Masters con Reconocimiento Universitario

Master de Formación Permanente en Seguridad Informática y Hacking Ético + 60 Créditos ECTS

INESEM BUSINESS SCHOOL

INESEM BUSINESS SCHOOL

Índice

Master de Formación Permanente en Seguridad Informática y Hacking Ético + 60 Créditos ECTS

SOBRE INESEM BUSINESS SCHOOL

INESEM Business School como Escuela de Negocios Online tiene por objetivo desde su nacimiento trabajar para fomentar y contribuir al desarrollo profesional y personal de sus alumnos. Promovemos ***una enseñanza multidisciplinar e integrada***, mediante la aplicación de ***metodologías innovadoras de aprendizaje*** que faciliten la interiorización de conocimientos para una aplicación práctica orientada al cumplimiento de los objetivos de nuestros itinerarios formativos.

En definitiva, en INESEM queremos ser el lugar donde te gustaría desarrollar y mejorar tu carrera profesional. ***Porque sabemos que la clave del éxito en el mercado es la "Formación Práctica" que permita superar los retos que deben de afrontar los profesionales del futuro.***

Master de Formación Permanente en Seguridad Informática y Hacking Ético + 60 Créditos ECTS

DURACIÓN	1500
PRECIO	1970 €
CRÉDITOS ECTS	60
MODALIDAD	Online

Programa de Becas / Financiación 100% Sin Intereses

Entidad impartidora:

INESEM BUSINESS SCHOOL

UNIVERSIDAD NEBRIJA

Titulación Masters con Reconocimiento Universitario

Doble Titulación:

- Titulación Propia Universitaria de Master de Formación Permanente en Seguridad Informática y Hacking Ético expedida por la Universidad Antonio de Nebrija con 60 créditos ECTS.

- Titulación propia de Master de Formación Permanente en Seguridad Informática y Hacking Ético, expedida y avalada por el Instituto Europeo de Estudios Empresariales.(INESEM) “Enseñanza no oficial y no conducente a la obtención de un título con carácter oficial o certificado de profesionalidad.”

Resumen

En la era de los grandes volúmenes de información y la continua transmisión de datos a través de la red en la que nos encontramos inmersos, quizás sea precisamente este activo empresarial el de mayor valor dentro de la organización. Es por este motivo, que el robo de la información o el ataque sobre las infraestructuras son los puntos calientes y objetivos de los hackers.Este máster te permite asimilar los objetivos y técnicas necesarias para desarrollarte como hacker ético y analizar los puntos débiles de las organizaciones mediante procesos de auditoría y la elaboración de informes periciales. Te capacitará para adoptar la mejor solución sin perder de vista la escalabilidad de los datos y la seguridad de la información que conlleva el proceso de gestión de incidentes.En INESEM podrás trabajar en un Entorno Personal de Aprendizaje donde el alumno es el protagonista, avalado por un amplio grupo de tutores especialistas en el sector.

A quién va dirigido

El Master Seguridad Informática y Hacking Ético va dirigido a titulados/as universitarios/as y deseen ampliar o actualizar sus conocimientos informáticos en el ámbito de la seguridad informática.

Objetivos

Con el Masters con Reconocimiento Universitario **Master de Formación Permanente en Seguridad Informática y Hacking Ético + 60 Créditos ECTS** usted alcanzará los siguientes objetivos:

- Conocer la legislación vigente en materia de seguridad informática.
- Analizar los diferentes tipos de ataques a los sistemas y las técnicas para afrontarlos.
- Aplicar los sistemas IDS/IPS para la gestión de incidentes de seguridad.
- Aprender las distintas técnicas y herramientas del hacking ético.
- Aplicar las técnicas necesarias para mantener la seguridad de la información y los requisitos legales que conlleva.

¿Y, después?

Para qué te prepara

El Master Seguridad Informática y Hacking Ético te preparada para hacer uso de herramientas y técnicas de ciberseguridad como la criptografía. Podrás gestionar incidentes implantando sistemas IDS-IPS y operar ante los malwares. Aprenderás las herramientas de Cracking y las fases de Hacking Ético en los distintos posibles ataques, además de los sistemas SIEM y de control para mejorar la seguridad. También sabrás realizar informes periciales.

