

## CIBERSEGURIDAD PARA USUARIOS

Código IFCT135PO

- 10 horas.

### OBJETIVOS

- Valorar la necesidad de la gestión de la seguridad en las organizaciones. Conocer las principales amenazas a los sistemas de información e identificar las principales herramientas de seguridad y su aplicación en cada caso.

### CONTENIDOS

#### 1. INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN.

- 1.1. Conceptos de seguridad en los sistemas.
- 1.2. Clasificación de las medidas de seguridad.
- 1.3. Requerimientos de seguridad en los sistemas de información.
  - 1.3.1. Principales características.
  - 1.3.2. Confidencialidad.
  - 1.3.3. Integridad.
  - 1.3.4. Disponibilidad.
  - 1.3.5. Otras características.
  - 1.3.6. Tipos de ataques.

#### 2. CIBERSEGURIDAD.

- 2.1. Concepto de ciberseguridad.
- 2.2. Amenazas más frecuentes a los sistemas de información.
- 2.3. Tecnologías de seguridad más habituales.
- 2.4. Gestión de la seguridad informática.

#### 3. SOFTWARE DAÑINO.

- 3.1. Conceptos sobre software dañino.
- 3.2. Clasificación del software dañino.
- 3.3. Amenazas persistentes y avanzadas.
- 3.4. Ingeniería social y redes sociales.

#### 4. SEGURIDAD EN REDES INALÁMBRICAS.

#### 5. HERRAMIENTAS DE SEGURIDAD.

- 5.1. Medidas de protección.
- 5.2. Control de acceso de los usuarios al sistema operativo.
  - 5.2.1. Permisos de los usuarios.
  - 5.2.2. Registro de usuarios.
  - 5.2.3. Autenticación de usuarios.
- 5.3. Gestión segura de comunicaciones, carpetas y otros recursos compartidos.
  - 5.3.1. Gestión de carpetas compartidas en la red.
  - 5.3.2. Tipos de accesos a carpetas compartidas.
  - 5.3.3. Compartir impresoras.

# PROGRAMA FORMATIVO

---

5.4. Protección frente a código malicioso.

5.4.1. Antivirus.

5.4.2. Cortafuegos (firewall).

5.4.3. Antimalware.