INESEM

BUSINESS SCHOOL

Máster en Seguridad Ofensiva, Hacking Ético y Ciberseguridad

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Máster en Seguridad Ofensiva, Hacking Ético y Ciberseguridad

duración total: 1.500 horas ***horas teleformación:*** 450 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

En la actualidad, las organizaciones de todo el mundo se enfrentan constantemente a decenas de ataques informáticos. Debido a la extrema digitalización a la que estamos sometidos, estos ataques cibernéticos son cada vez más frecuentes y representan un mayor peligro.
Esta problemática hace que, cada vez más, los profesionales en este sector estén más cotizados, por lo que tener una buena formación se torna fundamental para prevenir y hacer frente a este tipo de prácticas maliciosas que tanto daño causan.
Desde INESEM te ofrecemos este master en Seguridad Ofensiva, Hacking Ético y Ciberseguridad donde aprenderás cómo prevenir estos ataques fortificando los sistemas para minimizar riesgos, cómo solucionarlos una vez se han producido y cómo gestionarlos una vez se han solucionado.

a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Conocer las bases de la ciberseguridad.
- Manejar sistemas SIEM.
- Controlar y contener el malware.
- Responder ante incidentes de seguridad.
- Realizar análisis forense.
- Adentrarse en el hacking ético.
- Analizar la seguridad en la industria 4.0.

para qué te prepara

Este Master en Seguridad Ofensiva, Hacking Ético y Ciberseguridad te prepara para desarrollarte en uno de los campos más solicitados en la actualidad: la ciberseguridad enfocada a la seguridad ofensiva y el hacking ético. Aprenderás todo lo necesario sobre los sistemas SIEM, la detección y notificación de intrusiones en nuestros sistemas, el análisis forense y la seguridad en la industria 4.0.

salidas laborales

Las principales salidas profesionales a las que podrás optar con este Master en Seguridad Ofensiva, Hacking Ético y Ciberseguridad son las de experto en ciberseguridad, así como cualquier posición donde se requiera amplio conocimiento de seguridad informática, hacking ético y/o seguridad ofensiva.

titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).

INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) de (año)

La direccion General

MARIA MORENO HIDALGO

Sello

Firma del alumno/a

NOMBRE DEL ALUMNO/A

forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'Ciberseguridad: Normativa, Política de Seguridad y Ciberinteligencia'
- Manual teórico 'Herramientas, Técnicas de Ciberseguridad y Sistemas SIEM'
- Manual teórico 'Hacking Ético y Auditoría Informática'
- Manual teórico 'Gestión de Incidentes y Análisis Forense'
- Manual teórico 'Desarrollo Web Seguro Vol. I'
- Manual teórico 'Ciberseguridad Aplicada a Inteligencia Artificial (IA), Smartphones, Internet de las Cosas
- Manual teórico 'Desarrollo Web Seguro Vol. II'
- Manual teórico 'Cracking o Ingeniería Inversa'


Cuaderno
de Ejercicios
Manual
de Alumno
INESEM
FORMACIÓN
CONTINUA.EU

profesorado y servicio de tutorías

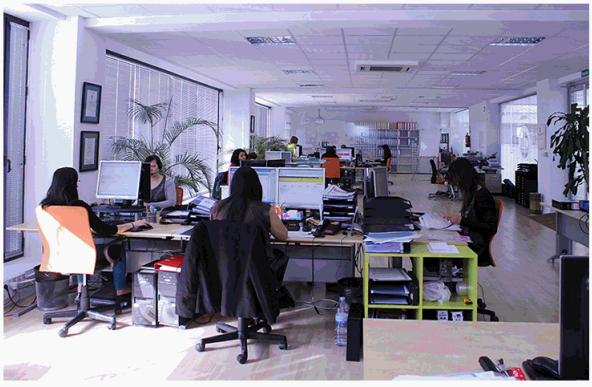
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio. Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail**: El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.

- **Por teléfono**: Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.

