

Formación financiada por:



# Monitorización avanzada

.....  
Aula Virtual • 30 horas de duración

# Monitorización Avanzada



## Objetivos principales del curso

Identificar los tipos de acceso al sistema informático, así como los mecanismos de seguridad del mismo, describiendo sus características principales y herramientas asociadas más comunes para garantizar el uso de los recursos del sistema.



## Conocimientos necesarios del alumno y requisitos técnicos para seguir el curso:

### Conocimientos previos:

- Deseable haber realizado previamente el Curso de Introducción a la ciberseguridad.
- Manejo de máquinas virtuales, preferiblemente en Virtualbox.
- Conocimiento de administración Windows. Creación de grupos y usuarios. Comandos básicos de terminal y powershell.
- Conocimiento de administración de sistemas GNU/Linux. Manejo fluido de terminal y comandos.
- Conocimientos básicos de la distribución KaliLinux.
- Conocimientos mínimos sobre redes IP: direccionamiento IP, protocolos HTTP, HTTPS, FTP, SSH, TCP y UDP.

### Requisitos mínimos hardware y software

- Hardware
  - Memoria RAM: 16 Gb.
  - Espacio libre en disco duro (preferiblemente SSD): 150 GB.
- Software
  - Virtualbox 6.1.0 o superior



## Metodología:

Impartición de la actividad formativa en modalidad aula virtual con personal cualificado y especializado en la materia, con jornadas de impartición de conocimientos teóricos y ejecución de jornadas prácticas para el desarrollo de los conocimientos.

# Temario

¿Qué aprenderás con nosotros?

- **Conceptos generales.**
- **La gestión de Logs. Syslog. Event Log/Sysmon.**
- **El ciclo de inteligencia y la monitorización.**
- **Monitorización en sistemas finales**
- **Tipos de malware. Herramientas Antimalware.**
- **HIDS/HIPS**
- **EDRs**
- **Monitorización de redes.**
- **Herramientas de captura y monitorización.**
- **Sistemas de detección de intrusiones en red. NIDS/NIPS SIEMs**
- **Indicadores de compromiso (IOCs). MISP. Reglas Yara.**

# Perfil del docente y empresa proveedora

## Juan Antonio Flores Caba

Ingeniero técnico superior, con amplia experiencia como consultor de sistemas informáticos y ciberseguridad, fundamentalmente en el mundo Linux aplicando dichos conocimientos a diversos campos. Consultor senior de Ciberseguridad, Sistemas y Cloud. Administrador de sistemas, desarrollo y testeo de producto. Analista forense. Inteligencia Artificial. Formador experto en Linux, Red Team, Blue Team, Ciberseguridad. Profesor titular para Boot Camp de ciberseguridad , también preparando propuestas formativas de ciberseguridad defensiva para el CNI

### Certificaciones:

- Ciberseguridad avanzada en entornos de las tecnologías de la operación, Octubre 2024 - IFCT 0050
- Oracle Cloud Infrastructure 2024 Generative AI Certified Professional, Julio 2024
- CompTIA Cloud+, Febrero 2024
- Oracle Cloud Infrastructure AI Foundations Associate , Octubre 2023
- Oracle Cloud Infrastructure Foundations Associate, Agosto 2023
- CompTIA CySA+ , Diciembre 2022
- CompTIA Security+ , Junio 2020
- EC-Council , Certified Ethical Hacker , Junio 2020
- Oracle Certified Associate, Oracle Linux 5 & 6, Septiembre 2016
- Oracle Database SQL Certified Associate , Noviembre 2016
- Linux Professional Institute 1 - 2 - 3 , Noviembre 2023
- Programador en Cobol

### **Empresa proveedora: GDoce Formación**

# Resumen de características del curso



Recomendable tener **certificado digital** para acceder a <https://campusvirtualemprego.xunta.gal/>



**Acceso las 24 horas** a los contenidos que el docente suba a <https://campusvirtualemprego.xunta.gal/> durante el período del curso.



**Nivel:** Avanzado.



Curso 100% en **castellano**.



**Acceso directo al tutor** para resolver todas tus dudas.



**Diploma emitido por la Consellería de Emprego, Comercio e Emigración** después de revisar que el alumno ha cumplido con los requisitos exigidos para superar el curso con la cualificación de APTO. El Clúster TIC Galicia no es responsable de la fecha de emisión de dicho diploma.



Formación financiada por:



**¿Tienes dudas?  
Contacta con nosotros:**

Tel.: +34 881 939 651

E-mail: [info@clusterticgalicia.com](mailto:info@clusterticgalicia.com)