

# Seguridad en Equipos Informáticos

**PRESENCIAL****DURACIÓN:**  
90 h.**LUGAR:**  
Vila-real**ALUMNADO:**  
Desempleados

## SEGURIDAD EN EQUIPOS INFORMÁTICOS (MF0486)

El módulo formativo Seguridad en Equipos Informáticos (MF0486) te prepara para proteger sistemas y equipos informáticos frente a amenazas digitales, aprendiendo a aplicar medidas de seguridad, prevención y mantenimiento en entornos tecnológicos profesionales.

Durante la formación adquirirás conocimientos sobre protección de datos, control de accesos, copias de seguridad, detección de vulnerabilidades y prevención de malware, además de aprender buenas prácticas de ciberseguridad y mantenimiento seguro de equipos informáticos. También conocerás procedimientos para garantizar la integridad, disponibilidad y confidencialidad de la información en redes y sistemas.

Completarás el aprendizaje con contenidos orientados a la seguridad informática aplicada en empresas y entornos profesionales, ideal si buscas iniciarte en el sector tecnológico, mejorar tus competencias digitales o ampliar tu perfil profesional en soporte y administración de sistemas informáticos.

Si este curso no estuviera subvencionado te costaría: 720 €

**Categorías:** [Presencial](#)  
**Etiquetas:** [Internet](#)

### TEMARIO



1. Criterios de seguridad y gestión de riesgos
  - 1.1. Fundamentos y modelos de seguridad orientados a la gestión de riesgos
  - 1.2. Identificación de amenazas, vulnerabilidades y salvaguardas
  - 1.3. Seguridad en software, redes y accesos
  - 1.4. Criptografía y cifrado de datos
2. Análisis de impacto y planificación
  - 2.1. Análisis de impacto de negocio (BIA)
  - 2.2. Evaluación de procesos críticos y recuperación ante desastres
  - 2.3. Políticas y auditorías de seguridad corporativa
  - 2.4. Desarrollo e implementación del plan de seguridad
3. Seguridad física y de sistemas
  - 3.1. Protección de datos de carácter personal
  - 3.2. Cumplimiento normativo y legal
  - 3.3. Seguridad física e industrial
  - 3.4. Protección ambiental de centros de procesamiento de datos
4. Robustecimiento y control de accesos
  - 4.1. Autenticación y control de accesos físicos y lógicos
  - 4.2. Identificación de servicios
  - 4.3. Hardening o robustecimiento de sistemas operativos y servidores
  - 4.4. Instalación y configuración de cortafuegos
  - 4.5. Administración y monitorización de firewalls

### METODOLOGÍA



Las sesiones formativas se imparten de forma presencial en nuestras aulas, guiadas por un/a docente especialista que combina explicación

teórica, ejercicios prácticos y actividades colaborativas en el aula. Todos los docentes disponen de gran experiencia en el sector.

**Sesiones de tutoría**

El alumnado puede plantear dudas y recibir orientación personalizada durante las clases y, en su caso, tutorías personalizadas con el/la docente.

**Sistema de evaluación**

La evaluación es continua. El alumno realizará actividades y/o pruebas al finalizar los temas o unidades, y, cuando proceda, una prueba final para comprobar la adquisición de los contenidos.

**Requisitos técnicos**

El centro proporciona el equipamiento necesario (ordenadores, software y conexión a internet) en el aula. El alumnado no necesita aportar equipo propio, salvo que lo desee de forma voluntaria.

**Material didáctico y recursos**

El material didáctico se entregará en formato libro, manual impreso y/o documentación digital, según las características del curso.

**Kit corporativo**

En los cursos presenciales se entrega un kit corporativo del centro, cuyo contenido puede variar en función de la duración de la acción formativa y puede incluir: mochila, pendrive, libreta y bolígrafo.

**SALIDAS PROFESIONALES**

Departamentos de soporte informático.

Empresas de mantenimiento informático.

Servicios de asistencia técnica.

Áreas de sistemas y redes.

Empresas de tecnología y telecomunicaciones.

Oficinas y empresas que gestionen equipos informáticos.

Puestos de apoyo en ciberseguridad y protección de datos