(IFCT106PO) Protección de equipos en la red

Sku: PIT095

Horas: 10

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

Unidad 1: La necesidad de protegerse en la red. • Necesidad de protección. • Ataques a la seguridad de la red. o Ataques pasivos o Ataques activos • Vulnerabilidades y amenazas. • Riesgos y medidas de seguridad. • Políticas de seguridad. **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. Unidad 3: Las soluciones: el antivirus. • Programas o software antivirus. • Técnicas de detección de virus. • Consideraciones para elegir un antivirus. **Unidad 4: Otros conceptos sobre seguridad informática.** • Firewall o cortafuegos. • Spam. • Phishing. **Unidad 5: Actualizaciones del software.** • Vulnerabilidad del software. • Tipos de errores frecuentes en el software. • Importancia de las actualizaciones del software.