



**INESEM**  
Instituto Europeo de  
Estudios Empresariales

## ***Máster Executive en Seguridad en las Comunicaciones y la Información***

+ Información Gratis

Titulación Oficial avalada por la Administración Pública

# Máster Executive en Seguridad en las Comunicaciones y la Información

**Duración:** 600 horas

**Precio:** 0 € \*

**Modalidad:** Online

\* 100 % bonificable para trabajadores.

## Descripción

La necesidad de ambientes computacionales más seguros es cada vez más importante, y la única forma de alcanzar nuestro objetivo y afrontar el reto es poner en práctica tres aspectos claves: - Estableciendo medidas de seguridad adecuadas, que se anticipen a posibles fallas del sistema y de forma efectiva protejan los activos de la red. - Utilizar la tecnología apropiada y correctamente configurada para mantener un sistema de datos confiable. - Conocimiento de los tipos de ataques de los que podemos ser víctimas y de posibles modalidades de código malicioso que interviene en dichos ataques. Este curso brinda los conocimientos suficientes y necesarios para apoyar a los profesionales en la toma de decisiones para mejorar la seguridad en las empresas.



## *A quién va dirigido*

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

## *Objetivos*

- Conocer los requisitos de Seguridad en Sistemas de las TIC.
- Identificar las amenazas y vulnerabilidades que representan las nuevas tecnologías.
- Tomar decisiones sobre las medidas a implantar para la mejora de la seguridad en las empresas .

## *Para que te prepara*

Al terminar el curso el alumno tendrá amplios conocimientos de Seguridad en Sistemas de las TIC.

## *Salidas laborales*

Departamentos de informática de empresas de todos los sectores.

## 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/master, 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, Fundación Tripartita para la Formación en el Empleo y Fondo Social Europeo).



## Forma de subvención

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

## Metodología

Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios. También se adjunta en CDROM una guía de ayuda para utilizar el campus online.

La metodología a seguir es ir avanzando a lo largo del itinerario de aprendizaje online, que cuenta con una serie de temas y ejercicios. Para su evaluación, el alumno/a deberá completar todos los ejercicios propuestos en el curso. La titulación será remitida al alumno/a por correo una vez se haya comprobado que ha completado el itinerario de aprendizaje satisfactoriamente.

## Materiales didácticos

- CDROM 'Manual del Alumno de la Plataforma E-Learning. INESEM'



## Profesorado y servicio de tutorías

Nuestro centro tiene su sede en el "Centro de Empresas Granada", un moderno complejo empresarial situado en uno de los centros de negocios con mayor proyección de Andalucía Oriental. 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 con rapidez.

- **Por teléfono:** Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.



## ***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.

Si una vez cumplido el plazo no se han cumplido los objetivos mínimos exigidos (entrega de ejercicios y evaluaciones correspondientes), el alumno podrá solicitar una prórroga con causa justificada.

## ***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.

## ***Club de alumnos***

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.

## Programa formativo

### **MÓDULO 1. Descripción de los problemas de seguridad en las comunicaciones y en la información**

Preguntas que caracterizan el problema de la seguridad informática.

Distintas soluciones realistas y razonables, ¿cómo afrontar el problema?

### **MÓDULO 2. La seguridad de los elementos físicos de las redes**

Sistemas de cableado.

Sistemas inalámbricos.

Repetidores y conmutadores.

Seguridad en encaminadores.

Servidores y otros dispositivos.

### **MÓDULO 3. La seguridad de los elementos software**

Sistemas operativos de estaciones y servidores.

La "inseguridad" básica de la pila de protocolos TCP/IP.

Aplicaciones basadas en conexiones sobre TCP.

Aplicaciones basadas en conexiones sobre UDP.

Aplicaciones heterodoxas sobre IP.

Introducción a las mejoras de seguridad en redes IPv6.

### **MÓDULO 4. Métodos de ataque a equipos y redes**

Taxonomía de los tipos de ataques.

Ataques orientados a la obtención de información.

Ataques basados en la mala administración de sistemas y redes.

Ataques basados en vulnerabilidades del software.

Ataques de ingeniería social.

El spam y el phishing.

Ataques de tipo denegación de servicio, ataques DDOS y los botnets.

### **MÓDULO 5. La política de seguridad informática, la respuesta razonable**

Definición de política de seguridad informática.

