

IFCT57PO. Internet seguro

Código del curso: 17940IN

Horas: 50

Descripción del curso:

Acerca de este curso

Cod: 17940IN

Unidad 1. Introducción y antivirus

Introducción a la seguridad
Antivirus. Definición de virus. Tipos de virus
Antes de instalar ningún programa
Antivirus. Descarga e instalación
Otros programas recomendados
Herramientas de desinfección gratuitas
Técnico. Ejemplo de infección por virus.
Tengo un mensaje de error, ¿y ahora?
Anexo. Referencias. Monográficos

Unidad 2. Antivirus. Configuración, utilización

Test de conocimientos previos
Antivirus. Configuración
Antivirus. Utilización
Antivirus. Actualización
Troyanos
Pantalla típica de un troyano cuando estamos a punto de infectarnos
Esquema de seguridad
Técnico. Detalles del virus Sasser
Anexo. Referencias

Unidad 3. Cortafuegos

Test de conocimientos previos
Cortafuegos. Definición

Tipos de cortafuegos
Concepto de puerto
Cortafuegos de Windows 10
Limitaciones de los cortafuegos
Descarga e instalación. ZoneAlarm
Configuración y utilización
Actualización
Consola del sistema
Otros programas recomendados
Direcciones de comprobación en línea
Esquema de seguridad
Novedad. USB Firewall
Técnico. Cómo funciona un IDS (sistema de detección de intrusos)
Inalámbricas
Anexo. Referencias

Unidad 4. Antiespías

Test de conocimientos previos
Definición de módulo espía
Tipos de espías
Cookies

Spybot

Malwarebyte

SpywareBlaster
Descarga e instalación
Técnico. Evidence Eliminator amenaza para que lo compres
Anexo. Referencias
Glosario

Unidad 5. Antiespías. Configuración, utilización

Conocimientos previos
Configuración y actualización
Utilización
Otros programas recomendados
Direcciones de comprobación en línea

Cómo eliminar los programas espía de un sistema: pasos
Esquema de seguridad
Kaspersky admite que están saturados de peligros en la red
“Apple está 10 años por detrás de Microsoft en materia de seguridad informática”
Anexo. Referencias

Unidad 6. Actualización del sistema operativo

Conocimientos previos
Windows Update
Configuraciones de Windows Update
Módulos espía en Windows 10
Complementos de Microsoft Edge
Navegadores alternativos
Anexo. Referencias

Unidad 7. Navegador seguro. Certificados

Conocimientos previos
Navegador seguro
Certificados
Anexo. Tarjetas criptográficas y token USB
Técnico. ¿Qué es un ataque de denegación de servicio (DoS)?
Anexo. Referencias
Anexo. DNI electrónico (eDNI)

Unidad 8. Correo seguro

Conocimientos previos
Correo seguro
Correo anónimo
Técnico. Correo anónimo
Hushmail
Esquema de seguridad
Anexo. Referencias

Unidad 9. Seguridad en las redes P2P

Conocimientos previos
Seguridad en las redes P2P
PeerGuardian
Seguridad al contactar con el proveedor de internet
Checkdialer
Esquema de seguridad
Técnico. Usuarios P2P prefieren anonimato a velocidad
España se posiciona como uno de los países del mundo con más fraudes en internet
Esquema de funcionamiento de una red
Anexo. Referencias

Unidad 10. Comprobar seguridad

Conocimientos previos
Microsoft Baseline Security Analyzer
Comprobaciones online de seguridad y antivirus
Técnico. Comprobar seguridad de un sistema Windows 10
Anexo. Instalación Panda Cloud Cleaner
Referencias

Unidad 11. Varios

Conocimientos previos
Copias de seguridad
Contraseñas
Control remoto
Mensajería electrónica
Privacidad y anonimato
Boletines electrónicos
Listas de seguridad
Compras a través de internet
Banca electrónica.
Enlaces y noticias sobre seguridad informática
Anexo. Navegador Firefox
Agenda de control
Técnico. PandaLabs descubre un nuevo troyano Briz que permite el control remoto del ordenador y

realizar estafas online
Técnico. Seguridad en Linux
Seguridad inalámbrica (wifi)
Referencias
Glosario de palabras en inglés

¿Qué aprenderás?

Manejar servicios y programas para trabajar de forma segura en la red.
Obtener una visión general de qué es la seguridad en el ámbito de la informática y saber por qué es necesario el uso de antivirus.
Saber configurar, utilizar y actualizar correctamente un antivirus y profundizar en el conocimiento sobre los virus troyanos.
Saber la definición de cortafuegos, cómo configurarlos y utilizarlos, y sus limitaciones.
Conocer el concepto de puerto y para qué sirve la consola del sistema.
Conocer el significado del término espía informático, cuáles son sus tipos, cuáles son sus formas de atacar y cómo protegerse frente a ellos.
Mantener el equipo libre de programas espía mediante el uso de diversas herramientas antiespía.
Saber actuar cuando un equipo ya ha sido infectado.
Mantener actualizado Windows 10 en todo momento.
Conocer las distintas funciones que ofrece Microsoft Edge y los navegadores alternativos más recomendados.
Conocer la seguridad que ofrecen los navegadores web.
Distinguir los tipos de certificado digital.
Enviar y recibir correos electrónicos de forma segura a través de la red.
Identificar entornos seguros e inseguros para el envío de correos electrónicos.
Conocer qué es una red P2P, cuáles son sus posibles brechas de seguridad, cómo suplirlas y su clasificación.
Introducir un nuevo tipo de ataque relacionado con los accesos a nuestro equipo mediante redes P2P.
Ampliar el catálogo de herramientas disponibles para mantener la seguridad de un equipo.
Destacar la importancia de mantener el sistema actualizado.
Complementar los conocimientos adquiridos con conceptos adicionales importantes que ayudarán a resolver de forma exitosa situaciones de seguridad adversas.