ESTUDIOS DE EXTENSIÓN UNIVERSITARIA

INVESTIGACIÓN Y RESPUESTA ANTE INCIDENTES (DFIR / BLUE TEAM) (1ª ED.)

INFORMACIÓN GENERAL

CURSO ACADÉMICO: 2025/2026
ÁREA: Enseñanzas Técnicas
CRÉDITOS: 3,00 créditos ECTS (*)
PRECIO DE MATRÍCULA: 221,00 € (Seguro: 4 €, a consultar)
DIRECCIÓN ACADÉMICA: Alexander Mendiburu y José Luís Jodra Luque

PRESENTACIÓN

Este curso se centra en la gestión operativa de incidentes de ciberseguridad y la aplicación de metodologías de Digital Forensics & Incident Response (DFIR). El estudiante aprenderá a implementar el ciclo de respuesta definido en el NIST SP 800-61, realizar triaje y análisis inicial de sistemas comprometidos, extraer indicadores de compromiso (IoCs), y elaborar informes técnicos y ejecutivos derivados de un incidente. Se abordarán herramientas y técnicas de adquisición y análisis forense básico, correlación de eventos en entornos SIEM, y aplicación práctica de frameworks como MITRE ATT&CK y Sigma para la detección y clasificación de ataques.

Objetivos específicos

- Implementar el ciclo de vida de respuesta a incidentes del NIST SP 800-61.
- Realizar triaje y análisis inicial de endpoints mediante la interpretación de logs y eventos.
- Aplicar técnicas de adquisición y preservación de evidencias en memoria y disco.
- Elaborar indicadores de compromiso (IoCs) y construir líneas temporales de ataque.
- Comprender las fases de contención, erradicación y recuperación en un entorno controlado.
- Elaborar un reporte técnico y ejecutivo que sintetice las acciones realizadas, hallazgos y medidas de mejora.

Contenidos

1. Marco de respuesta a incidentes (IR Framework)
2. Telemetría y detección
3. Triaje y adquisición de evidencias
4. Análisis inicial de malware
5. Contención y erradicación
6. Elaboración de informes y lecciones aprendidas.

TE BUSCAMOS A TI

La ciberseguridad se ha convertido en una competencia estratégica para las organizaciones de todos los sectores. Consciente de esta realidad, la Facultad de Informática de la Universidad del País Vasco ofrece un conjunto de siete cursos, diseñados para personas que deseen actualizar, reforzar o reorientar su perfil profesional.

SALIDAS PROFESIONALES

Los cursos ofertados te permitirán adquirir diferentes conocimientos en el ámbito de la ciberseguridad, adquiriendo competencias sobre los fundamentos de la ciberseguridad, el gobierno y cumplimiento, las arquitecturas y desarrollos seguros, la investigación ante incidentes, la seguridad ofensiva y defensiva, o la ciberseguridad en entorno OT.

REQUISITOS

No existen requisitos para esta formación, pero se recomiendan conocimientos y experiencia en el ámbito de las TICs.

IMPARTICIÓN

FECHAS DE IMPARTICIÓN: 13/04/2026 – 07/06/2026
LUGAR DE IMPARTICIÓN: Virtual
IDIOMA DE IMPARTICIÓN: Euskera y castellano.

INFORMACIÓN / INSCRIPCIÓN

DEPARTAMENTO U ÓRGANO RESPONSABLE: Facultad de Informática
DIRECCIÓN: Paseo Manuel de Lardizabal, 1. 20018 Donostia-San Sebastian
TELÉFONO: 943 015 020
CORREO ELECTRÓNICO: dif.zibersegurtasuna@ehu.eus

(*) 1 Crédito ECTS equivale a 25 horas