- **A través del Campus Virtual**: El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como disponer de toda su documentación



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de inesem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

programa formativo

MÓDULO 1. CIBERSEGURIDAD: NORMATIVA, POLÍTICA DE SEGURIDAD 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 2. HERRAMIENTAS, TÉCNICAS DE CIBERSEGURIDAD Y SISTEMAS SIEM

UNIDAD DIDÁCTICA 1. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1.Seguridad a Nivel Físico
2.Seguridad a Nivel de Enlace
3.Seguridad a Nivel de Red
4.Seguridad a Nivel de Transporte

5.Seguridad a Nivel de Aplicación

UNIDAD DIDÁCTICA 2. CRIPTOGRAFÍA

1.Perspectiva histórica y objetivos de la criptografía
2.Teoría de la información
3.Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía
4.Criptografía de clave privada o simétrica
5.Criptografía de clave pública o asimétrica
6.Algoritmos criptográficos más utilizados
7.Funciones hash y los criterios para su utilización
8.Protocolos de intercambio de claves
9.Herramientas de cifrado

UNIDAD DIDÁCTICA 3. 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 4. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1.Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2.Identificación y caracterización de los datos de funcionamiento del sistema
3.Arquitecturas más frecuentes de los IDS
4.Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5.Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 5. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1.Análisis previo
2.Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3.Análisis de los eventos registrados por el IDS/IPS
4.Relación de los registros de auditoría del IDS/IPS
5.Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 6. INTRODUCCIÓN A LOS SISTEMAS SIEM

1.¿Qué es un SIEM?
2.Evolución de los sistemas SIEM: SIM, SEM y SIEM
3.Arquitectura de un sistema SIEM

UNIDAD DIDÁCTICA 7. CAPACIDADES DE LOS SISTEMAS SIEM

1.Problemas a solventar
2.Administración de logs
3.Regulaciones IT
4.Correlación de eventos
5.Soluciones SIEM en el mercado

MÓDULO 3. HACKING ÉTICO Y AUDITORÍA INFORMÁTICA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y CONCEPTOS PREVIOS

1.¿Qué es el hacking ético?
2.Aspectos legales del hacking ético
3.Perfiles del hacker ético

UNIDAD DIDÁCTICA 2. FASES DEL HACKING ÉTICO EN LOS ATAQUES A SISTEMAS Y REDES

1.Tipos de ataques
2.Herramientas de hacking ético
3.Tests de vulnerabilidades

UNIDAD DIDÁCTICA 3. FASES DEL HACKING ÉTICO EN LOS ATAQUES A REDES WIFI

1.Tipos de ataques
2.Herramientas de hacking ético
3.Tipos de seguridad WiFi
4.Sniffing

UNIDAD DIDÁCTICA 4. FASES DEL HACKING ÉTICO EN LOS ATAQUES WEB

1.Tipos de ataques
2.Herramientas de hacking ético
3.Tipos de seguridad web
4.Tipo de test de seguridad en entornos web

UNIDAD DIDÁCTICA 5. AUDITORÍA DE SEGURIDAD INFORMÁTICA

1.Criterios Generales
2.Aplicación de la normativa de protección de datos de carácter personal
3.Herramientas para la auditoría de sistemas
4.Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
5.Guías para la ejecución de las distintas fases de la auditoría de sistemas de información

MÓDULO 4. 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 event 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 5. 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 6. DESARROLLO WEB SEGURO

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 7. CIBERSEGURIDAD APLICADA A INTELIGENCIA ARTIFICIAL (IA), SMARTPHONES, INTERNET DE LAS COSAS (IOT) E INDUSTRIA 4.0

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD EN NUEVAS TECNOLOGÍAS

1.Concepto de seguridad TIC
2.Tipos de seguridad TIC
3.Aplicaciones seguras en Cloud
4.Plataformas de administración de la movilidad empresarial (EMM)
5.Redes WiFi seguras
6.Caso de uso: Seguridad TIC en un sistema de gestión documental

UNIDAD DIDÁCTICA 2. CIBERSEGURIDAD EN SMARTPHONES

1.Buenas prácticas de seguridad móvil
2.Protección de ataques en entornos de red móv

UNIDAD DIDÁCTICA 3. INTELIGENCIA ARTIFICIAL (IA) Y CIBERSEGURIDAD

1.Inteligencia Artificial
2.Tipos de inteligencia artificial
3.Impacto de la Inteligencia Artificial en la ciberseguridad

UNIDAD DIDÁCTICA 4. CIBERSEGURIDAD E INTERNET DE LAS COSAS (IOT)

1.Contexto Internet de las Cosas (IoT)
2.¿Qué es IoT?
3.Elementos que componen el ecosistema IoT
4.Arquitectura IoT
5.Dispositivos y elementos empleados
6.Ejemplos de uso
7.Retos y líneas de trabajo futuras
8.Vulnerabilidades de IoT
9.Necesidades de seguridad específicas de IoT

UNIDAD DIDÁCTICA 5. SEGURIDAD INFORMÁTICA EN LA INDUSTRIA 4.0

1.Industria 4.0
2.Necesidades en ciberseguridad en la Industria 4.0

MÓDULO 8. PROYECTO FIN DE MÁSTER