ENTIENDE. COMPRUEBA. MEJORA.

¿Qué información no debes introducir en herramientas públicas de IA?

No introduzcas información sensible: datos personales, contratos, información de clientes, contraseñas o código privado. El NCSC del Reino Unido recuerda que lo que escribes en una herramienta pública es visible para su proveedor, que puede almacenarlo y usarlo para desarrollar futuros modelos.



Una guía para pasar a la acción

Explicaciones claras, un ejemplo ficticio y una hoja para organizar tus próximas tres acciones.

Consulta la versión web y sus actualizaciones ↗

¿Qué información no debes introducir en herramientas públicas de IA?

01 / COMPRENDER

Qué conviene dejar fuera

- Datos personales de clientes o de compañeros.
- Contratos, ofertas y otra información confidencial.
- Contraseñas, claves y cualquier otra credencial.
- Código y configuraciones privadas.
- Datos financieros que no sean públicos.

02 / COMPRENDER

Quitar un nombre no siempre basta

El resto del texto puede seguir revelando de quién o de qué se trata. Un contrato sin el nombre del cliente sigue teniendo sus condiciones, sus importes y sus fechas.

03 / COMPRENDER

Qué puede hacer una empresa

- Publica qué herramientas están aprobadas y para qué.
- Explica qué información se puede usar en cada una.
- Antes de aprobarlas, revisa sus condiciones: qué conservan, durante cuánto tiempo y para qué lo usan.
- Forma a tu equipo con ejemplos de su trabajo diario.
- Pide que alguien revise lo que produce la herramienta antes de usarlo.

DEL CONOCIMIENTO A LA PRÁCTICA

Llévalo a tu empresa

EJEMPLO FICTICIO

Pedir ayuda sin pegar un contrato real

Una persona quiere resumir un contrato de un cliente con una herramienta pública de IA. En lugar de pegarlo entero, puede pedir una estructura de resumen usando un ejemplo ficticio. Si necesita analizar datos reales, debe usar un servicio y un procedimiento aprobados por su empresa.

Eliminar el nombre no garantiza que el documento deje de identificar al cliente. Importes, fechas y detalles de un proyecto también pueden revelar información.

01

Hoy

Define qué no se comparte

Aclara qué hacer con datos de clientes, contraseñas, código privado, contratos y documentos internos. Da ejemplos que el equipo pueda reconocer.

02

Esta semana

Acuerda herramientas y usos

Revisa las condiciones del servicio, los accesos y cómo trata la información. Una cuenta de pago no basta, por sí sola, para autorizar cualquier dato.

03

Antes de usar la respuesta

Comprueba el resultado

Contrasta hechos, cifras y fuentes. Una respuesta convincente puede contener errores. Mantén una revisión humana cuando afecte a clientes o decisiones de la empresa.

Qué conviene conservar

Una lista breve de herramientas y usos aprobados, ejemplos de información que no debe introducirse y un canal para consultar dudas o comunicar una exposición accidental.

TU HOJA DE TRABAJO

Tres acciones. Un siguiente paso.

Completa esta hoja con tu equipo. Define cómo comprobaréis cada mejora. No anotes contraseñas, claves ni información confidencial.

01 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

02 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

03 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

Preguntas frecuentes

¿Las versiones de pago para empresas son más seguras?

Pueden ofrecer más garantías sobre el uso de tus datos, pero depende del contrato. Compruébalo antes de autorizarlas.

¿Puedo fiarme de lo que responde?

No sin comprobarlo. El NCSC advierte de que estas herramientas pueden equivocarse e inventar datos, aunque suenen seguras.

Fuentes y siguiente paso

- NCSC (Reino Unido): ChatGPT and large language models: what's the risk? ↗

El uso responsable de la IA es uno de los temas de la evaluación de conocimientos. Ver Evaleris Equipo ↗

Información general. No es una auditoría, una certificación ni una garantía de seguridad. Ejemplos ficticios. Edición: 5 de noviembre de 2026.