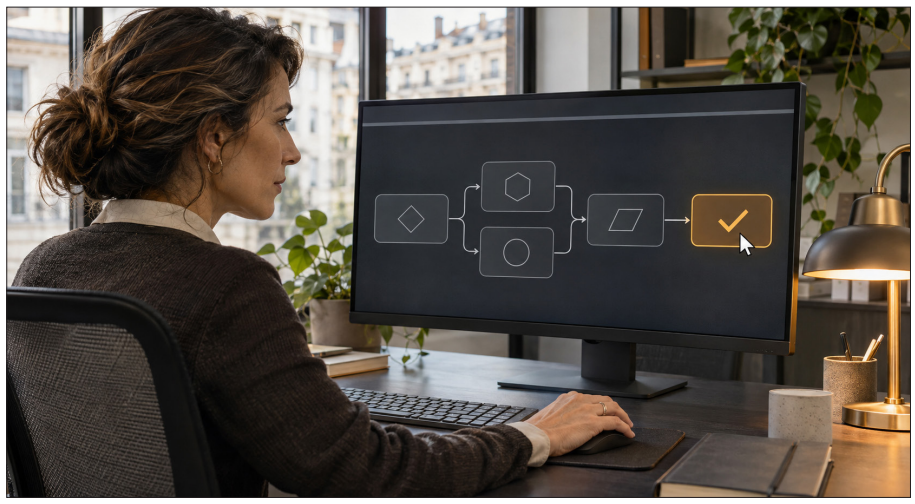
# LA HERRAMIENTA ESPAÑOLA DE PENTESTING CON INTELIGENCIA ARTIFICIAL





**Minery Report desarrolla una plataforma de pentesting autónomo supervisado que identifica vulnerabilidades, demuestra su existencia y mantiene el control humano de cada auditoría.**

Detectar una vulnerabilidad informática es importante, pero demostrar que realmente puede comprometer la seguridad de una empresa resulta determinante para poder corregirla. Con los ciberataques evolucionando constantemente, las organizaciones necesitan proteger sus sistemas, y la inteligencia artificial abre nuevas posibilidades para anticiparse a las amenazas. Por ello, Minery Report, compañía española especializada en ciberseguridad y fundada por profesionales procedentes del ámbito militar, ha desarrollado RAPTOR (nombre provisional, según informan desde la empresa), una plataforma de pentesting autónomo supervisado que utiliza inteligencia artificial para identificar, verificar y documentar fallos de seguridad. Su propuesta combina autonomía tecnológica, evidencias comprobables y supervisión humana, con capacidad para operar incluso en redes completamente aisladas de Internet, gracias a la ejecución local de su inteligencia artificial». Sin problema si tienes que modificarlo para que cuadre, por supuesto.

El pentesting, también conocido como prueba de intrusión, consiste en simular de manera controlada un ataque informático para descubrir posibles debilidades antes de que sean aprovechadas por ciberdelincuentes. RAPTOR lleva este procedimiento un paso más allá mediante agentes inteligentes capaces de investigar vulnerabilidades, reproducirlas y generar pruebas que faciliten su corrección.

## LA IA QUE NO SOLO DETECTA, TAMBIÉN DEMUESTRA

Una de las principales diferencias de RAPTOR respecto a los escáneres convencionales es su sistema de verificación: mientras que las herramientas tradicionales pueden generar largas listas de alertas que posteriormente deben comprobar los especialistas, la plataforma de Minery Report está diseñada para incorporar a sus informes únicamente aquellos fallos cuya existencia ha conseguido acreditar. Para ello, cada indicio se somete a un proceso de investigación que puede incluir hasta siete tipos de comprobación. Si las pruebas no resultan concluyentes, no se presenta como una vulnerabilidad confirmada. Además, cada hallazgo queda respaldado por evidencias documentadas, mientras que su nivel de gravedad se calcula mediante el sistema CVSS a partir de los resultados obtenidos, en lugar de depender de una estimación de la inteligencia artificial. Este planteamiento busca reducir los falsos positivos y facilitar el trabajo de los equipos de seguridad, que pueden concentrar sus recursos en resolver problemas verificados.



Pero la innovación no se limita a la detección técnica, porque RAPTOR también analiza cómo funciona una aplicación desde la perspectiva de sus usuarios, y examina los distintos roles, permisos y procesos para identificar situaciones que un escáner convencional podría pasar por alto.

Por ejemplo, puede comprobar si un cliente consigue acceder a las facturas de otro usuario o si una cuenta dispone de privilegios que no le corresponden. Para ello, reproduce operaciones con diferentes identidades y compara qué información puede consultar o modificar cada perfil.

La trazabilidad constituye otro elemento diferencial: en una ejecución y duraciones de ejemplo, la plataforma trabajó durante dos horas y 43 minutos, realizó 8.152 peticiones y registró 97 decisiones, cada una acompañada de su correspondiente justificación. El resultado es un informe que no se limita a señalar posibles riesgos, sino que incorpora pruebas, niveles de criticidad y recomendaciones para facilitar su resolución. Una documentación especialmente relevante cuando las empresas necesitan justificar sus actuaciones ante responsables internos, clientes o auditores.

## TECNOLOGÍA SOBERANA Y AUTONOMÍA BAJO SUPERVISIÓN HUMANA

El desarrollo de RAPTOR responde a tres principios: soberanía tecnológica, evidencia verificable y autonomía bajo control. Diseñada y desarrollada en España por Minery Report, cuyo origen está vinculado al Ejército del Aire y del Espacio, la plataforma permite ejecutar su inteligencia artificial en entornos locales sin depender de conexiones externas. Esta capacidad resulta especialmente importante para organizaciones que gestionan información sensible o trabajan con infraestructuras críticas.

RAPTOR contempla tres modalidades de despliegue: desde la nube, directamente en las instalaciones del cliente o mediante un sistema completamente aislado, sin conexión a Internet.

Pero la autonomía tampoco implica ausencia de supervisión, ya que antes de iniciar cada auditoría, los especialistas establecen qué sistemas pueden analizarse, cuáles quedan excluidos y bajo qué condiciones debe desarrollarse el trabajo. El auditor mantiene el control de las operaciones sensibles y puede detener la ejecución cuando resulte necesario. Esta combinación amplía sus posibilidades de aplicación en diferentes sectores: para las empresas, Minery Report ofrece pruebas de intrusión sobre aplicaciones web a precio cerrado, con informes de resultados y una posterior comprobación de las correcciones realizadas.

En el ámbito de Defensa, la plataforma puede trabajar sobre redes aisladas y generar indicadores de compromiso que permitan a los centros de operaciones de seguridad identificar posibles intentos de ataque; por su parte, las administraciones públicas encuentran una solución alineada con el Esquema Nacional de Seguridad (ENS), capaz de realizar auditorías, en sus modalidades locales, sin que la información abandone sus instalaciones.

RAPTOR incorpora más de 200 herramientas integradas y más de una docena de agentes especializados para analizar aplicaciones web y sus interfaces de programación, combinando distintas técnicas de investigación con verificaciones documentadas. Con esta tecnología, Minery Report impulsa una nueva generación de auditorías en las que la inteligencia artificial asume tareas complejas y repetitivas, mientras los profesionales mantienen el control. Todo para facilitar el acceso a pruebas de seguridad avanzadas, capaces de detectar vulnerabilidades, demostrar su existencia y aportar información útil para solucionarlas.

www.mineryreport.com