

- REF: SI015
- NOMBRE: SEGURIDAD EN INTERNET
- 25 HORAS

Objetivos:

- *Comprender y planificar una política de seguridad*
- *Comprender los puntos vulnerables y agujeros de seguridad*
- *Construir defensas contra los ataques comunes en redes*
- *Usar criptografía y autenticación para proteger datos*
- *Verificar transacciones usando certificados de clave pública y firmas digitales*
- *Asegurar el tráfico de Web y de correo*
- *Diseñar una arquitectura de seguridad*
- *Apreciar la naturaleza evolutiva de los ataques y defensas*

Dirigido:

- *Jefes de Proyecto.*
- *Responsables de departamentos IT.*
- *Administradores de Redes.*
- *Integradores de sistemas.*
- *Consultores y Auditores.*

Requisitos:

Conocimientos superiores de administración de sistemas Unix, Linux o NT/2000. Conocimientos altos en comunicaciones TCP/IP.

Contenido:

CURSO DE SEGURIDAD EN INTERNET

- **Introducción a la Seguridad de Red**
Definiciones de seguridad; Protección de su organización; Medidas de seguridad; Vulnerabilidades de sistemas (UNIX, NT, OS/2 y Windows)
- **Seguridad en el Mundo Real**
Crackers y hackers; Alarmas de seguridad y los medios; Seguridad y los vendedores; Seguridad y usted
- **Ataques de Sistema**
Riesgos de seguridad de los sistemas; Suplantación; Puertas traseras; Robo de contraseñas; Programas de ataque – Caballos de Troya; Virus y Gusanos
- **Ataques de Red**
Riesgos de seguridad de red; Espiar y escuchar la red; Análisis de tráfico; Ataques de repetición; Ataques de denegación de servicio
- **Seguridad del Protocolo Internet**
TCP/IP y seguridad; Asuntos relacionados con IP, ICMP y TCP; Ataques IP, ICMP, TCP y DNS
- **Política de Seguridad**
Implementación de una política de seguridad; Políticas de usuario; Principio del menor privilegio; Registro y auditoria; Detección de la intrusión; Actuación frente ataques; Herramientas de auditoria de seguridad
- **Protección con Encriptación**
Protección de la información via encriptación; Encriptación de red; Algoritmos de encriptación; Sistemas de encriptación por clave simétrica; Encriptación por clave pública; Sistemas Challenge-Response; Ataques a los sistemas de encriptación – criptoanálisis y fuerza bruta
- **Protección con Autenticación**
Autenticación de clientes y servidores; Autenticación de datos; Autenticación por clave pública/privada; Firmas digitales; Certificados digitales X.509; Entidades de confianza; Autoridades de certificación; Infraestructura y servicios de certificación
- **Seguridad Transaccional**
Seguridad de nivel de red; Point-to-point Tunnelling Protocol (PPTP); Secure Wide Area Networks (S/WAN), Seguridad de aplicaciones específicas; Pretty Good Privacy (PGP), Secure MIME (S/MIME), Secure Socket Layer (SSL); Private Communications Technology (PGT); Seguridad financiera; Secure Electronic Transactions (SET)
- **Seguridad de Servidor**
Servidores y seguridad; Seguridad de servidores WEB y de Correo; Seguridad de servicios Internet; Desarrollo de aplicaciones y seguridad (CGI, ISAPI, NSAPI y conectividad a bases de datos)

- **Arquitecturas de Seguridad**
Construcción de una arquitectura segura; Cortafuegos- principios, filosofía, implementaciones clásicas, productos y soluciones; Servicio de Proxy; Proxies de aplicación – Web/FTP; Proxies de nivel de red
- **Evolución de los Riesgos**
Evolución del riesgo y de las defensas; El camino a seguir

