IFCT057PO. Internet Seguro

Horas	50

Acerca de este curso

Cod: 17940IN

1. INTRODUCCIÓN Y ANTIVIRUS
1.1. Introducción a la seguridad.
1.2. Introducción a la seguridad.
1.3. Antivirus. Definición de virus. Tipos de virus.
1.4. Previo a instalar ningún programa.
1.5. Antivirus. Descarga e instalación.
1.6. Otros programas recomendados.
1.7. Herramientas de desinfección gratuitas.
1.8. Técnico. Ejemplo de infección por virus.
1.9. Anexo.
1.10. Referencias.
1.11. Tengo un mensaje de error ¿y ahora?
1.12. Monográficos.

2. ANTIVIRUS. CONFIGURACIÓN, UTILIZACIÓN
2.1. Test de conocimientos previos.
2.2. Antivirus. Configuración.
2.3. Antivirus. Utilización.
2.4. Antivirus. Actualización.
2.5. Troyanos.
2.6. Pantalla típica de un troyano cuando estamos a punto de infectarnos.
2.7. Esquema de seguridad.
2.8. Técnico. Detalles del virus Sasser.
2.9. Anexo.
2.10. Referencias.

3. CORTAFUEGOS
3.1. Test de conocimientos previos.
3.2. Cortafuegos. Definición.
3.3. Tipos de cortafuegos.
3.4. Concepto de puerto.
3.5. Tipos de cortafuegos.
3.6. Cortafuegos de Windows XP.
3.7. Cortafuegos de Windows 7.

3.8. Cortafuegos de Windows 8.
3.9. Limitaciones de los cortafuegos.
3.10. Descarga e instalación. Zonealarm.
3.11. Configuración.
3.12. Utilización.
3.13. Actualización.
3.14. Consola del sistema.
3.15. Otros programas recomendados.
3.16. Direcciones de comprobación en línea.
3.17. Esquema de seguridad.
3.18. Novedad. USB Firewall.
3.19. Técnico. Cómo funciona un IDS (sistema de detección de intrusos) Inalámbricas.
3.20. Anexo.
3.21. Referencias.

4. ANTIESPÍAS
4.1. Test de conocimientos previos.
4.2. Definición de módulo espía.
4.3. Tipos de espías.
4.4. Cookies.
4.5. SpyBot.
4.6. Malwarebytes.
4.7. Spywareblaster.
4.8. Descarga e instalación.
4.9. Técnico. Evidence Eliminator, amenaza para que lo compres.
4.10. Anexo.
4.11. Referencias.
4.12. Glosario.

5. ANTIESPÍAS. CONFIGURACIÓN, UTILIZACIÓN
5.1. Test de conocimientos previos.
5.2. Configuración.
5.3. Utilización.
5.4. Actualización.
5.5. Otros programas recomendados.
5.6. Direcciones de comprobación en línea.
5.7. Cómo eliminar los programas espía de un sistema (Pasos).
5.8. Esquema de seguridad.
5.9. Kaspersky admite que están saturados de peligros en la red.
5.10. “Apple está 10 años detrás de Microsoft en materia de seguridad informática”.
5.11. Anexo.
5.12. Referencias.

6. ACTUALIZACIÓN DEL SISTEMA OPERATIVO
6.1. Test de conocimientos previos.
6.2. WindowsUpdate.
6.3. Configuraciones de Windows Update.

6.4. Módulos espía en Windows XP.
6.5. SafeXP.
6.6. Objetos (o complementos) del Internet Explorer.
6.7. Navegadores alternativos.
6.8. Anexo.
6.9. Referencias.

7. NAVEGADOR SEGURO. CERTIFICADOS
7.1. Test de conocimientos previos.
7.2. Navegador seguro.
7.3. Certificados.
7.4. Anexo. Tarjetas criptográficas y Token USB.
7.5. Técnico. ¿Qué es un ataque de denegación de servicio (Ddos)?
7.6. Anexo.
7.7. Referencias.
7.8. Anexo. DNI electrónico (eDNI).

8. CORREO SEGURO
8.1. Test de conocimientos previos.
8.2. Correo seguro.
8.3. Correo anónimo.
8.4. Técnico. Correo anónimo.
8.5. Hushmail.
8.6. Esquema de seguridad.
8.7. Anexo.
8.8. Referencias.

9. SEGURIDAD EN LAS REDES P2P
9.1. Test de conocimientos previos.
9.2. Seguridad en las redes P2P.
9.3. Peerguardian.
9.4. Seguridad al contactar con el Proveedor de Internet.
9.5. Checkdialer.
9.6. Esquema de seguridad.
9.7. Técnico. Usuarios P2P prefieren anonimato a velocidad.
9.8. España se posiciona como uno de los países del mundo con más fraudes en Internet.
9.9. Esquema de funcionamiento de una red.
9.10. Anexo.
9.11. Referencias.

10. COMPROBAR SEGURIDAD
10.1. Test de conocimientos previos.
10.2. Microsoft Baseline Security Analyzer.
10.3. Comprobaciones on-line de seguridad y antivirus.
10.4. Técnico. Comprobar seguridad de un sistema Windows XP.
10.5. Anexo.
10.6. Referencias.

11. VARIOS
11.1. Test de conocimientos previos.
11.2. Copias de seguridad.
11.3. Contraseñas.
11.4. Control remoto.
11.5. Mensajería electrónica.
11.6. Privacidad y anonimato.
11.7. Boletines electrónicos.
11.8. Listas de seguridad.
11.9. Compras a través de Internet.
11.10. Banca electrónica.
11.11. Enlaces y noticias sobre seguridad informática.
11.12. Anexo. Navegador Firefox.
11.13. Agenda de control.
11.14. Técnico. PandaLabs descubre un nuevo troyano Briz que permite el control remoto del ordenador y realizar estafas online.
11.15. Técnico. Seguridad en Linux.
11.16. Seguridad inalámbrica (Wifi).
11.17. Referencias.
11.18. 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.