

IFCT106PO. Protección de equipos en la red.



Sku: PA_IFCT106PO

Horas: 10

Formato: HTML

OBJETIVOS

- Describir los objetivos de la seguridad física y de la lógica.
- Analizar la importancia de la seguridad en el puesto del usuario.
- Describir las características de virus informáticos y definir sus métodos de propagación.
- Identificar los sistemas que ayudan a luchar contra los ataques de código malicioso.
- Listar un conjunto de buenas prácticas que nos permitirán estar más seguros.
- Identificar las distintas arquitecturas de los sistemas cortafuegos.
- Describir las técnicas de ingeniería social que utilizan las técnicas de suplantación.
- Clasificar los tipos de actualizaciones que publican los fabricantes.
- Distinguir las técnicas de actualización más habituales.

CONTENIDOS

- **Unidad 1. La necesidad de protegerse en la red**
 - ¿Por qué hay que protegerse?
 - Objetivos de la seguridad informática
 - La seguridad
 - Seguridad en el puesto de usuario
- **Unidad 2. Los peligros posibles: los virus informáticos**
 - Características de los virus informáticos
 - Métodos de propagación
 - Tipos de virus
 - Tendencias
- **Unidad 3. Las soluciones: el antivirus**
 - Tipos de medidas
 - Sistemas de detección y contención de código malicioso
 - Buenas prácticas para protegernos de los virus y del resto de código malicioso

- **Unidad 4. Otros conceptos sobre seguridad informática**
 - Firewall
 - Spam
 - Phising
 - Copias de seguridad
 - Respuesta a incidentes de seguridad
 - Tendencias

- **Unidad 5. Actualizaciones del software**
 - Tipos de actualizaciones
 - Determinación de los requerimientos y técnicas de actualización