



# INESEM

BUSINESS SCHOOL

## ***Curso en Gestión de la Seguridad en Redes de Área Local***

**+ Información Gratis**

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

# Curso en Gestión de la Seguridad en Redes de Área Local

**duración total:** 150 horas

**horas teleformación:** 75 horas

**precio:** 0 € \*

**modalidad:** Online

\* hasta 100 % bonificable para trabajadores.

## descripción

En la actualidad es un hecho los distintos ataques informáticos que se producen contra las empresas, por lo que la seguridad en sus redes de área local es algo fundamental, ya que el robo y pérdida de información es algo que una organización no se puede permitir.

Con esta acción formativa podrá desarrollarse como profesional de la seguridad capacitándose para actuar proactivamente ante los problemas de seguridad que pueden aparecer en una red de área local, planteando respuestas y anticipándose a las posibles amenazas de seguridad.

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*

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

## *objetivos*

Obtener una visión global de la gestión de la seguridad en redes de área local  
Asimilar los conocimientos y técnicas de criptografía  
Afianzar los conocimientos necesarios para conocer cómo aplicar un infraestructura de clave pública  
Conocer la arquitectura de las redes de área local y los tipos de incidentes que se presentan  
Aplicar control de accesos físicos y lógicos en la red local

## *para qué te prepara*

El Curso en Gestión de la Seguridad en Redes de Área Local te formará en las principales técnicas criptográficas y en el establecimiento de una correcta política de seguridad por niveles. Podrás llevar a cabo auditorías de seguridad informática sobre redes de área local, aplicando una infraestructura de clave pública e implantando servicios de seguridad. Obtendrás una visión global de la gestión de la seguridad y de las herramientas de notificación de alertas y alarmas en redes de área local.

## *salidas laborales*

Analista de seguridad informática  
Auditor de seguridad informática  
Gestor de seguridad  
Consultor de Ciberseguridad  
Técnico de seguridad  
Administrador de redes

## 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 'Herramientas y Técnicas de Ciberseguridad'
- Manual teórico 'Gestión de la Seguridad en la Red de Área local'



## 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 ineseem 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. HERRAMIENTAS Y TÉCNICAS DE CIBERSEGURIDAD**

### **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 componente 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

## **MÓDULO 2. GESTIÓN DE LA SEGURIDAD EN LA RED DE ÁREA LOCAL**

### **UNIDAD DIDÁCTICA 1.INTRODUCCIÓN A LAS REDES DE ÁREA LOCAL**

- 1.Arquitectura de redes de área local
- 2.Elementos de una red de área local
- 3.Instalación y configuración de los nodos de la red de área local
- 4.Tipos de incidencias en una red de área local

### **UNIDAD DIDÁCTICA 2. GESTIÓN DE LA SEGURIDAD**

- 1.Funciones de la gestión de la seguridad
- 2.Ciclo de seguridad

### **UNIDAD DIDÁCTICA 3. IMPLANTACIÓN DE SERVICIOS DE SEGURIDAD**

- 1.Control de acceso físico
- 2.Control de acceso lógico
- 3.Protección de la información en tránsito

### **UNIDAD DIDÁCTICA 4. GESTIÓN DE LA SEGURIDAD DE LA RED LOCAL**

- 1.Factores de seguridad en la red local
- 2.Procedimiento de seguridad en redes locales
- 3.Sondas de monitorización remota y detección de intrusos
- 4.Herramientas de notificación de alertas y alarmas en redes locales

**+ Información Gratis**