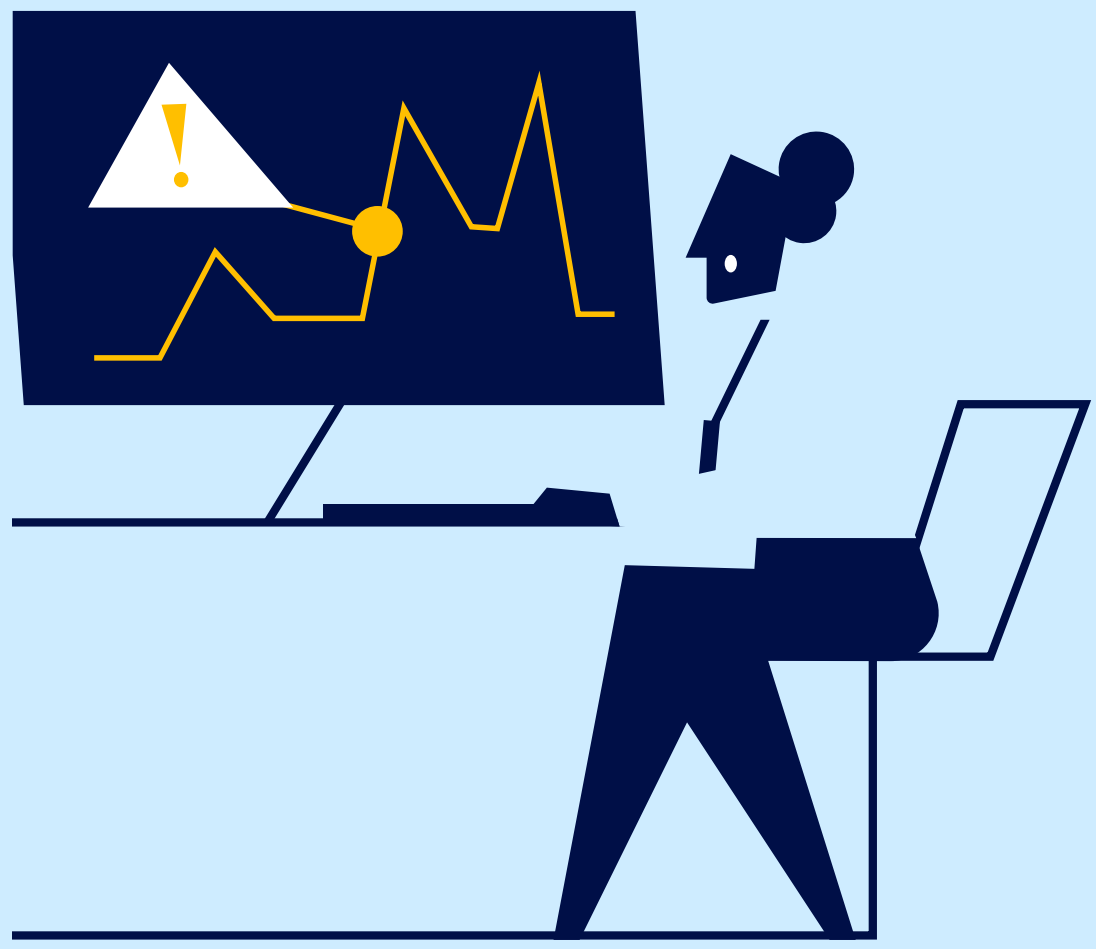
MARSH

Cyber Securitity Strategy powered by AI

La IA está cambiando el equilibrio entre ataque y defensa. Su capacidad para acelerar pruebas, detectar fallas y automatizar acciones exige integrar controles desde el diseño.



1

La IA amplía la superficie de ataque. Modelos avanzados ya pueden identificar vulnerabilidades reales, automatizar pruebas y encadenar exploits; la innovación debe avanzar con controles integrados.

2

La adopción de IA no debe medirse solo por eficiencia o velocidad. Para generar confianza, la alta dirección necesita asegurar gobierno de modelos, protección de datos, monitoreo de usos no autorizados y una estrategia de ciberseguridad basada en riesgo.

3

La IA introduce riesgos que no siempre se gestionan con controles tradicionales. Proteger datos, modelos, accesos, salidas y niveles de autonomía debe formar parte de la estrategia desde el diseño.

4

La madurez debe evolucionar. Pasar de seguridad improvisada a ciberseguridad basada en riesgo y datos permite reducir tiempos de detección, respuesta y recuperación.

5

La IA solo genera valor sostenible si se gestiona con una estrategia de ciberseguridad integrada. Para la alta dirección, esto implica visibilidad sobre usos no autorizados, monitoreo de amenazas, controles específicos, pruebas continuas y métricas claras de exposición.