IFCT106PO. Protección de equipos en la red

Objetivos

Objetivo General

- Prevenir los ataques de la red en equipos.

Objetivos Específicos

- Conocer la importancia de la protección.
- Identificar los tipos de ataques en el proceso de transmisión de datos.
- Analizar la vulnerabilidad y las amenazas que representan un riesgo.
- Tener conocimiento de las políticas de seguridad que se deben implementar para minimizar los riesgos.
- Conocer el funcionamiento básico de los virus informáticos.
- Diferenciar virus, gusanos y troyanos.
- Analizar diferentes formas de infección y qué precauciones hay que tomar.
- Conocer qué es un software antivirus.
- Diferenciar entre vacunas, detectores y eliminadores.
- Técnicas de detección de virus.
- Cómo elegir un antivirus.
- Conocer los distintos tipos de firewall o cortafuegos.
- Analizar los distintos tipos de spam.
- Conocer qué es el phishing.
- Conocer las vulnerabilidades en las aplicaciones.
- Analizar los errores más frecuentes de los programas.
- Analizar la seguridad de los navegadores más utilizados.
- Conocer la importancia de las actualizaciones.

Contenidos

IFCT106PO. Protección de equipos en la red	Tiempo estimado

Unidad 1: La necesidad de protegerse en la red.
• Necesidad de protección.
• Ataques a la seguridad de la red.
  ○ Ataques pasivos
  ○ Ataques activos
• Vulnerabilidades y amenazas.
• Riesgos y medidas de seguridad.
• Políticas de seguridad.
	1.5 horas

Examen UA 01	**0.5 hora**
Tiempo total de la unidad	**2 horas**
Unidad 2: Los peligros posibles: los virus informáticos. • Funcionamiento básico de los virus informáticos. • Virus, gusanos, troyanos y otros programas dañinos. • Precauciones para evitar una infección.	**1.5 horas**
Examen UA 02	**0.5 hora**
Tiempo total de la unidad	**2 horas**
Unidad 3: Las soluciones: el antivirus. • Programas o software antivirus. • Técnicas de detección de virus. • Consideraciones para elegir un antivirus.	**1.5 horas**
Examen UA 03	**0.5 hora**
Tiempo total de la unidad	**2 horas**
Unidad 4: Otros conceptos sobre seguridad informática. • Firewall o cortafuegos. • Spam. • Phishing.	**1.5 horas**
Examen UA 04	**0.5 hora**

Tiempo total de la unidad	**2 horas**
Unidad 5: Actualizaciones del software. • Vulnerabilidad del software. • Tipos de errores frecuentes en el software. • Importancia de las actualizaciones del software.	**1.5 horas**
Examen UA 05	**0.5 hora**
Tiempo total de la unidad	**2 horas**
5 unidades	**10 horas**

Tiempo del curso

El curso precisa un tiempo de estudio de 5.5 horas, englobando el tiempo dedicado a la lectura de las pantallas entre otros conceptos.

Por otro lado, contamos con un tiempo de realización de 4.5 horas, el cual implica la realización de actividades de aprendizaje que forman parte de este curso.

Por tanto, para la realización de esta acción formativa se requiere de 10 horas de formación.