Cursos Superiores

Curso Superior en Gestión de Incidencias y Auditoría de Seguridad Informática

INESEM BUSINESS SCHOOL

Índice

Curso Superior en Gestión de Incidencias y Auditoría de Seguridad Informática

1. Sobre INESEM
2. Curso Superior en Gestión de Incidencias y Auditoría de Seguridad Informática

Descripción / Para que te prepara / Salidas Laborales / Resumen / A quién va dirigido / Objetivos

3. Programa académico
4. Metodología de Enseñanza
5. ¿Por qué elegir INESEM?
6. Orientación
7. Financiación y Becas

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.***

Curso Superior en Gestión de Incidencias y Auditoría de Seguridad Informática

DURACIÓN	300
PRECIO	460 €
MODALIDAD	Online

Entidad impartidora:

INESEM BUSINESS SCHOOL

Programa de Becas / Financiación 100% Sin Intereses

Titulación Cursos Superiores

- Título Propio del 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 actualidad unos de los principales activos de las empresas es la información que maneja, información que se gestiona con dispositivos conectados a la red y que por tanto son vulnerables a ataques y robo mediante lo que se conoce como ciberdelincuencia. Una mala gestión de la seguridad puede por tanto dañar la imagen de una empresa mermando su reputación y la marca que representa.Con esta acción formativa podrá desarrollarse como profesional de la seguridad implantando sistemas de detección y prevención de intrusiones (IDS/IPS), que le permitirán tener un control del malware así como llevar a cabo técnicas de análisis forense.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

Los profesionales dedicados al área de la informática y las TICS, como Ingenieros Informáticos, Ingenieros de Telecomunicaciones, entre otros, son los principales beneficiarios del Curso Gestión de Incidencias y Auditoría de Seguridad Informática. Del mismo modo, cualquier persona interesada en este ámbito podrá realizar el presente curso.

Objetivos

Con el Cursos Superiores **Curso Superior en Gestión de Incidencias y Auditoría de Seguridad Informática** usted alcanzará los siguientes objetivos:

- Dominar la normativa esencial sobre el sistema de gestión de la seguridad de la información.
- Conocer las herramientas para la auditoría de seguridad informática.
- Conocer los criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS.
- Dominar el sistema de detección y contención de Malware y sus herramientas.
- Llevar a cabo la categorización de los incidentes derivados de intentos de intrusión.
- Conocer los conceptos generales y los objetivos del análisis forense.

¿Y, después?

Para qué te prepara

El Curso Gestión de Incidencias y Auditoría de Seguridad Informática, proporciona al alumnado los conocimientos necesarios para su correcta introducción en la gestión de sistemas de seguridad de la información y ciberinteligencia, por medio del análisis de gestión de riesgos y de la auditoría de seguridad. Además, el alumno será capaz de llevar a cabo el proceso de notificación y gestión de intentos de intrusión y el análisis forense informático.

Salidas Laborales

Tras la correcta realización del Curso Gestión de Incidencias y Auditoría de Seguridad Informática, el alumno podrá realizar su profesión, tanto de forma propia como ajena, ocupando puestos de trabajo como Analista de Seguridad Informática, Auditor de Seguridad Informática, Consultor de Ciberseguridad, Analista de Malware, Forense Informático, entre otros.

¿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.

Módulo 1. **Legislación, política de seguridad y ciberinteligencia**

Módulo 2. **Herramientas, técnicas de ciberseguridad y sistemas siem**

Módulo 3. **Hacking ético y auditoría informática**

Módulo 4. **Gestión de incidentes y análisis forense**

Módulo 1.
Legislación, 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, 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 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

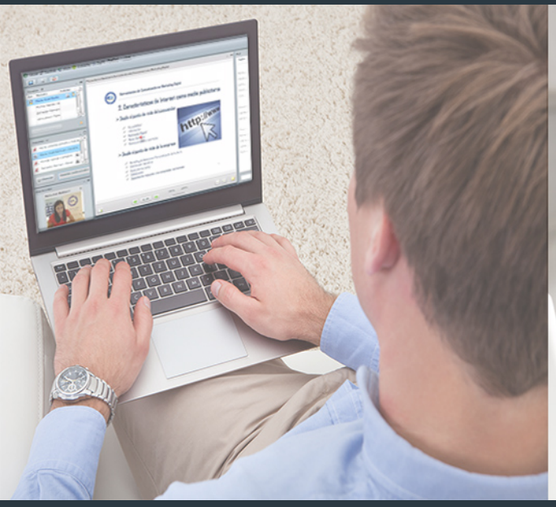
Unidad didáctica 4.

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

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.

Cursos Superiores

Curso Superior en Gestión de Incidencias y Auditoría de Seguridad Informática

Impulsamos tu carrera profesional

INESEM

BUSINESS SCHOOL

www.inesem.es

958 05 02 05 formacion@inesem.es

Gestionamos acuerdos con más de 2000 empresas y tramitamos más de 500 ofertas profesionales al año.
Facilitamos la incorporación y el desarrollo de los alumnos en el mercado laboral a lo largo de toda su carrera profesional.