Aspectos físicos de cualquier política de seguridad.

Aspectos lógicos de cualquier política de seguridad.

Aspectos humanos y organizativos de cualquier política de seguridad.

Creación de Sistemas de Gestión de Seguridad Informática siguiendo los estándares ISO/IEC 27001 y 27002.

### **MÓDULO 6. Ley orgánica de protección de datos personales y su reglamento**

Tipos de datos personales.

Obligaciones básicas a cumplir.

Derechos de los titulares de los datos.

Infracciones y sanciones, órganos de control.

Ejemplos de aplicación del reglamento de la LOPD en sistemas Microsoft.

### **MÓDULO 7. Herramientas técnicas para la implementación correcta de la política de seguridad.**

Distintas herramientas para las diferentes fases de la política de seguridad.

Herramientas para la implementación de la política de seguridad.

Herramientas para la monitorización de la política de seguridad.

Otros elementos típicos a tener en cuenta: disponibilidad física y fiabilidad de sistemas y dispositivos de comunicaciones.

## **MÓDULO 8. Cortafuegos, elementos básicos de la política de seguridad e redes**

Diferentes tecnologías de cortafuegos.

Los filtros de paquetes y sus características.

Los routers de Cisco, ejemplo de filtro de paquetes.

Los servidores proxy o gateways de aplicaciones.

Los cortafuegos stateful inspection

Ejemplos de tecnologías de última generación: PIX y ASA de Cisco Systems, Firewall-1 de Checkpoint.

Una nueva aproximación para "todo en uno": los appliances de seguridad.

## **MÓDULO 9. Análisis de vulnerabilidades de seguridad**

Análisis de sistemas y dispositivos de red.

Casos prácticos: Internet Security Systems.

Aplicaciones antivirus.

Aplicaciones antispymware.

## **MÓDULO 10. Sistemas de detección de intrusiones para monitorización c la política de seguridad**

Definición de un sis de detección/prevenición de intrusiones (IDS).

Sistemas IDS basados en red y basados en host.

Casos prácticos: Cisco Secure IDS.

Casos prácticos en código abierto: Snort.

Introducción a las honey pots.

## **MÓDULO 11. Introducción a la criptografía aplicada para la seguridad de información**

Introducción histórica de la criptografía.

Propiedades de seguridad alcanzables: confidencialidad, integridad y autenticación.

Elementos básicos de cualquier sis criptográfico.

Niveles de implementación de un sis criptográfico.

Ataques típicos a sistemas criptográficos.

Definición y ejemplos (RC4, DES, 3DES, AES) de algoritmos de criptografía simétrica o de clave secreta.

Definición y ejemplos (MD5, SHA) de funciones de una sola vía o hash.

Los crackers de contraseñas. Peligros reales y defensas básicas.

Definición y ejemplos (RSA, DSA, Diffie-Hellmann) de algoritmos de criptografía asimétrica o de clave pública.

El problema de seguridad de la distribución de claves.

## **MÓDULO 12. Certificación, autenticación, firma digital e infraestructuras de clave pública (PKI).**

Soluciones criptográficas a la distribución de claves.

Los sistemas de firma digital.

Los certificados digitales X.509 y las Autoridades de Certificación.

Las infraestructuras y estándares de clave pública de las PKI.

Problemas de seguridad de firmas digitales y PKI.

Ejemplos: el DNI digital.

## **MÓDULO 13. Protocolos criptográficos: SSL, PGP, IPSEC Y**

Comercio electrónico y sus protocolos: SSL y SET.

Funcionamiento del protocolo SSL.

Funcionamiento del protocolo SET.

Introducción al protocolo PGP (Pretty Good Privacy).

Los protocolos IPSec: AH (Authentication Header), ESP (Encapsulation Security Payload) y KMP (Key Management Protocol).

Introducción al uso de IPSec para redes privadas virtuales.

Los protocolos de correo electrónico seguro y sus problemas de implementación.

## **MÓDULO 14. Construcción, gestión y problemas de las redes privadas virtuales.**

Caracterización de las redes privadas virtuales.

Ventajas e inconvenientes de las redes privadas virtuales.

Arquitecturas de redes privadas virtuales.

Diseño y planificación de redes privadas virtuales.

Problemas de rendimiento, mantenimiento y seguridad.