



INESEM

BUSINESS SCHOOL

Auditoría de Seguridad Informática (Online)

+ Información Gratis

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

Auditoría de Seguridad Informática (Online)

duración total: 90 horas

horas teleformación: 56 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Hoy en día la seguridad informática es un tema muy importante y sensible, que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados.

Con la realización del presente curso el alumno aprenderá los conocimientos necesarios para auditar redes de comunicación y sistemas informáticos.



a quién va dirigido

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

objetivos

- Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática.
- Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.
- Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.

para qué te prepara

La presente formación se ajusta al itinerario formativo del Módulo Formativo MF0487_3 Auditoría de Seguridad Informática, certificando el haber superado las distintas Unidades de Competencia en él incluidas, y va dirigido a la acreditación de las Competencias Profesionales adquiridas a través de la experiencia laboral y de la formación no formal, vía por la que va a optar a la obtención del correspondiente Certificado de Profesionalidad, a través de las respectivas convocatorias que vayan publicando las distintas Comunidades Autónomas, así como el propio Ministerio de Trabajo (Real Decreto 659/2023, de 18 de julio, que desarrolla la ordenación del Sistema de Formación Profesional y establece un procedimiento permanente para la acreditación de competencias profesionales adquiridas por experiencia laboral o formación no formal).

salidas laborales

Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

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 'MF0487_3 Auditoría de Seguridad Informática'

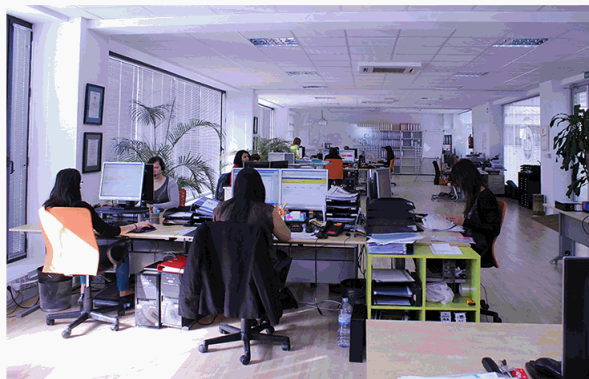


profesorado y servicio de tutorías

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. AUDITORÍA DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

- 1.Código deontológico de la función de auditoría
- 2.Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- 3.Criterios a seguir para la composición del equipo auditor
- 4.Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
- 5.Tipos de muestreo a aplicar durante el proceso de auditoría
- 6.Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
- 7.Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- 8.Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- 9.Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

UNIDAD DIDÁCTICA 2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

- 1.Principios generales de protección de datos de carácter personal
- 2.Normativa europea recogida en la directiva 95/46/CE
- 3.Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
- 4.Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- 5.Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
- 6.Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

UNIDAD DIDÁCTICA 3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

- 1.Introducción al análisis de riesgos
- 2.Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- 3.Particularidades de los distintos tipos de código malicioso
- 4.Principales elementos del análisis de riesgos y sus modelos de relaciones
- 5.Metodologías cualitativas y cuantitativas de análisis de riesgos
- 6.Identificación de los activos involucrados en el análisis de riesgos y su valoración
- 7.Identificación de las amenazas que pueden afectar a los activos identificados previamente
- 8.Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
- 9.Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- 10.Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y efecto sobre las vulnerabilidades y amenazas
- 11.Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializar
- 12.Determinación de la probabilidad e impacto de materialización de los escenarios
- 13.Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- 14.Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
- 15.Relación de las distintas alternativas de gestión de riesgos
- 16.Guía para la elaboración del plan de gestión de riesgos
- 17.Exposición de la metodología NIST SP 800-30
- 18.Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

- 1.Herramientas del sistema operativo tipo Ping, Traceroute, etc
- 2.Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
- 3.Herramientas de análisis de vulnerabilidades tipo Nessus
- 4.Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
- 5.Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
- 6.Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS.

- 1.Principios generales de cortafuegos
- 2.Componentes de un cortafuegos de red
- 3.Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- 4.Arquitecturas de cortafuegos de red
- 5.Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 6. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

- 1.Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
- 2.Guía para la elaboración del plan de auditoría
- 3.Guía para las pruebas de auditoría
- 4.Guía para la elaboración del informe de auditoría