



**EUROINNOVA**  
INTERNATIONAL ONLINE EDUCATION



**inesem**  
business school



**UTAMED**

**Máster de Formación Permanente en Implantación, Gestión y Auditoría de  
Sistemas de Seguridad de Información ISO 27001-ISO 27002 + 60 Créditos ECTS**





Elige aprender en la escuela  
líder en formación online

# ÍNDICE

1 | Somos  
INESEM

2 | Alianza

3 | Rankings

4 | By EDUCA  
EDTECH  
Group

5 | Metodología  
LXP

6 | Razones  
por las que  
elegir  
Euroinnova

7 | Financiación  
y Becas

8 | Métodos de  
pago

9 | Programa  
Formativo

10 | Temario

11 | Contacto

## SOMOS INESEM

---

INESEM es una **Business School online** especializada con un fuerte sentido transformacional. En un mundo cambiante donde la tecnología se desarrolla a un ritmo vertiginoso nosotros somos activos, evolucionamos y damos respuestas a estas situaciones.

Apostamos por **aplicar la innovación tecnológica a todos los niveles en los que se produce la transmisión de conocimiento**. Formamos a profesionales altamente capacitados para los trabajos más demandados en el mercado laboral; profesionales innovadores, emprendedores, analíticos, con habilidades directivas y con una capacidad de añadir valor, no solo a las empresas en las que estén trabajando, sino también a la sociedad. Y todo esto lo podemos realizar con una base sólida sostenida por nuestros objetivos y valores.

Más de

**18**

años de  
experiencia

Más de

**300k**

estudiantes  
formados

Más de un

**90%**

tasa de  
empleabilidad

Hasta un

**100%**

de financiación

Hasta un

**50%**

de los estudiantes  
repite

Hasta un

**25%**

de estudiantes  
internacionales

[Ver en la web](#)



Leaders driving change  
**Elige Inesem**

## ALIANZA INESEM Y UTAMED

---

**NESEM y UTAMED** se unen para liderar la transformación de la educación superior online.

INESEM Business School destaca como business school de referencia en formación online para profesionales, con especial énfasis en áreas como empresa, marketing, recursos humanos, tecnología y gestión empresarial. Su modelo formativo combina accesibilidad, innovación y un fuerte enfoque en el desarrollo de competencias.

UTAMED, desde su origen digital y su mirada Atlántico-Mediterránea, comparte esa visión orientada al futuro. Como universidad 100% online, apuesta por programas actualizados, multidisciplinares y adaptados a las demandas de un mercado global.

Esta alianza refuerza el puente entre la formación profesional y la formación universitaria, creando itinerarios integrados que permiten a los estudiantes avanzar en sus carreras con titulaciones avaladas académicamente y conectadas con el entorno laboral.

Ambas instituciones coinciden en ofrecer una experiencia educativa ágil, práctica y con fuerte base tecnológica, gracias a la novedosa metodología EDUCA LXP.



[Ver en la web](#)



## RANKINGS DE INESEM

---

INESEM Business School ha obtenido reconocimiento tanto a nivel nacional como internacional debido a su firme compromiso con la innovación y el cambio.

Para evaluar su posición en estos rankings, se consideran diversos indicadores que incluyen la percepción online y offline, la excelencia de la institución, su compromiso social, su enfoque en la innovación educativa y el perfil de su personal académico.



Ver en la web

## ALIANZAS Y ACREDITACIONES

---

### Relaciones institucionales



### Relaciones internacionales



### Accreditaciones y Certificaciones



[Ver en la web](#)

## BY EDUCA EDTECH

---

Inesem es una marca avalada por **EDUCA EDTECH Group**, que está compuesto por un conjunto de experimentadas y reconocidas **instituciones educativas de formación online**. Todas las entidades que lo forman comparten la misión de **democratizar el acceso a la educación** y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.



### ONLINE EDUCATION

---



Ver en la web



# METODOLOGÍA LXP

---

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.



