IFCT100PO. Seguridad de los sistemas informáticos y de comunicación.

Sku: 74863IN

Horas: 150

OBJETIVOS

- Gestionar la seguridad de las redes de comunicación.
- Conocer la seguridad informática, así como los principales problemas asociados a esta.
- Identificar los problemas de seguridad informática.
- Saber cuáles son los aspectos vitales del RGPD y la LOPDGDD.
- Solucionar los problemas de seguridad informática.
- Identificar y clasificar el malware actual.
- Aplicar la seguridad física y del entorno que rodea a los dispositivos informáticos.
- Identificar la seguridad informática de la empresa.
- Gestionar la seguridad web.
- Clasificar los principales problemas de seguridad en redes wifi.
- Conocer los principales motivos de actualización para mejorar la seguridad.

CONTENIDOS

Unidad 1. Introducción a la seguridad.
Introducción.
La seguridad informática actual.
¿Qué es la seguridad informática?
Objetivos de la seguridad informática.
Amenazas.
Servicios de seguridad.
Criptografía.
Seguridad física versus seguridad lógica.
Clasificación de la seguridad en función de las medidas oportunas.
Resumen.

Unidad 2. Principales problemas de la seguridad informática.
Introducción.
De Von Neumann a nuestros días.
Configuraciones de redes.

Protocolos de red.
Tipos de vulnerabilidades.
Resumen.

Unidad 3. Gestión de la seguridad.
Introducción.
LOPDGDD y RGPD.
Series ISO/IEC 27000.
Resumen.

Unidad 4. Sistemas operativos seguros.
Introducción.
Los sistemas operativos en la actualidad.
Tipos sistemas operativos.
Windows 11. Instalación.
Ubuntu 19.04. Instalación.
Debian. Instalación.
Tipos de seguridad.
Resumen.

Unidad 5. Malware total.
Introducción
Malware infeccioso.
Malware oculto.
Malware para obtener beneficios.
Malware para robar información personal.
Ataques distribuidos.
Programas antimalware.
Métodos de protección.
Resumen.

Unidad 6. La seguridad física y el entorno.
Introducción.
La seguridad del edificio.
El entorno físico del hardware.
Resumen.

Unidad 7. Seguridad de la informática en la empresa.
Introducción.
¿Qué es OSSIM?
Componentes y herramientas integradas en OSSIM.
Conceptos básicos.
Resumen.

Unidad 8. Seguridad web.
Introducción.
Tipos de ataques.
Wargames.

Hacking Google.
Resumen.

Unidad 9. Seguridad en redes inalámbricas.
Introducción.
Las redes inalámbricas.
Riesgos de las redes inalámbricas.
Mecanismos de seguridad.
Guía básica de ataques Wireless.
Wifi segura.
Resumen.

Unidad 10. Seguridad en continua actualización.
Introducción.
Herramientas de seguridad.
La importancia de estar actualizado.
Resumen.