Salidas Laborales

Con la realización de este Master Seguridad Informática y Hacking Ético podrás desarrollar tu carrera profesional como administrador de seguridad informática, consultor en seguridad informática, diseñador de sistema de seguridad, analista de riesgos de seguridad, técnico en administración de sistemas informáticos, en ámbitos como departamentos de informática de empresas públicas y privadas.

¿Por qué elegir INESEM?

El alumno es el protagonista

01

Nuestro modelo de aprendizaje se adapta a las necesidades del alumno, quién decide cómo realizar el proceso de aprendizaje a través de itinerarios formativos que permiten trabajar de forma autónoma y flexible.

Innovación y Calidad

Ofrecemos un servicio de orientación profesional y programas de entrenamiento de competencias con el que ayudamos a nuestros alumnos a crear y optimizar su perfil profesional.

02

Empleabilidad y desarrollo profesional

03

Ofrecemos el contenido más actual y novedoso, respondiendo a la realidad empresarial y al entorno cambiante con una alta rigurosidad académica combinada con formación práctica.

INESEM Orienta

Ofrecemos una asistencia complementaria y personalizada que impulsa la carrera de nuestros alumnos a través de nuestro Servicio de Orientación de Carrera Profesional permitiendo la mejora de competencias profesionales mediante programas específicos.

04

Facilidades Económicas y Financieras

05

Ofrecemos a nuestros alumnos facilidades para la realización del pago de matrículas 100% sin intereses así como un sistema de Becas para facilitar el acceso a nuestra formación.

PROGRAMA ACADÉMICO

Master de Formación Permanente en Seguridad Informática y Hacking Ético + 60 Créditos ECTS

Módulo 1. **Ciberseguridad: normativa, política de seguridad y ciberinteligencia**

Módulo 2. **Herramientas de ciberseguridad osint**

Módulo 3. **Redes informáticas: arquitectura, protocolos y ciberseguridad**

Módulo 4. **Criptografía y redes privadas virtuales (vpn)**

Módulo 5. **Análisis de malware, cracking e ingeniería inversa**

Módulo 6. **Pentesting y hacking tools**

Módulo 7. **Hacking training platforms**

Módulo 8. **Cibercrimen**

Módulo 9. **Ciberdelitos**

Módulo 10. **Análisis forense y herramientas para peritaje informático**

Módulo 11. **Proyecto fin de master**

PROGRAMA ACADÉMICO

Master de Formación Permanente en Seguridad Informática y Hacking Ético + 60 Créditos ECTS

Módulo 1.

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 27001 e ISO 27002
2. Legislación: Leyes aplicables a los SGSI (RGPD)

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 al phishing
7. Phishing
8. Man in the middle

Unidad didáctica 5.

Ciberinteligencia y 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

Módulo 2.
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 3.
Redes informáticas: arquitectura, protocolos y ciberseguridad

Unidad didáctica 1.
Introducción a la red

1. Elementos principales de una red
2. Tecnología de redes
3. Soporte para la continuidad de la actividad

Unidad didáctica 2.
Estandarización de protocolos

1. Modelo OSI
2. Enfoque pragmático del modelo de capas
3. Estándares y organismos

Unidad didáctica 3.
Transmisión de datos en la capa física

1. Papel de una interfaz de red
2. Opciones y parámetros de configuración
3. Arranque desde la red
4. Codificación de los datos
5. Conversión de las señales
6. Soportes de transmisión

Unidad didáctica 4.
Software de comunicación

1. Configuración de la tarjeta de red
2. Instalación y configuración del controlador de la tarjeta de red
3. Pila de protocolos
4. Detección de un problema de red

Unidad didáctica 5.
Arquitectura de red e interconexión

1. Topologías
2. Elección de la topología de red adaptada
3. Gestión de la comunicación
4. Interconexión de redes

Unidad didáctica 6.
Capas bajas de las redes personales y locales

1. Capas bajas e IEEE
2. Ethernet e IEEE 802.3
3. Token Ring e IEEE 802.5
4. Wi-Fi e IEEE 802.11
5. Bluetooth e IEEE 802.15
6. Otras tecnologías

