INTERNET SEGURO

30 HORAS
AF: 36269

Obtener una visión general sobre la seguridad informática y dotar de conocimientos al alumnado para que puedan identificar los problemas de seguridad informática que se produzcan en entorno de red con acceso a Internet, y hacer frente a ellos. Además se verán los siguientes puntos:
Utilización de cortafuegos o firewall.
Conocimiento sobre modelos de prevención de intrusiones y diseño de redes privadas.
Tipos de ataques y navegación segura.

UNIDAD 1. CORTAFUEGOS O FIREWALL
1 DEFINICION CORTA FUEGOS
1.1 ¿PARA QUE SIRVE UN FIREWALL?
1.2 ¿COMO FUNCIONA UN FIREWALL?
1.3 DEIFINICION DE PUERTO
2 TIPOS DE FIREWALL
3 FIREWALLS MAS POPULARES
4 LIMITACIONES DE UN FIREWALL
5 EL FIREWALL DE WINDOWS
6 ARQUITECTURA DE CORTAFUEGOS
7 ¿QUE SIGNIFICA LOS ICONOS DE SEGURIDAD?

UNIDAD 2. LA RED
Introducción
1. Qué es la RED
2. Funcionamiento y tipos de redes
3. Seguridad de red
4. Modelos de prevención de intrusiones o IPS
4.1. Clasificación de los IPS
4.2. Funcionamiento
5. Diseño de redes privadas virtuales o VPN
5.1. Recomendaciones de seguridad
6. Red social y sus vulnerabilidades

UNIDAD 3.NAVEGAR SEGURO
1. NAVEGAR DE FORMA SEGURA
2. CERTIFICADOS SEGURIDAD
2.1. ¿QUE ES UN CERTIFICADO DE SEGURIDAD SSL ?
2.2. ¿COMO FUNCIONA UN CERTIFICADO SSL?
2.3. TIPOS DE CERTIFICADOS DE SEGURIDAD
2.4. DIFERENCIAS ENTRE HTTP Y HTTPS
3. ¿COMO SABER SI UNA PAGINA ES SEGURA?
4. ATAQUE DE NEGACION DE SERVICIO DDoS
4.1. ¿QUE ES UN ATAQUE DE DDOS?
4.2. ¿COMO FUNCIONA UN ATAQUE DDoS?
4.3. TIPOS DE ATAQUES DDoS
4.4. ¿COMO PROTEGERTE DE UN ATAQUE DDoS?