



**Denominación:** SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIÓN.

**Código:** IFCT100PO

**Familia Profesional:** INFORMÁTICA Y COMUNICACIONES

**Área profesional:** SISTEMAS Y TELEMÁTICA

**Duración:** 150 horas

## OBJETIVOS DE LA ACCIÓN FORMATIVA

Gestionar la seguridad de las redes de comunicación.

## CONTENIDOS DE LA ACCIÓN FORMATIVA

### 1. INTRODUCCIÓN A LA SEGURIDAD.

- 1.1. ¿Qué es la seguridad Informática?.
- 1.2. Objetivos de la seguridad informática.
- 1.3. Amenazas.
- 1.4. Servicios de Seguridad.
- 1.5. Criptografía.
- 1.6. Seguridad física VS. Seguridad Lógica.
- 1.7. Clasificación de la Seguridad en función de las medidas oportunas.

### 2. PRINCIPALES PROBLEMAS DE LA SEGURIDAD INFORMÁTICA.

- 2.1. Configuraciones de redes.
- 2.2. Tipos de vulnerabilidades.

### 3. GESTIÓN DE LA SEGURIDAD

- 3.1. LOPD.
- 3.2. Series ISO/IEC 27000.

### 4. SISTEMAS OPERATIVOS SEGUROS 4.1. Windows XP.

- 4.2. Windows Vista.
- 4.3. Debian.

### 5. MALWARE TOTAL.

- 5.1. Malware infeccioso.
- 5.2. Malware oculto.
- 5.3. Malware para obtener beneficios.
- 5.4. Malware para robar información personal.
- 5.5. Ataques distribuidos.
- 5.6. Programas antimalware.
- 5.7. Métodos de protección.

### 6. LA SEGURIDAD FÍSICA Y EL ENTORNO.

- 6.1. La seguridad del edificio.
- 6.2. El entorno físico del hardware.

## 7. SEGURIDAD DE LA INFORMÁTICA EN LA EMPRESA.

7.1. ¿Qué es OSSIM?.

7.2. Herramientas integradas en OSSIM.

7.3. Componentes de OSSIM.

7.4. Conceptos básicos.

## 8. SEGURIDAD WEB.

8.1. Tipos de ataques.

8.2. Wargames.

8.3. Hacking google.

## 9. SEGURIDAD EN REDES INALÁMBRICAS.

9.1. Riesgos de las redes inalámbricas.

9.2. Mecanismos de seguridad.

9.3. Guía básica de ataques wireless.

9.4. WiFi Segura.

## 10. SEGURIDAD EN CONTINUA ACTUALIZACIÓN.

10.1. Herramientas de seguridad.

10.2. La importancia de estar actualizado.