Unidad didáctica 7.
Redes man y wan, protocolos

1. Interconexión de la red local
2. Acceso remoto y redes privadas virtuales

Unidad didáctica 8.
Protocolos de capas medias y altas

1. Principales familias de protocolos
2. Protocolo IP versión 4
3. Protocolo IP versión 6
4. Otros protocolos de capa Internet
5. Voz sobre IP (VoIP)
6. Protocolos de transporte TCP y UDP
7. Capa de aplicación TCP/IP

Unidad didáctica 9.
Protección de una red

1. Comprensión de la necesidad de la seguridad
2. Herramientas y tipos de ataque
3. Conceptos de protección en la red local
4. Protección de la interconexión de redes

Unidad didáctica 10.
Reparación de red

1. Introducción a la reparación de red
2. Diganóstico en capas bajas
3. Utilización de herramientas TCP/IP adaptadas
4. Herramientas de análisis de capas altas

Unidad didáctica 11.

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 12.

Aplicación de una infraestructura de clave pública (pki)

1. Identificación de los componente 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 13.

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 14.

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 15.

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 16.

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 4.
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 Dígitales

Unidad didáctica 6.
Protocolos criptográficos y firmas digitales

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

Unidad didáctica 7.
Diferentes aplicaciones de la criptografía de clave pública

1. Aplicaciones de la criptografía pública y privada
2. Certificado dígital
3. DNI Electrónico
4. Bitcoin

Unidad didáctica 8.
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 9.
Hashing

Unidad didáctica 10.
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 11.
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 12.
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 13.
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 14.
Protocolos de tunelización vpn

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

Unidad didáctica 15.
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 16.
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 5.
Análisis de malware, cracking e ingeniería inversa

Unidad didáctica 1.
Introducción al análisis de malware

Unidad didáctica 2.
Técnicas y herramientas para análisis de malware

Unidad didáctica 3.
Control malware

1. Sistemas de detección y contención de Malware
2. Herramientas de control de Malware
3. Criterios de seguridad para la configuración de las herramientas de protección frente a Malware
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a Malware
5. Relación de los registros de auditoría de las herramientas de protección frente a Malware
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a Malware
7. Análisis de Malware mediante desensambladores y entornos de ejecución controlada

Unidad didáctica 4.
Fundamentos de la ingeniería inversa

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

Unidad didáctica 5.
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 6.
Herramientas de ingeniería inversa

1. Ghidra
2. IDA
3. Winhex
4. Hiew
5. x64dbg
6. Radare2
7. Cutter

Unidad didáctica 7.
Introducción al cracking

Unidad didáctica 8.
Herramientas de cracking

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

Módulo 6.
Pentesting y hacking tools

Unidad didáctica 1.
Introducción al hacking ético

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.
Kali linux

Unidad didáctica 6.
Nmap

Unidad didáctica 7.
Metasploit

Unidad didáctica 8.
Wireshark

Unidad didáctica 9.
John the ripper

Unidad didáctica 10.
Hashcat

Unidad didáctica 11.
Hydra

Unidad didáctica 12.
Burp suite

Unidad didáctica 13.
Zed attack proxy

Unidad didáctica 14.
Sqlmap

Unidad didáctica 15.
Aircrack-ng

Módulo 7.
Hacking training platforms

Unidad didáctica 1.
Introducción a hacking training platforms

1. ¿Qué es el hacking ético?
2. Máquinas virtuales
3. Plataformas para practicar hacking ético

Unidad didáctica 2.
Hack the box (htb)

1. Introducción a Hack The Box
2. Crear una cuenta
3. Tutoriales

Unidad didáctica 3.
Tryhackme

1. ¿Qué es TryHackMe?
2. Crear una cuenta
3. Interfaz de TryHackMe
4. Introducción a la ciberseguridad
5. Seguridad ofensiva
6. Ciencia forense digital