## 1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.



## 2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.



## 3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.



## 4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.



## 5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.



## 6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.



Programas  
**PROPIOS**  
**UNIVERSITARIOS**  
**OFICIALES**

## RAZONES POR LAS QUE ELEGIR INESEM

---

### 1. Nuestra Experiencia

- ✓ Más de **18 años de experiencia**.
- ✓ Más de **300.000 alumnos** ya se han formado en nuestras aulas virtuales
- ✓ Alumnos de los 5 continentes.
- ✓ **25%** de alumnos internacionales.
- ✓ **97%** de satisfacción
- ✓ **100% lo recomiendan**.
- ✓ Más de la mitad ha vuelto a estudiar en Inesem.

### 2. Nuestro Equipo

En la actualidad, Inesem cuenta con un equipo humano formado por más **400 profesionales**. Nuestro personal se encuentra sólidamente enmarcado en una estructura que facilita la mayor calidad en la atención al alumnado.

### 3. Nuestra Metodología



#### 100% ONLINE

Estudia cuando y desde donde quieras. Accede al campus virtual desde cualquier dispositivo.



#### APRENDIZAJE

Pretendemos que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva



#### EQUIPO DOCENTE

Inesem cuenta con un equipo de profesionales que harán de tu estudio una experiencia de alta calidad educativa.



#### NO ESTARÁS SOLO

Acompañamiento por parte del equipo de tutorización durante toda tu experiencia como estudiante

## 4. Calidad AENOR

- ✓ Somos Agencia de Colaboración N°99000000169 autorizada por el Ministerio de Empleo y Seguridad Social.
- ✓ Se llevan a cabo auditorías externas anuales que garantizan la máxima calidad AENOR.
- ✓ Nuestros procesos de enseñanza están certificados por AENOR por la ISO 9001.



## 5. Somos distribuidores de formación

Como parte de su infraestructura y como muestra de su constante expansión Euroinnova incluye dentro de su organización una **editorial** y una **imprenta digital industrial**.

## MÉTODOS DE PAGO

---

Con la Garantía de:



Fracciona el pago de tu curso en cómodos plazos y sin interéres de forma segura.



Nos adaptamos a todos los métodos de pago internacionales:



y muchos más...



Protección al  
Comprador

[Ver en la web](#)

## Máster de Formación Permanente en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 + 60 Créditos ECTS



**DURACIÓN**  
1500 horas



**MODALIDAD  
ONLINE**



**ACOMPANIAMIENTO  
PERSONALIZADO**



**CREDITOS**  
60 ECTS

### Titulación

---

Titulación de Máster de Formación Permanente en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 con 1500 horas y 60 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.

[Ver en la web](#)




**INESEM BUSINESS SCHOOL**  
**UNIVERSIDAD TECNOLÓGIC ALTÁNTICO - MEDITERRÁNEO**

como centro acreditado para la impartición de acciones formativas  
expide el presente título propio

**NOMBRE DEL ALUMNO/A**  
con número de documento XXXXXXXX ha superado los estudios correspondientes de

**NOMBRE DEL CURSO**  
con una duración de XXX horas, perteneciente al Plan de Formación de UTAMED.  
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXXXXXX-XXXX-XXXXXX.  
Con una calificación XXXXXXXXXXXXXXXX.  
Y para que conste expido la presente titulación en Granada, a (día) de (mes) del (año).

NOMBRE ALUMNO/A

Firma del Alumno/a

NOMBRE DE AREA MANAGER

La Dirección Académica







Con Sello de Consulta. Colegio Español del Comercio Exterior y Social de la UNED. Num. Producción 4509

## Descripción

Este Master en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 ofrece una formación especializada en materia de seguridad en entornos informáticos. Hoy en día la seguridad informática es un tema de vital importancia para todo tipo de organizaciones, ya que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados, aptos para emplearse en cualquier tipo de empresas. La adecuada y correcta implementación de un SGSI permite a las empresas asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

## Objetivos

- Abordar los lineamientos básicos para la aplicación de la Norma ISO/IEC 27001 dentro de su organización.
- Dominar las pautas para implementar un sistema de gestión de seguridad de información basado en el estándar ISO/IEC 27001.
- Conocer los controles recomendados por el estándar ISO/IEC 27002 en sus respectivas cláusulas.
- Exponer una serie de buenas prácticas para conseguir la seguridad de la información a través de la ciberseguridad.
- Gestionar el buen funcionamiento de las redes informáticas de la organización.
- Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
- Detectar y responder ante incidentes de seguridad informática.

