

Formación en Resposta a Incidentes (DFIR) e Análise Forense

Descrición

O curso componse dos seguintes módulos:

- Análise forense e DFIR en Redes
- Análise forense e DFIR en Windows
- Análise forense e DFIR en Linux
- Adestramento 100% práctico de DFIR Vol.1
- Adestramento 100% práctico de DFIR Vol.2
- Exame de certificación IRCP (Incident Response Certified Professional) de Securízame Neles, ensínase como levar a cabo a adquisición de evidencias dixitais tanto de sistemas Windows e Linux vivos, como de imaxes forenses, así como doutros sistemas auxiliares, típicos dunha rede corporativa como poden ser firewalls, servidores DHCP, VPN, etc, ...

Dos artefactos forenses extraídos ensínase a interpretación do seu contido para comprender que utilidade poden ter nun incidente de seguridade que se identificou na organización.

Aínda que o compoñente práctico dos tres primeiros módulos é moi elevado, nos chamados adestramentos 100% prácticos, o compoñente práctico é completo posto que o alumnado se enfrontará a un caso real do que terá que extraer artefactos forenses e interpretar o seu contido, elixindo ademais por que sistema da rede empezar, aprendendo a metodoloxía necesaria para acoutar o incidente e saber onde ter que ir a continuación. Isto é vital á hora de identificar tanto o punto de entrada que posibilitou o incidente en si, como a post-explotación sucedida no mesmo no caso dun compromiso externo. Igualmente verase, de forma 100% práctica, situacións de atacantes internos á propia organización.

Obxectivos

- Que o alumnado aprenda a extraer de forma adecuada evidencias dixitais co fin de análise forense
 - Que o alumnado aprenda a interpretar as devanditas evidencias para entender a actividade realizada polos/as usuarios/as dun sistema Windows ou Linux que forma parte dunha rede corporativa.
 - Que o alumnado sexa capaz de comprender un incidente de seguridade no que estiveron involucrados diferentes sistemas dunha rede corporativa.

Dirixido a

Profesionais de seguridade informática que queiran especializarse en resposta ante incidentes en sistemas Windows e Linux integrados en contornas corporativas, facendo uso de técnicas de análise forense dixital con ferramentas gratuítas.

Debe terse en conta que:

- Os cursos requiren traballo adicional ás horas adicadas na clase.
- A realización dos cursos esize adicación plena durante as horas de clase.
- As formacións, documentación, titorías, forma de comunicación cos profesores e o exame será unicamente en idioma castelán.

BENEFICIOS

Diploma de asistencia

Opción gratuita dun exame de certificación oficial

Perfil do docente

- Enxeñeiro en Informática - Deusto 2001
- Perito informático forense con ampla experiencia en sala
- 25 anos de experiencia profesional en ciberseguridade
- Certificado CISA (Certified Information Systems Auditor) - (2010 - 2014)
- Certificado CISSP (Certified Information Systems Security Professional) - (2008 - 2014)
- Experto en Ciberseguridade especializado en resposta ante incidentes e Informática

Forense

PROGRAMA

Programación 2025/26

TIPO

CURSO

MATRÍCULA

Gratuíta

PERIODO INSCRICIÓN

20/10/2025 - 02/11/2025

PROBA DE SELECCIÓN

06/11/2025 (16:30)

CRITERIOS DE SELECCIÓN	Proba técnica presencial no CNTG en Santiago de Compostela
Nº PRAZAS	20 (Mínimo 10)
METODOLOXÍA	Virtual
TIPO DE EDICIÓN	Edición única (desempregados/as e ocupados/as)
DURACIÓN	90 horas
DATA INICIO	01/12/2025
DATA FIN	12/02/2026
HORARIO	De luns a xoves de 16:00 a 21:00 horas. Decembro do 1 ao 4 e
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	IRCP (Incident Response Certified Professional)
MÓDULOS TRANSVERSAIS	Igualdade de 10 horas
TECNOLOXÍA	Ciberseguridade/Ciberseguridad
PERIODO DOCENCIA	01/12/2025 - 12/02/2026

Temario

Curso DFIR e Análise Forense en Redes

- Introducción
- Análise forense de rede

Formación en Resposta a Incidentes (DFIR) e Análise Forense

- Fontes de evidencia
- Metodoloxía OSCAR
- Repaso a conceptos de redes
- Topoloxías típicas de rede
- Conceptos de switching e routing
- Ataques de rede
- Despregamento de infraestrutura necesaria
- Ferramentas de captura de rede: Suite Wireshark
- TCPFlows
- Despregamento de infraestrutura de IDS: snort, suricata, bro e Wazuh
- Ferramentas de monitorización de tráfico
- Security Onion
- Intercepción, Captura e Análise de protocolos
- Exfiltración de información
- Outras fontes de evidencia: Firewalls, proxies, WAFs
- Casos prácticos e instalacións

Curso DFIR e Análise Forense en Windows

- Introducción aos incidentes de ciberseguridade
- Metodoloxía e peritaxe
- Adquisición e clonado de evidencias
- Artefactos forenses de usuario/a, sistema e sistema de ficheiros
- Sistemas de ficheiros: Envorcado, interpretación e análise de sistemas de ficheiros

NTFS

- Análise forense á memoria

Curso DFIR e Análise Forense en Linux

- Conceptos e Distribucións Forenses
- Dixital Forensics Incident Response
- Triage en Linux
- Forense á Memoria RAM
- Análise de sistemas de ficheiros
- Recuperación avanzada de información eliminada
- Funcionamento detallado e artifacts de GNU/Linux
- Diferenzas entre System V e Systemd
- Recuperación de elementos cruce
- Ferramentas de monitorización e axuda para análise forense
- Análise de casos reais