Unidad didáctica 4.
Hacker101

1. ¿Qué es Hacker101?
2. Hacker101 CTF
3. Tutoriales

Unidad didáctica 5.
Vulnhub

1. ¿Qué es Vulnhub?
2. Interfaz de Vulnhub
3. Tutoriales

Unidad didáctica 6.
Hack this site

1. ¿Qué es Hack This Suite?
2. Desafíos Hack This Site

Unidad didáctica 7.
Google xss game

1. ¿Qué es Google XSS Game?
2. Niveles de Google XSS game

Unidad didáctica 8.
Hackthis

1. ¿Qué es HackThis?
2. Tutorial HackThis
3. Basic+

Módulo 8.
Cibercrimen

Unidad didáctica 1.
¿qué son los delitos informáticos?

1. Concepto de delincuencia informática y cibercriminalidad
2. ¿Qué es el cibercrimen?
3. Tipos de cibercrimen

Unidad didáctica 2.
Clasificación atendiendo a la incidencia de las tic

1. Ciberataques puros
2. Ciberataques réplica
3. Ciberataques de contenido

Unidad didáctica 3.
Clasificación atendiendo al móvil criminológico

1. Cibercrimen económico
2. Cibercrimen social
3. Cibercrimen político

Unidad didáctica 4.
¿qué es el ciberespacio?

1. Arquitectura del ciberespacio
2. Teoría criminológica y cibercrimen

Unidad didáctica 5.
Cibervíctima

1. La importancia de la víctima en el cibercrimen
2. Prevención del cibercrimen
3. Multiplicidad de cibervíctimas
4. Victimización en el ciberespacio

Unidad didáctica 6.
Ciberdelincuente

1. ¿Cuál es el perfil común de un ciberdelincuente?
2. Especialidades de ciberdelincuente

Unidad didáctica 7.
El cibercrimen como problema internacional

1. Seguridad cibernética
2. Deep web
3. Cooperación Internacional en asuntos de seguridad cibernética
4. Prevención del delito cibernético

Módulo 9.
Ciberdelitos

Unidad didáctica 1.
Privacidad y protección de datos

1. ¿Por qué es importante la privacidad?
2. Privacidad y Seguridad
3. Ciberdelitos que comprometen la privacidad
4. Normativa sobre privacidad y protección de datos

Unidad didáctica 2.
Propiedad intelectual

1. ¿Qué es la propiedad intelectual?
2. Tipos de propiedad intelectual
3. Teorías criminológicas en delitos contra la propiedad intelectual por medios cibernéticos

Unidad didáctica 3.
Delincuencia organizada

1. Delincuencia cibernética organizada y actores que intervienen
2. Perfil de los grupos delictivos
3. Actividades de los ciberdelitos organizados
4. Prevención de este tipo de ciberdelitos

Unidad didáctica 4.
Trata de personas y tráfico ilícito de inmigrantes

1. ¿La tecnología facilita este tipo de delitos?
2. Trata de personas y tráfico ilícito de inmigrantes como ciberdelito organizado

Unidad didáctica 5.
Ciberdelitos contra las personas

1. Explotación y abuso sexual infantil
2. Hostigamiento
3. Acoso
4. Violencia de género

Unidad didáctica 6.
Ciberterrorismo

1. Hacktivismo
2. Ciberespionaje
3. Ciberterrorismo
4. Guerra cibernética
5. La guerra de la información, la desinformación y el fraude electoral

