



INESEM

BUSINESS SCHOOL

***Curso en Auditoría y Seguridad Informática
(Titulación Universitaria + 8 Créditos ECTS)***

+ Información Gratis

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

Curso en Auditoría y Seguridad Informática (Titulación Universitaria + 8 Créditos ECTS)

duración total: 200 horas

horas teleformación: 100 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Este CURSO HOMOLOGADO DE AUDITORÍA Y SEGURIDAD INFORMÁTICA trata sobre la seguridad informática, que es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial. ES UN CURSO HOMOLOGADO BAREMABLE PARA OPOSICIONES.



a quién va dirigido

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

objetivos

- Conocer el concepto y modelos de seguridad, los tipos de control de acceso, autenticación de datos y posibles ataques a los que pueden estar sometidos los sistemas informáticos.
- Aprender las pautas y ámbitos de aplicación para el Reglamento de Seguridad y la aplicación de sus principales puntos del reglamento en Windows.
- Saber aplicar la ley de protección de datos aplicada en España: los principios de protección de datos y la forma en que se debe aplicar.
- Garantizar la continuidad de las operaciones de los elementos críticos que componen los sistemas de información, mediante acciones y procedimientos.
- Determinar si los planes de contingencia individuales son capaces de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos de la empresa, probando la efectividad de los procedimientos expuestos en el plan de contingencias.
- Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.
- Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.
- Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

para qué te prepara

El CURSO ONLINE HOMOLOGADO DE AUDITORÍA Y SEGURIDAD INFORMÁTICA le prepara para aprender el mundo de la seguridad informática, tanto el control de acceso, los protocolos de comunicación, las transferencias de datos, etc., que son procesos que deben ser estudiados y planificados por los usuarios para la definición de sus políticas de seguridad y la planificación. Al ser un CURSO UNIVERSITARIO está HOMOLOGADO para OPOSICIONES.

salidas laborales

Seguridad Informática.

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 dirección General

MARIA MORENO HIDALGO

Firma del alumno/a

Sello



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 'Seguridad Informática. Vol II'
- Manual teórico 'Gestión de Incidentes de Seguridad Informática'
- Manual teórico 'Seguridad Informática. Vol I'

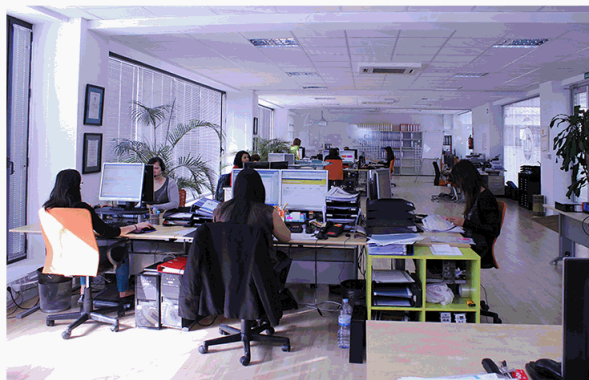


profesorado y servicio de tutorías

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: SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y CONCEPTOS BÁSICOS

- 1.La sociedad de la información
- 2.Diseño, desarrollo e implantación
- 3.Factores de éxito en la seguridad de la información

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
- 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. 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

UNIDAD DIDÁCTICA 5. 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 6: CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

- 1.Identificación de los dispositivos de comunicaciones
- 2.Análisis de los protocolos y servicios de comunicaciones
- 3.Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
- 4.Procesos de monitorización y respuesta
- 5.Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
- 6.Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
- 7.Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
- 8.Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc)

UNIDAD DIDÁCTICA 7. SISTEMAS SIEM

- 1.¿Qué es un SIEM?
- 2.Evolución de los sistemas SIEM: SIM, SEM y SIEM
- 3.Arquitectura de un sistema SIEM
- 4.Problemas a solventar
- 5.Administración de logs
- 6.Regulaciones IT
- 7.Correlación de eventos
- 8.Soluciones SIEM en el mercado

UNIDAD DIDÁCTICA 8. SEGURIDAD EN ENTORNOS MÓVILES

- 1.Aplicaciones seguras en Cloud
- 2.Protección de ataques en entornos de red móvil
- 3.Plataformas de administración de la movilidad empresarial (EMM)

4.Redes WiFi seguras

MÓDULO 2. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. 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 2. 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 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. 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 5. 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 6. 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