Ver en la web

## Para qué te prepara

---

Este Master en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 está dirigido a profesionales relacionados con la seguridad de la información de cualquier nivel y tipo y que desean conocer, desarrollar y aplicar, implantar un SGI robusto y fiable para su organización.

## A quién va dirigido

---

Este Master en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 prepara para gestionar la Seguridad de la Información de todo tipo de organizaciones, tanto desde un punto de vista interno como externo, (ofreciendo el servicio a terceros), al gestionar las incidencias de seguridad informática y los servicios del sistema informático, de seguros de acceso y transmisión de datos.

## Salidas laborales

---

Las salidas profesionales de este Master en Implantación, Gestión y Auditoría de Sistemas de Seguridad de Información ISO 27001-ISO 27002 están relacionadas con el mundo de la ciberseguridad como, por ejemplo: director de seguridad de la información, analista de seguridad informática, arquitecto de ciberseguridad, administrador de seguridad o analista de riesgo informático.

[Ver en la web](#)

# TEMARIO

---

## MÓDULO 1. LA SEGURIDAD DE LA INFORMACIÓN

### UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD Y SOCIEDAD DE LA INFORMACIÓN

1. ¿Qué es la ciberseguridad?
2. La sociedad de la información
3. Diseño, desarrollo e implantación
4. Factores de éxito en la seguridad de la información
5. Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

### UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI. ISO 27001 e ISO 27002
2. Legislación: Leyes aplicables a los SGSI

### UNIDAD DIDÁCTICA 3. INTRODUCCIÓN A LA NIS2

1. Historia y evolución de la NIS2
2. Objetivos y alcance de la NIS2
3. Diferencias entre NIS1 y NIS2
4. Sectores críticos afectados por la NIS2

### UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

### UNIDAD DIDÁCTICA 5. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

1. Contexto
2. Liderazgo
3. Planificación
4. Soporte 213

### UNIDAD DIDÁCTICA 6. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1. Operación
2. Evaluación del desempeño
3. Mejora

### UNIDAD DIDÁCTICA 7. AUDITORÍA DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN POR LA DIRECCIÓN

1. El porqué de la auditoría

2. La auditoría interna
3. El proceso de certificación

#### UNIDAD DIDÁCTICA 8. REVISIÓN POR LA DIRECCIÓN Y MEJORA DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN

1. Revisión del sistema de gestión de la información por la dirección
2. Mejora del sistema de gestión de la seguridad de la información

#### UNIDAD DIDÁCTICA 9. GUÍAS DE SEGURIDAD: NORMATIVAS Y BUENAS PRÁCTICAS

1. Introducción a las guías de seguridad CCN-STIC
2. CCN-STIC-800 Glosario de términos y abreviaturas del ENS
3. CCN-STIC-801 Responsabilidades y funciones en el ENS
4. CCN-STIC-802 Auditoría del ENS
5. CCN-STIC-803 Valoración de Sistemas en el ENS
6. CCN-STIC-804 Medidas de implantación del ENS
7. CCN-STIC-805 Política de seguridad de la información
8. CCN-STIC-806 Plan de adecuación al ENS
9. CCN-STIC-807 Criptología de empleo en el ENS
10. CCN-STIC-808 Verificación del cumplimiento del ENS

#### MÓDULO 2. CIBERSEGURIDAD: NORMATIVA, POLÍTICA DE SEGURIDAD Y CIBERINTELIGENCIA

##### UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD Y SOCIEDAD DE LA INFORMACIÓN

1. ¿Qué es la ciberseguridad?
2. La sociedad de la información
3. Diseño, desarrollo e implantación
4. Factores de éxito en la seguridad de la información
5. Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

##### UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI. ISO 2. Legislación: Leyes aplicables a los SGSI

##### UNIDAD DIDÁCTICA 3. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

##### UNIDAD DIDÁCTICA 4. INGENIERÍA SOCIAL, ATAQUES WEB Y PHISHING

1. Introducción a la Ingeniería Social
2. Recopilar información
3. Herramientas de ingeniería social
4. Técnicas de ataques

