INESEM

BUSINESS SCHOOL

Seguridad en Equipos Informáticos (Online)

+ Información Gratis

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

Seguridad en Equipos Informáticos (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 asegurar equipos 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 los planes de implantación de la organización para identificar los elementos del sistema implicados y los niveles de seguridad a implementar.
- Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad.
- Evaluar la función y necesidad de cada servicio en ejecución en el servidor según las especificaciones de seguridad.
- Instalar, configurar y administrar un cortafuegos de servidor con las características necesarias según especificaciones de seguridad.

para qué te prepara

La presente formación se ajusta al itinerario formativo del Módulo Formativo MF0486_3 Seguridad en Equipos Informáticos, 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 1224/2009 de reconocimiento de las competencias profesionales adquiridas por experiencia laboral)

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 direccion General — Firma del alumno/a

MARIA MORENO HIDALGO — 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 'MF0486_3 Seguridad en Equipos Informáticos'

profesorado y servicio de tutorías

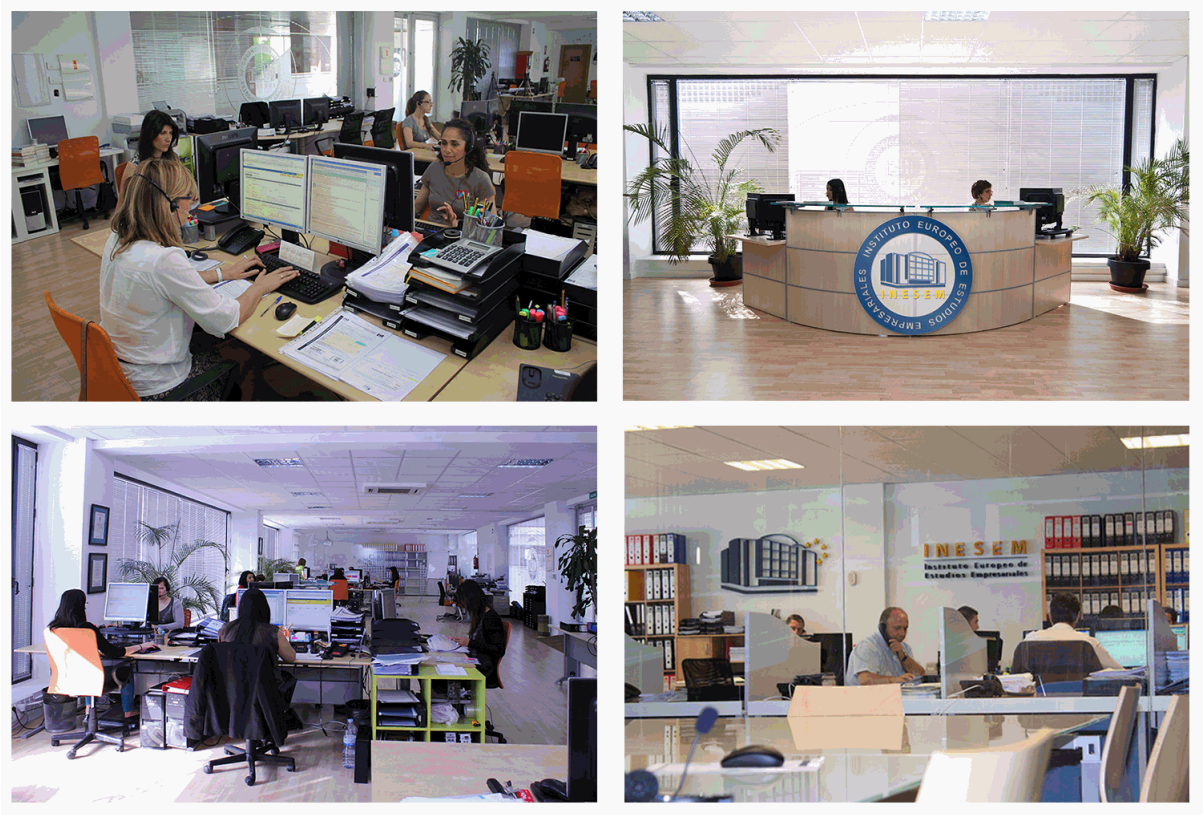
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “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

+ Información Gratis

programa formativo

MÓDULO 1. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1.Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
2.Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
3.Salvaguardas y tecnologías de seguridad más habituales
4.La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

1.Identificación de procesos de negocio soportados por sistemas de información
2.Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
3.Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

1.Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
2.Metodologías comúnmente aceptadas de identificación y análisis de riesgos
3.Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1.Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
2.Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
3.Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1.Principios generales de protección de datos de carácter personal
2.Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
3.Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
4.Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1.Determinación de los perímetros de seguridad física
2.Sistemas de control de acceso físico mas frecuentes a las instalaciones de la organización y a las áreas en las qu estén ubicados los sistemas informáticos
3.Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4.Exposición de elementos mas frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
5.Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
6.Elaboración de la normativa de seguridad física e industrial para la organización
7.Sistemas de ficheros más frecuentemente utilizados
8.Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organizació
9.Configuración de políticas y directivas del directorio de usuarios
10.Establecimiento de las listas de control de acceso (ACLs) a ficheros
11.Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
12.Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
13.Sistemas de autenticación de usuarios débiles, fuertes y biométricos
14.Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
15.Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

1.Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
2.Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
3.Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

UNIDAD DIDÁCTICA 8. ROBUSTECIMIENTO DE SISTEMAS

1.Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
2.Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
3.Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
4.Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
5.Actualización de parches de seguridad de los sistemas informáticos
6.Protección de los sistemas de información frente a código malicioso
7.Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
8.Monitorización de la seguridad y el uso adecuado de los sistemas de información

UNIDAD DIDÁCTICA 9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1.Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
2.Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
3.Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
4.Definición de reglas de corte en los cortafuegos
5.Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6.Establecimiento de la monitorización y pruebas del cortafuegos

+ Información Gratis