Módulo 10.
Análisis forense y herramientas para peritaje informático

Unidad didáctica 1.
Análisis forense de dispositivos físicos informáticos

Unidad didáctica 2.
Análisis forense en windows

Unidad didáctica 3.
Análisis forense en gnu/linux

Unidad didáctica 4.
Análisis forense en mac os

Unidad didáctica 5.
Análisis forense en android

Unidad didáctica 6.
Análisis forense en ios

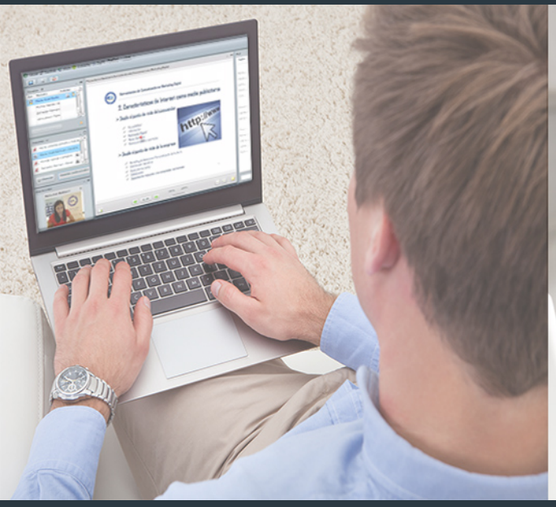
Unidad didáctica 7.
Análisis forense de emails, whatsapps y otras comunicaciones

Unidad didáctica 8.
Informe pericial

Módulo 11.
Proyecto fin de master

metodología de aprendizaje

La configuración del modelo pedagógico por el que apuesta INESEM, requiere del uso de herramientas que favorezcan la colaboración y divulgación de ideas, opiniones y la creación de redes de conocimiento más colaborativo y social donde los alumnos complementan la formación recibida a través de los canales formales establecidos.



Con nuestra metodología de aprendizaje online, el alumno comienza su andadura en INESEM Business School a través de un campus virtual diseñado exclusivamente para desarrollar el itinerario formativo con el objetivo de mejorar su perfil profesional. El alumno debe avanzar de manera autónoma a lo largo de las diferentes unidades didácticas así como realizar las actividades y autoevaluaciones correspondientes.

El 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.

Nuestro sistema de aprendizaje se fundamenta en *cinco pilares* que facilitan el estudio y el desarrollo de competencias y aptitudes de nuestros alumnos a través de los siguientes entornos:

Secretaría

Sistema que comunica al alumno directamente con nuestro asistente virtual permitiendo realizar un seguimiento personal de todos sus trámites administrativos.

Campus Virtual

Entorno Personal de Aprendizaje que permite gestionar al alumno su itinerario formativo, accediendo a multitud de recursos complementarios que enriquecen el proceso formativo así como la interiorización de conocimientos gracias a una formación práctica, social y colaborativa.

Revista Digital

Espacio de actualidad donde encontrar publicaciones relacionadas con su área de formación. Un excelente grupo de colabradores y redactores, tanto internos como externos, que aportan una dosis de su conocimiento y experiencia a esta red colaborativa de información.

Comunidad

Espacio de encuentro que pemite el contacto de alumnos del mismo campo para la creación de vínculos profesionales. Un punto de intercambio de información, sugerecias y experiencias de miles de usuarios.

Webinars

Píldoras formativas mediante el formato audiovisual para complementar los itinerarios formativos y una práctica que acerca a nuestros alumnos a la realidad empresarial.

SERVICIO DE **Orientación** de Carrera

Nuestro objetivo es el asesoramiento para el desarrollo de tu carrera profesional. Pretendemos capacitar a nuestros alumnos para su adecuada adaptación al mercado de trabajo facilitándole su integración en el mismo. Somos el aliado ideal para tu crecimiento profesional, aportando las capacidades necesarias con las que afrontar los desafíos que se presenten en tu vida laboral y alcanzar el éxito profesional. Gracias a nuestro Departamento de Orientación de Carrera se gestionan más de 500 convenios con empresas, lo que nos permite contar con una plataforma propia de empleo que avala la continuidad de la formación y donde cada día surgen nuevas oportunidades de empleo. Nuestra bolsa de empleo te abre las puertas hacia tu futuro laboral.

Financiación y becas

En INESEM

Ofrecemos a nuestros alumnos facilidades económicas y financieras para la realización del pago de matrículas,

todo ello
100%
sin intereses.

INESEM continúa ampliando su programa de becas para acercar y posibilitar el aprendizaje continuo al máximo número de personas. Con el fin de adaptarnos a las necesidades de todos los perfiles que componen nuestro alumnado.

Masters con Reconocimiento Universitario

Master de Formación Permanente en Seguridad Informática y Hacking Ético + 60 Créditos ECTS