5. Prevención de ataques
6. Introducción a Phising
7. Phising
8. Man In The Middle

#### UNIDAD DIDÁCTICA 5. CIBERINTELIGENCIA Y CIBERSEGURIDAD

1. Ciberinteligencia
2. Herramientas y técnicas de ciberinteligencia
3. Diferencias entre ciberinteligencia y ciberseguridad
4. Amenazas de ciberseguridad

#### UNIDAD DIDÁCTICA 6. MÉTODOS DE INTELIGENCIA DE OBTENCIÓN DE INFORMACIÓN

1. Contextualización
2. OSINT
3. HUMINT
4. IMINT
5. Otros métodos de inteligencia para la obtención de información

#### UNIDAD DIDÁCTICA 7. CIBERINTELIGENCIA Y TECNOLOGÍAS EMERGENTES

1. Tecnologías emergentes
2. Desafíos y oportunidades de la ciberinteligencia en las tecnologías emergentes
3. Análisis de amenazas avanzado
4. Usos de las tecnologías emergentes en la ciberinteligencia

#### MÓDULO 3. CRIPTOGRAFÍA Y REDES PRIVADAS VIRTUALES (VPN)

##### UNIDAD DIDÁCTICA 1. HISTORIA Y EVOLUCIÓN DE LA CRIPTOGRAFÍA

1. La criptografía a lo largo de la historia
2. El nacimiento del criptoanálisis
3. La criptografía en nuestros tiempos
4. Criptografía en el futuro

##### UNIDAD DIDÁCTICA 2. SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA

1. Seguridad Informática
2. Uso de seguridad informática y criptografía
3. Tipo de amenazas
4. Respuesta ante un ataque
5. Amenazas del futuro

##### UNIDAD DIDÁCTICA 3. CRIPTOGRAFÍA SIMÉTRICA Y CRIPTOGRAFÍA ASIMÉTRICA

1. Criptografía simétrica
2. Criptografía asimétrica
3. Criptografía híbrida
4. Criptografía y seguridad informática: El Ciclo de vida de las claves y contraseñas

#### UNIDAD DIDÁCTICA 4. CRIPTOGRAFÍA DE CLAVE PRIVADA

1. Cifrado de clave privada
2. Cifrado DES
3. Función F

#### UNIDAD DIDÁCTICA 5. CRIPTOGRAFÍA DE CLAVE PÚBLICA

1. Cifrado de clave pública
2. PKC como herramienta de cifrado
3. Uso en Generación de Firmas Digitales
4. Aplicaciones de la criptografía pública y privada
5. Certificado digital
6. DNI Electrónico
7. Bitcoin

#### UNIDAD DIDÁCTICA 6. PROTOCOLOS CRIPTOGRÁFICOS Y FIRMAS DIGITALES

1. Protocolo criptográfico
2. Protocolo criptográfico avanzado
3. Firma segura hacia delante

#### UNIDAD DIDÁCTICA 7. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

#### UNIDAD DIDÁCTICA 8. HASHING

#### UNIDAD DIDÁCTICA 9. TIPOS DE ALGORITMOS Y CIFRADOS CRIPTOGRÁFICOS

1. Métodos criptográficos históricos
2. Challenge Handshake Authentication Protocol (CHAP)
3. Federal Information Processing Standards (FIPS)
4. Private Communication Technology (PCT)
5. Secure Electronic Transaction (SET)
6. Secure Sockets Layer (SSL)
7. Simple Key Management for Internet Protocol (SKIP)
8. IP Security Protocol (IPSec)

#### UNIDAD DIDÁCTICA 10. HERRAMIENTAS CRIPTOGRÁFICAS Y EJEMPLOS DE USO

1. Herramientas Criptográficas de Microsoft
2. CrypTool-Online (CTO)

3. Java Cryptographic Architecture (JCA)
4. GNU Privacy Guard
5. Whisply
6. DiskCryptor
7. AES Crypt
8. Ejemplos criptográficos en Python

