IFCT057PO - INTERNET SEGURO

DURACIÓN:

50 horas

MODALIDAD:

Presencial

OBJETIVO:

Manejar servicios y programas para trabajar de forma segura en la red.

Aprender las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los archivos de los equipos informáticos ya que se vincula directamente con competencias y conocimientos vinculados a entornos de ciberseguridad.

Adquirir los conocimientos y competencias clave para diseñar y aplicar de forma autónoma medidas y controles de seguridad relacionadas con Internet en el ámbito de la educación, mejorando la empleabilidad de los participantes y facilitando su incorporación y desarrollo en equipos profesionales dentro de esta área.

Asimilar los conceptos base sobre gestión de la seguridad tecnológica en Internet, tanto en equipos independientes como en el entorno del sistema de información de la organización.

Conocer cómo aplicar de forma práctica medidas de seguridad en equipos informáticos.

PARTICIPANTES:

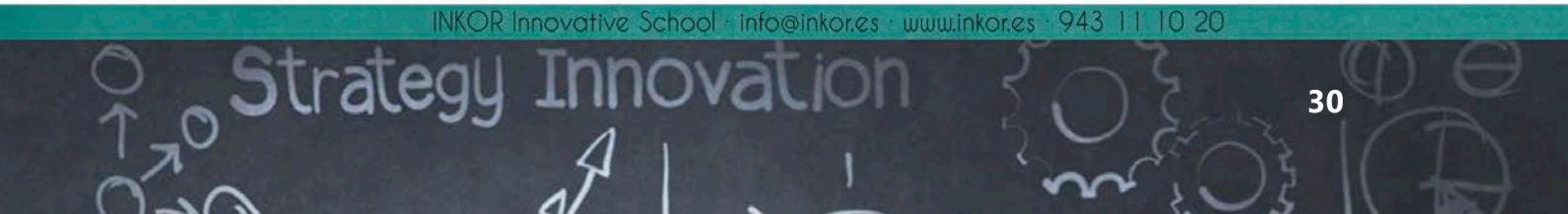
Prioritariamente PERSONAS OCUPADAS.
Personas trabajadoras DESEMPLEADAS inscritas en los servicios públicos de empleo.(*)
(*) Consultar programa de becas y ayudas.

REQUISITOS DE ACCESO:

Si bien no se requieren conocimientos o titulación específica para el acceso al curso, dado los contenidos a tratar, es deseable que el alumno disponga de algunos conocimientos de base relacionados con el manejo en sistemas microinformáticos y navegación en Internet.

CONTENIDOS:

1. INTRODUCCIÓN Y ANTIVIRUS
2. ANTIVIRUS. CONFIGURACIÓN, UTILIZACIÓN
3. CORTAFUEGOS
4. ANTIESPÍAS
5. ANTIESPÍAS. CONFIGURACIÓN, UTILIZACIÓN
6. ACTUALIZACIÓN DEL SISTEMA OPERATIVO
7. NAVEGADOR SEGURO.
8. CORREO SEGURO
9. SEGURIDAD EN LAS REDES P2P
10. COMPROBAR SEGURIDAD
11. VARIOS
12. GESTIÓN DE LA CIBERSEGURIDAD.



CONTENIDOS AMPLIADOS:

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.

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.
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
11.16. Seguridad inalámbrica (Wifi).

12. GESTIÓN DE LA CIBERSEGURIDAD.
12.1. Conceptos generales sobre ciberseguridad de los sistemas de información.
12.2. Análisis de los riesgos existentes tales como ciberacoso, estafas, sectas...
12.3. Implantación de un sistema de gestión de la seguridad de la información y Certificación CISM.
12.4. Cumplimiento de la normativa.