# Seguridad de los sistemas informáticos y de comunicación

Modalidad: curso e-Learning Duración: 150 horas

Categorías: Ofimática, informática y comunicaciones

**OBJETIVOS**

Aplicar técnicas y protocolos de seguridad y realizar una hoja de ruta de la implantación del protocolo de seguridad en la organización

**CONTENIDOS**

**UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA SEGURIDAD.**
¿Qué es la seguridad Informática?.
Objetivos de la seguridad informática.
Amenazas.
Servicios de Seguridad.
Criptografía.
Seguridad física VS. Seguridad Lógica.
Clasificación de la Seguridad en función de las medidas oportunas.

**UNIDAD DIDÁCTICA 2. PRINCIPALES PROBLEMAS DE LA SEGURIDAD INFORMÁTICA.**
Configuraciones de redes.
Tipos de vulnerabilidades.

**UNIDAD DIDÁCTICA 3. GESTIÓN DE LA SEGURIDAD**
LOPD.
Series ISO/IEC 27000.

**UNIDAD DIDÁCTICA 4. SISTEMAS OPERATIVOS SEGUROS**
Windows XP.
Windows Vista.
Debian.

**UNIDAD DIDÁCTICA 5. MALWARE TOTAL.**
Malware infeccioso.
Malware oculto.
Malware para obtener beneficios.
Malware para robar información personal.
Ataques distribuidos.
Programas antimalware.
Métodos de protección.

**UNIDAD DIDÁCTICA 6. LA SEGURIDAD FÍSICA Y EL ENTORNO.**
La seguridad del edificio.
El entorno físico del hardware.



**UNIDAD DIDÁCTICA 7. SEGURIDAD DE LA INFORMÁTICA EN LA EMPRESA.**
¿Qué es OSSIM?.

Herramientas integradas en OSSIM.
Componentes de OSSIM.
Conceptos básicos.

**UNIDAD DIDÁCTICA 8. SEGURIDAD WEB.**

Tipos de ataques.
Wargames.
Hacking google.

**UNIDAD DIDÁCTICA 9. SEGURIDAD EN REDES INALÁMBRICAS.**

Riesgos de las redes inalámbricas.
Mecanismos de seguridad.
Guía básica de ataques wireless.
WiFi Segura.

**UNIDAD DIDÁCTICA 10. SEGURIDAD EN CONTINUA ACTUALIZACIÓN.**

Herramientas de seguridad.
La importancia de estar actualizado.