#### UNIDAD DIDÁCTICA 11. INTRODUCCIÓN A LAS REDES PRIVADAS VIRTUALES (VPN)

1. ¿Qué son las redes privadas virtuales o VPN?
2. Bloques de construcción de VPN
3. Tecnologías VPN, Topología y Protocolos
4. VPN vs IP móvil

#### UNIDAD DIDÁCTICA 12. ARQUITECTURAS VPN

1. Requisitos y arquitecturas VPN
2. Arquitecturas VPN basadas en seguridad y en capas
3. VPN de acceso remoto y extranet

#### UNIDAD DIDÁCTICA 13. PROTOCOLOS DE TUNELIZACIÓN VPN

1. PPTP
2. L2TP
3. L2F
4. IPSec
5. MPLS

#### UNIDAD DIDÁCTICA 14. AUTENTICACIÓN Y CONTROL DE ACCESO EN VPN

1. Autenticación PPP
2. RADIO y Kerberos
3. Autenticación de VPN
4. Control de acceso en VPN

#### UNIDAD DIDÁCTICA 15. GESTIÓN DE SERVICIOS Y REDES VPN

1. Protocolos y arquitectura de gestión de red
2. Gestión de servicios VPN
3. Centros de operaciones de red (NOC)
4. Redundancia y equilibrio de carga

#### MÓDULO 4. CRACKING O INGENIERÍA INVERSA

##### UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y DEFINICIONES BÁSICAS

1. Concepto de Ingeniería Inversa
2. Características de la Ingeniería Inversa
3. Ventajas del uso de Ingeniería Inversa

## UNIDAD DIDÁCTICA 2. TIPOS DE INGENIERÍA INVERSA

1. Ingeniería inversa de datos
2. Ingeniería inversa de lógica o proceso
3. Ingeniería inversa de interfaces de usuario

## UNIDAD DIDÁCTICA 3. HERRAMIENTAS DE CRACKING

1. Depuradores
2. Desensambladores
3. Compiladores Inversos o Decompiladores

## MÓDULO 5. HERRAMIENTAS DE CIBERSEGURIDAD OSINT

### UNIDAD DIDÁCTICA 1. QUÉ SON LAS HERRAMIENTAS OSINT

1. Introducción

### UNIDAD DIDÁCTICA 2. GOOGLE DORK

1. Qué es Google Dork
2. Uso y aplicación de Google Dork

### UNIDAD DIDÁCTICA 3. SHODAN

1. Qué es Shodan
2. Uso y aplicación de Shodan

### UNIDAD DIDÁCTICA 4. MALTEGO

1. Qué es Maltego
2. Uso y aplicación de Maltego

### UNIDAD DIDÁCTICA 5. THE HARVESTER

1. Qué es The Harvester
2. Uso y aplicación de The Harvester

### UNIDAD DIDÁCTICA 6. RECON-NG

1. Qué es Recon-ng
2. Uso y aplicación de Recon-ng

### UNIDAD DIDÁCTICA 7. CREEPY

1. Qué es Creepy
2. Uso y aplicación de Creepy

### UNIDAD DIDÁCTICA 8. FOCA

1. Qué es Foca

2. Uso y aplicación de Foca

MÓDULO 6. GESTIÓN DE INCIDENTES Y ANÁLISIS FORENSE

UNIDAD DIDÁCTICA 1. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. Procedimiento de recolección de información relacionada con incidentes de seguridad
2. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
3. Proceso de verificación de la intrusión
4. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

UNIDAD DIDÁCTICA 2. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1. Establecimiento de las responsabilidades
2. Categorización de los incidentes derivados de intentos de intrusión
3. Establecimiento del proceso de detección y herramientas de registro de incidentes
4. Establecimiento del nivel de intervención requerido en función del impacto previsible
5. Establecimiento del proceso de resolución y recuperación de los sistemas
6. Proceso para la comunicación del incidente a terceros

UNIDAD DIDÁCTICA 3. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas
4. Guía para el análisis de las evidencias electrónicas recogidas
5. Guía para la selección de las herramientas de análisis forense

