

# INTERNET SEGURO

AF: 26202

HORAS: 60

## OBJETIVOS

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: Conocimiento sobre virus y actuación ante ellos. Utilización de cortafuegos o firewall. Conocimiento sobre modelos de prevención de intrusiones y diseño de redes privadas. Tipos de ataques y navegación segura. Correo seguro y recomendaciones de seguridad.

## CONTENIDOS

UNIDAD 1. LA SEGURIDAD 1.1 ¿A QUÉ NOS REFERIMOS CON SEGURIDAD? 1.2 ANTIVIRUS. Definición y clasificación de virus 1.2.1 Definición y clasificación de virus 1.2.2 ¿Cómo evitar los virus? 1.3 PASOS PREVIOS A LA INSTALACION DE ALGUN PROGRAMA 1.3.1 COMO DESCARGAR UN PROGRAMA 1.3.2 COMO INSTALAR O DESINSTALAR UN PROGRAMA 1.4 LIMPIADORES DE VIRUS 1.5 COMO ELIMINAR UN VIRUS INFORMATICO 1.6 TIPOS DE SEGURIDAD INFORMATICA 1.7 LA IMPORTANCIA DE LA DE SEGURIDAD INFORMATICA DENTRO DE UNA EMPRESA 1.8 FASES DE LA CIBERSEGURIDAD UNIDAD 2. ANTIVIRUS 2.1 CONFIGURACION ANTIVIRUS 2.1.1 WINDOWS DEFENDER 2.1.2 AVAST 2.2 TECNICAS DE DETECCION DE VIRUS 2.3 ACTUALIZAR UN ANTIVIRUS 2.4 TROYANOS 2.4.1 ¿QUE ES UN TROYANO? 2.4.2 ¿COMO PROTEGERSE DE UN TROYANO? 2.4.3 TIPOS DE TROYANOS 2.5 TECNICO EN SOPORTE INFORMATICO 2.5.1 ¿QUIEN ES EL TECNICO EN SOPORTE INFORMATICO? 2.5.2 ¿CUALES SON LAS FUNCIONES DE UN TECNICO EN SOPORTE INFORMATICO? 2.5.3 ¿QUE VENTAJAS TIENE EL SERVICIO TECNICO INFORMATICO PARA LAS EMPRESAS? 2.6 VIRUS SASSER 2.6.1 ¿QUE ES EL VIRUS SASSER? 2.6.2 COMO ELIMINAR EL VIRUS UNIDAD 3. CORTAFUEGOS O FIREWALL 3.1 DEFINICION CORTA FUEGOS 3.1.1 ¿PARA QUE SIRVE UN FIREWALL? 3.1.2 ¿COMO FUNCIONA UN FIREWALL? 3.1.3 DEFINICION DE PUERTO 3.2 TIPOS DE FIREWALL 3.3 FIREWALLS MAS POPULARES 3.4 LIMITACIONES DE UN FIREWALL 3.5 EL FIREWALL DE WINDOWS 3.6 ARQUITECTURA DE CORTAFUEGOS 3.7 ¿QUE SIGNIFICA LOS ICONOS DE SEGURIDAD? UNIDAD 4. LA RED Introducción 4.1. Qué es la RED 4.2. Funcionamiento y tipos de redes 4.3. Seguridad de red 4.4. Modelos de prevención de intrusiones o IPS 4.4.1. Clasificación de los IPS 4.4.2. Funcionamiento 4.5. Diseño de redes privadas virtuales o VPN 4.5.1. Recomendaciones de seguridad 4.6. Red social y sus vulnerabilidades UNIDAD 5. NAVEGAR SEGURO 5.1 NAVEGAR DE FORMA SEGURA 5.2 CERTIFICADOS SEGURIDAD 5.2.1 ¿QUE ES UN CERTIFICADO DE SEGURIDAD SSL? 5.2.2 ¿COMO FUNCIONA UN CERTIFICADO SSL? 5.2.3 TIPOS DE CERTIFICADOS DE SEGURIDAD 5.2.4 DIFERENCIAS ENTRE HTTP Y HTTPS 5.3 ¿COMO SABER SI UNA PAGINA ES SEGURA? 5.4 ATAQUE DE NEGACION DE SERVICIO DDoS 5.4.1 ¿QUE ES UN ATAQUE DE DDoS? 5.4.2 ¿COMO FUNCIONA UN ATAQUE DDoS? 5.4.3 TIPOS DE ATAQUES DDoS 5.4.4 ¿COMO PROTEGERSE DE UN ATAQUE DDoS? UNIDAD 6. CORREO SEGURO 6.1 CORREO SEGURO 6.2 ¿COMO CONSEGUIR UN CORREO MAS SEGURO? 6.3 ¿QUE ES UN CORREO ENcriptado? 6.4 ¿COMO ENcriptar un correo? 6.5 HUSHMAIL