

N.º EXPEDIENTE: DCIBERID/25/PA/0003

LÍNEA: 2025 Proyectos Empresariales de I+D en Ciberseguridad

TÍTULO DEL PROYECTO: Desarrollo de un nuevo sistema IDS/IPS y monitorización centralizada de vulnerabilidades en redes

PLAZO DE EJECUCIÓN: Desde el 01/10/2024 hasta el 31/08/2026

SUBVENCIÓN CONCEDIDA: 171.618,07 €

El proyecto tuvo como objetivo general el diseño, desarrollo y validación de una nueva solución software avanzada de ciberseguridad, capaz de integrar funcionalidades de detección y prevención de intrusiones (IDS/IPS), monitorización centralizada de vulnerabilidades, correlación inteligente de eventos de seguridad y análisis predictivo de amenazas, con el fin de mejorar la protección de infraestructuras empresariales e industriales frente a ciberataques y riesgos tecnológicos.

La actuación ha permitido desarrollar la plataforma **Alsis Guard**, una solución orientada a reforzar la resiliencia digital de las organizaciones mediante la detección temprana de amenazas, la automatización de procesos de respuesta y la gestión centralizada de la información de seguridad.

Objetivos específicos:

- Desarrollar un sistema IDS/IPS propio capaz de detectar y bloquear intentos de intrusión en tiempo real mediante mecanismos avanzados de análisis y respuesta.
- Diseñar y desarrollar una plataforma SIEM para la centralización, normalización y correlación de eventos de seguridad procedentes de múltiples fuentes.
- Implementar mecanismos de monitorización continua de vulnerabilidades que permitan identificar, clasificar y priorizar riesgos de seguridad de forma centralizada.
- Desarrollar sistemas automatizados de alertas, informes técnicos e indicadores de riesgo para facilitar la toma de decisiones y el cumplimiento normativo.
- Incorporar capacidades avanzadas de correlación predictiva de eventos mediante técnicas de aprendizaje automático orientadas a reducir los tiempos de detección (MTTD) y respuesta (MTTR).
- Implementar mecanismos de monitorización de integridad de activos digitales y respuesta activa frente a amenazas en entornos Windows y Linux.
- Validar experimentalmente la eficacia del sistema mediante pruebas controladas y simulaciones de incidentes de seguridad en entornos representativos.
- Contribuir al fortalecimiento de las capacidades tecnológicas de ciberseguridad en Castilla y León, en línea con los objetivos del Programa Red Argos (RETECH), la Estrategia RIS3 y el Plan de Recuperación, Transformación y Resiliencia.