

Planificación de la seguridad informática en la empresa

Modalidad: curso e-Learning Duración: 80 horas

Categorías: Ofimática, informática y comunicaciones

OBJETIVOS

Planificar la seguridad informática en la empresa

CONTENIDOS

UNIDAD DIDÁCTICA 1. DEBILIDADES, AMENAZAS Y ATAQUES

- Tipos de atacantes
- Motivaciones del atacante
- Metodología de un atacante determinado
- Vulnerabilidades y ataques comunes
- Herramientas de hacking
- Ingeniería social
- Prevención de ataques
- Respuesta a contingencias

UNIDAD DIDÁCTICA 2. ADMINISTRACIÓN DE LA SEGURIDAD EN REDES.

- Diseño e implantación de políticas de seguridad

UNIDAD DIDÁCTICA 3. TECNOLOGÍAS CRIPTOGRÁFICAS.

- Encriptación simétrica
- Encriptación asimétrica
- Firmas digitales
- Certificados digitales
- SSL/TLS
- La herramienta de encriptación multiusos
- Navegación segura: HTTPS

UNIDAD DIDÁCTICA 4. SISTEMAS DE AUTENTIFICACIÓN.

- Tecnologías de Identificación
- PAP y CHAP
- RADIUS
- El protocolo 802.1X
- La suite de protocolos EAP: LEAP, PEAP, EAP-TLS

Sistemas biométricos

UNIDAD DIDÁCTICA 5. REDES VIRTUALES PRIVADAS.

Beneficios y características

IP Sec

VPNs con SSL-TLS

UNIDAD DIDÁCTICA 6. FIREWALLS

Arquitectura de Firewalls

Filtrado de paquetes sin estados

Servidores Proxy

Filtrado dinámico o "stateful"

Firewalls de siguiente generación

Funciones avanzadas

UNIDAD DIDÁCTICA 7. DETECCIÓN Y PREVENCIÓN AUTOMATIZADA DE INTRUSIONES (IDS-IPS)

Arquitectura de sistemas IDS

Herramientas de software

Captura de intrusos con Honeypots