaria»).
Identidad personal (DNI/CUIT)	DNI, pasaportes, identificaciones tributarias directas	Reemplazar por roles: «Cliente A», «Proveedor 1».
Datos personales de contacto	Nombre completo + teléfono personal + dirección o correo	Anonimizar: conservar solo rubro, tipo de cliente y situación.
Datos de salud o sensibles	Diagnósticos, tratamientos, información médica particular	No incluir. Describir la situación administrativa general.
Confidencial de terceros	Contratos bajo NDA, tarifas reservadas, datos de proveedores	Resumir sin nombres ni importes que permitan identificar.
Finanzas del negocio	Balances completos, extractos con saldo, nómina salarial	Utilizar porcentajes, proporciones o importes redondeados.

Las 7 reglas de oro de privacidad en IA

- 1. Si no lo publicarías en un cartel, no lo pegues.** Trate cada consulta con una IA como si pudiera ser leída por un tercero en un registro de auditoría.
- 2. Anonimizar siempre por defecto.** Reemplazá nombres propios por roles («el cliente», «la aseguradora», «el comprador») y quitá números de identificación antes de enviar el prompt.
- 3. Revisar la configuración de privacidad.** En cada herramienta de IA, desactivá la opción de "compartir datos para entrenamiento de modelos" cuando el plan lo permita.
- 4. Separar cuentas personales de cuentas de trabajo.** Operá con cuentas corporativas dedicadas, contraseñas robustas y autenticación en dos factores (2FA).
- 5. Principio de mínimo privilegio (no conectar a todo).** Si conectás un asistente a correo o archivos, dale acceso únicamente a la carpeta o buzón indispensable.
- 6. La IA afirma con seguridad cosas que son falsas.** Verificá siempre números, nombres de leyes, citas y cálculos antes de tomar decisiones operativas.
- 7. Ante la duda, tratarlo como confidencial.** Si dudás de si un dato califica como sensible, aplícale el nivel máximo de protección.

Las 3 preguntas de control antes de presionar Enviar

1. ¿Este texto permite identificar a una persona, a un cliente o a una cuenta específica?
2. ¿Tengo autorización explícita para procesar esta información en una herramienta externa?
3. ¿Qué consecuencia tendría para el negocio si este texto fuera público mañana?

Si alguna respuesta genera incertidumbre, anonimizá los datos o no utilices la IA para ese paso.

Siguiente paso

Descargá la guía y plantilla de cinco preguntas de gobernanza antes de darle acceso a un agente en:
kalkoralabs.com/guia