Inteligencia artificial local

El despliegue de sistemas de inteligencia artificial (IA) en entornos sensibles —como la administración pública, la sanidad o la defensa— plantea un reto clave: **proteger la seguridad, confidencialidad y control de los datos utilizados y generados**. En este contexto, el uso de una **IA local o en entorno controlado (on-premise)** emerge como una solución estratégica frente a los modelos en la nube de proveedores externos.

A diferencia de las soluciones basadas en servidores remotos, una IA local se ejecuta **dentro de la infraestructura propia de la organización**, lo que **minimiza los riesgos de fuga de información, accesos no autorizados o exposición a jurisdicciones extranjeras**. Este enfoque permite que los datos sensibles —como contratos, historiales, patrones de comportamiento o información personal— **no salgan del entorno protegido**, reforzando la soberanía digital y el cumplimiento normativo (por ejemplo, el RGPD en Europa).

Además, la IA local ofrece **mayor trazabilidad y control del ciclo de vida del algoritmo**, permitiendo auditar sus decisiones, evitar conexiones externas no deseadas y aplicar políticas personalizadas de seguridad, cifrado y respaldo. Esto resulta especialmente valioso en sistemas donde la transparencia, la fiabilidad y la rendición de cuentas son críticas.

Aunque su implementación puede requerir una mayor inversión inicial en infraestructura y personal técnico, el modelo local proporciona **una barrera adicional frente a amenazas externas y una base sólida para el desarrollo de sistemas éticos, auditables y responsables**.