UNIDAD DIDÁCTICA 4. SOPORTE DE DATOS

1. Adquisición de datos: importancia en el análisis forense digital
2. Modelo de capas
3. Recuperación de archivos borrados
4. Análisis de archivos

MÓDULO 7. SEGURIDAD EN DESARROLLO WEB

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA SEGURIDAD WEB

1. ¿Qué es la seguridad web?
2. Amenazas para un sitio web
3. Consejos para mantener un sitio web seguro
4. Otros consejos de seguridad web
5. Proveedores de alojamiento web seguros

UNIDAD DIDÁCTICA 2. OWASP DEVELOPMENT

1. ¿Qué es OWASP? ¿Y OWASP Development?

2. ¿Qué es ASVS?
3. Uso del ASVS
4. Requisitos de arquitectura, diseño y modelado de amenazas
5. Requisitos de verificación de autenticación
6. Requisitos de verificación de gestión de sesión
7. Requisitos de verificación de control de acceso
8. Requisitos de validación, desinfección y verificación de la codificación
9. Requisitos de verificación de criptografía almacenados
10. Requisitos de manejo de verificaciones y registro de errores
11. Requisitos de verificación de protección de datos
12. Requisitos de verificación de comunicaciones
13. Requisitos de verificación de código malicioso
14. Requisitos de verificación de lógica de negocios
15. Requisitos de verificación de archivos y recursos
16. Requisitos de verificación de API y servicio web
17. Requisitos de verificación de configuración
18. Requisitos de verificación de Internet de las Cosas
19. Glosario de términos

#### UNIDAD DIDÁCTICA 3. OWASP TESTING GUIDE

1. Aspectos introductorios
2. La Guía de Pruebas de OWASP
3. El framework de pruebas de OWASP
4. Pruebas de seguridad de aplicaciones web
5. Reportes de las pruebas

#### UNIDAD DIDÁCTICA 4. OWASP CODE REVIEW

1. Aspectos introductorios
2. Revisión de código seguro
3. Metodología

#### UNIDAD DIDÁCTICA 5. OWASP TOP TEN

1. Broken Access Control - Control de acceso roto (A01:2021)
2. Cryptographic Failures - Fallos criptográficos (A02:2021)
3. Injection - Inyección (A03:2021)
4. Insecure Design - Diseño Inseguro (A04:2021)
5. Security Misconfiguration - Configuración incorrecta de seguridad (A05:2021)
6. Vulnerable and Outdated Components - Componentes vulnerables y obsoletos (A06:2021)
7. Identification and Authentication Failures - Fallos de Identificación y Autenticación (A07:2021)
8. Software and Data Integrity Failures - Fallos de integridad de software y datos (A08:2021)
9. Security Logging and Monitoring Failures - Registro de seguridad y fallos de monitoreo (A09:2021)
10. Server-Side Request Forgery (SSRF) - Falsificación de solicitud del lado del servidor (A10:2021)

#### MÓDULO 8. PROYECTO FINAL

## ¿Te ha parecido interesante esta información?

Si aún tienes dudas, nuestro equipo de asesoramiento académico estará encantado de resolverlas.

Pregúntanos sobre nuestro método de formación, nuestros profesores, las becas o incluso simplemente conócenos.

## Solicita información sin compromiso

### Teléfonos de contacto

España		+34 900 831 200	Argentina		54-(11)52391339
Bolivia		+591 50154035	Estados Unidos		1-(2)022220068
Chile		56-(2)25652888	Guatemala		+502 22681261
Colombia		+57 601 50885563	Mexico		+52-(55)11689600
Costa Rica		+506 40014497	Panamá		+507 8355891
Ecuador		+593 24016142	Perú		+51 1 17075761
El Salvador		+503 21130481	República Dominicana		+1 8299463963

### !Encuétranos aquí!

Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH,  
C.P. 18.200, Maracena (Granada)

 [formacion@euroinnova.com](mailto:formacion@euroinnova.com)

 [www.euroinnova.com](http://www.euroinnova.com)

### Horario atención al cliente

Lunes a viernes: 9:00 a 20:00h Horario España

Ver en la web

¡Síguenos para estar al tanto de todas nuestras novedades!



Ver en la web

