



Ciberseguridad para la **Inteligencia Artificial**

Adopte la IA con control: gobierno, seguridad técnica y cumplimiento normativo en un mismo equipo.

La IA ya está en su empresa. ¿Y su seguridad?

La inteligencia artificial ha entrado en las organizaciones más rápido que cualquier tecnología anterior: en los navegadores, en el correo, en el software de siempre y en las aplicaciones que se desarrollan para clientes. Con ella han llegado riesgos nuevos que los controles tradicionales no siempre ven.

43%

de las organizaciones que sufrieron una brecha registraron un incidente de Shadow AI (20% un año antes).

1 de 4

brechas maliciosas ya utiliza la IA como arma.

2 de 3

organizaciones afectadas no tenían un gobierno de IA capaz de detectar la Shadow AI.

Fuente: IBM y Ponemon Institute, Cost of a Data Breach Report 2026.



Shadow AI

Herramientas de IA usadas sin aprobación, con cuentas personales y fuera del control de la organización.



Fuga de información

Datos personales, contratos o código introducidos en prompts y documentos que salen de la empresa.



Manipulación de la IA

Chatbots y agentes que pueden ser manipulados mediante inyección de instrucciones o abusar de sus permisos.



Proveedores de IA

Modelos y servicios de terceros que tratan sus datos sin una evaluación técnica ni contractual suficiente.



Cumplimiento normativo

El AI Act, el RGPD y, en sectores regulados, DORA exigen saber qué IA se utiliza, con qué datos y con qué riesgos.

Del uso descontrolado a una IA segura y auditable

Combinamos la visión normativa con la técnica: el mismo equipo que diseña el marco de gobierno pone a prueba la seguridad real de sus sistemas de IA.

01

Diagnóstico de Shadow AI

Descubrimos qué herramientas de IA se usan realmente, con qué datos y en qué cuentas, y priorizamos los riesgos.

Inventario de uso

Mapa de riesgos

02

Gobierno de IA

Inventario y clasificación de sistemas, políticas, roles y controles alineados con ISO/IEC 42001 y el AI Act.

ISO/IEC 42001

AI Act

03

AI Red Teaming

Atacamos de forma controlada sus chatbots, copilotos y agentes para encontrar fallos antes que un atacante.

OWASP Top 10 LLM

Pentesting

04

Proveedores de IA

Evaluación técnica y contractual de los proveedores de IA que acceden a sus datos o a sus sistemas.

TPRM

DORA

05

Formación en IA

Programas prácticos para la plantilla y la dirección sobre el uso seguro de la IA, en línea con la obligación de alfabetización del AI Act.

Plantilla

Comité de Dirección

AI Act

Un recorrido en cuatro fases

01

Descubrir

Qué IA se usa, quién la usa y con qué datos.

02

Evaluar

Riesgos de cada uso, de cada proveedor y del marco normativo aplicable.

03

Proteger

Controles técnicos y pruebas de seguridad sobre los sistemas de IA.

04

Gobernar

Políticas, roles y seguimiento continuo para escalar la IA con seguridad.

POR QUÉ FORVIS MAZARS

Un solo equipo

Del marco de gobierno a las pruebas de intrusión, sin perder el hilo entre ambos.

Sectores regulados

Trabajamos con entidades financieras y aseguradoras sujetas a DORA, NIS2 y RGPD.

Visión práctica

Entregables accionables y priorizados, pensados para el Comité de Dirección y para los equipos técnicos.

La IA ya forma parte de su negocio.
Hablemos de cómo protegerla.

Contactos

Luis Reinoso

Director de Consultoría Tecnológica y Ciberseguridad

luis.reinoso@forvismazars.com

Forvis Mazars es la marca de la red Forvis Mazars Global (Forvis Mazars Global Limited), una red mundial de servicios profesionales. La red opera bajo una única marca en todo el mundo, con sólo dos miembros: Forvis Mazars, LLP en Estados Unidos y Forvis Mazars Group SC, una asociación internacional integrada que opera en más de 100 países y territorios.

Las entidades de la red Forvis Mazars en España prestan servicios de auditoría & assurance, asesoramiento fiscal, legal, financiero, consultoría, outsourcing y sostenibilidad a través de más de 900 profesionales en 8 oficinas.

Visita forvismazars.com/es para conocer más.

© Forvis Mazars 2026. Todos los derechos reservados.