# ¿Qué es el EDR y qué aporta a mi empresa?

**RESUMEN**: Un sistema EDR (Endpoint Detection Response), es un sistema de protección de los equipos e infraestructuras de la empresa. Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.

**CATEGORÍAS:** CIBERSEGURIDAD

**Nº HIPERVINCULOS: 1**

Un sistema **EDR (Endpoint Detection Response)**, es un sistema de protección de los equipos e infraestructuras de la empresa. Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.

Gracias a esta conjunción de elementos y tecnologías permite detectar todos aquellos riesgos y amenazas que pueden provocar de forma silenciosa e inadvertida un incidente de seguridad, poniendo en riesgo la viabilidad de la empresa.

## Características de un sistema EDR

Un sistema EDR se caracteriza por aunar varios elementos de detección y de tecnologías.

Entre las aplicaciones y herramientas que incorpora, además del antivirus tradicional destacan, según señala INCIBE:

- Herramientas de análisis apoyadas en el uso del aprendizaje automático para mejorar la detección de amenazas.
- **Sandbox:** el sistema virtual y aislado de pruebas para comprobar el comportamiento de los archivos descargados, por ejemplo.
- **Escaneo de IOCs y reglas YARA**, que permiten analizar y detectar las amenazas provocadas por amenazas complejas en tiempo real.
- El uso de listas blancas y negras de correos electrónicos, páginas web e IP.
- Interoperatibilidad e interacción con otras herramientas de seguridad, como SIEM, IPS/IDS o herramientas antimalware.

Los principales fabricantes del mercado de soluciones de seguridad ofrecen este tipo de sistemas en su portafolio de aplicaciones. En el caso de que una empresa no cuente con técnicos o con un Departamento de Informática, siempre tiene la posibilidad de subcontratar este servicio a un proveedor o contratar el servicio completo con el fabricante.

Pero esto no es todo, porque además esta herramienta contiene una serie **de ventajas y fortalezas** frente a los antivirus tradicionales o EPP, como, por ejemplo:

- Recopila información exhaustiva y detallada de las características del dispositivo.
- Permite recopilar y almacenar información de forma automática, así como crear patrones de detección automatizados, facilitando el trabajo de detección.
- Monitoriza la integridad de los sistemas y de los archivos de configuración claves, avisando en caso de modificación o acceso a los mismos por actores sospechosos.
- Autoriza localizar en un solo punto toda la información, posibilitando en caso de incidente la realización de una investigación de forma rápida.

**FUENTE: INCIBE*