INESEM

BUSINESS SCHOOL

Curso de Gestión de la Seguridad Informática en la Empresa

+ Información Gratis

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

Curso de Gestión de la Seguridad Informática en la Empresa

duración total: 200 horas ***horas teleformación:*** 100 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Siendo los datos digitales cada vez más importantes en el mundo de las empresas, es de vital importancia prestar mucha atención a la seguridad informática. La información ha de ser protegida con fuertes medidas de seguridad para evitar que terceros accedan a información de carácter personal y confidencial sin autorización previa, es algo que se conoce como ciberseguridad

a quién va dirigido

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

objetivos

- Conocer las políticas de seguridad.
- Conocer defensas de seguridad tales como: postura de fallo seguro, punto de choque, postura de permiso establecido, etc...
- Conocer los ataques remotos y locales.
- Aprender a realizar labores de seguridad en las redes inalámbricas

para qué te prepara

El presente Curso de Gestión de a Seguridad Informática en la Empresa le proporcionará la formación necesaria para poder realizar tareas de seguridad informática dentro de la empresa y cómo gestionarla.

salidas laborales

Auditor Informático / Jefe de Seguridad Informática / Administrador de sistema

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

MARIA MORENO HIDALGO

Sello

Firma del alumno/a

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 'Gestión de la Seguridad Informática en la Empresa'

profesorado y servicio de tutorías

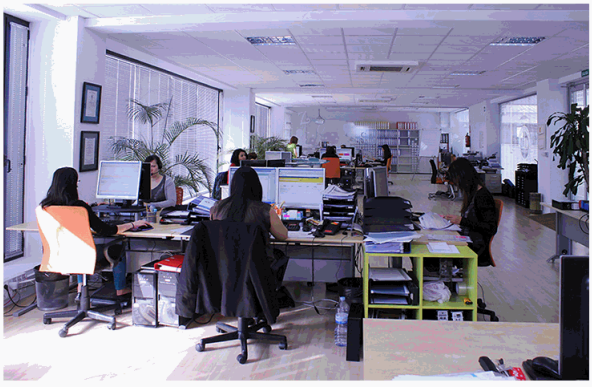
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado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

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA SEGURIDAD

1.Introducción a la seguridad de información.
2.Modelo de ciclo de vida de la seguridad de la información.
3.Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.
4.Políticas de seguridad.
5.Tácticas de ataque.
6.Concepto de hacking.
7.Árbol de ataque.
8.Lista de amenazas para la seguridad de la información.
9.Vulnerabilidades.
10.Vulnerabilidades en sistemas Windows.
11.Vulnerabilidades en aplicaciones multiplataforma.
12.Vulnerabilidades en sistemas Unix y Mac OS.
13.Buenas prácticas y salvaguardas para la seguridad de la red.
14.Recomendaciones para la seguridad de su red.

UNIDAD DIDÁCTICA 2. POLÍTICAS DE SEGURIDAD.

1.Introducción a las políticas de seguridad.
2.¿Por qué son importantes las políticas?
3.Qué debe de contener una política de seguridad.
4.Lo que no debe contener una política de seguridad.
5.Cómo conformar una política de seguridad informática.
6.Hacer que se cumplan las decisiones sobre estrategia y políticas.

UNIDAD DIDÁCTICA 3. AUDITORIA Y NORMATIVA DE SEGURIDAD.

1.Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
2.Ciclo del sistema de gestión de seguridad de la información.
3.Seguridad de la información.
4.Definiciones y clasificación de los activos.
5.Seguridad humana, seguridad física y del entorno.
6.Gestión de comunicaciones y operaciones.
7.Control de accesos.
8.Gestión de continuidad del negocio.
9.Conformidad y legalidad.

UNIDAD DIDÁCTICA 4. ESTRATEGIAS DE SEGURIDAD.

1.Menor privilegio.
2.Defensa en profundidad.
3.Punto de choque.
4.El eslabón más débil.
5.Postura de fallo seguro.
6.Postura de negación establecida: lo que no está prohibido.
7.Postura de permiso establecido: lo que no está permitido.
8.Participación universal.
9.Diversificación de la defensa.
10.Simplicidad.

UNIDAD DIDÁCTICA 5. EXPLORACIÓN DE LAS REDES.

1.Exploración de la red.
2.Inventario de una red. Herramientas del reconocimiento.
3.NMAP Y SCANLINE.
4.Reconocimiento. Limitar y explorar.

5.Reconocimiento. Exploración.
6.Reconocimiento. Enumerar.

UNIDAD DIDÁCTICA 6. ATAQUES REMOTOS Y LOCALES.

1.Clasificación de los ataques.
2.Ataques remotos en UNIX.
3.Ataques remotos sobre servicios inseguros en UNIX.
4.Ataques locales en UNIX.
5.¿Qué hacer si recibimos un ataque?

UNIDAD DIDÁCTICA 7. SEGURIDAD EN REDES ILANÁMBRICAS

1.Introducción.
2.Introducción al estándar inalámbrico 802.11 - WIFI
3.Topologías.
4.Seguridad en redes Wireless. Redes abiertas.
5.WEP.
6.WEP. Ataques.
7.Otros mecanismos de cifrado.

UNIDAD DIDÁCTICA 8. CRIPTOGRAFÍA Y CRIPTOANÁLISIS.

1.Criptografía y criptoanálisis: introducción y definición.
2.Cifrado y descifrado.
3.Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
4.Ejemplo de cifrado: criptografía moderna.
5.Comentarios sobre claves públicas y privadas: sesiones.

UNIDAD DIDÁCTICA 9. AUTENTICACIÓN.

1.Validación de identificación en redes.
2.Validación de identificación en redes: métodos de autenticación.
3.Validación de identificación basada en clave secreta compartida: protocolo.
4.Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.
5.Validación de identificación usando un centro de distribución de claves.
6.Protocolo de autenticación Kerberos.
7.Validación de identificación de clave pública.
8.Validación de identificación de clave pública: protocolo de interbloqueo.