
SEGURIDAD EN REDES”

COMO LOGRAR UNA ARQUITECTURA DE SEGURIDAD EN LA RED SIN SACRIFICAR EL DESEMPEÑO, NI LA DISPONIBILIDAD

ANTECEDENTES

La seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización. Este curso de seguridad en redes enfocado a las redes de datos convergentes, le permitirá por medio de metodologías de análisis de riesgo, identificar las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de su red y, por otro lado, entender la importancia de definir políticas, procedimientos y estándares, de acuerdo a los requerimientos de su negocio, basados en recomendaciones a nivel internacional. Se busca también en el curso de seguridad en redes, identificar las herramientas o productos tecnológicos que apoyen los controles que permiten mitigar el riesgo y mejorar de esta manera la seguridad en la red.

El curso sobre seguridad en redes cubre también aspectos como: disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y lógico, de tal forma que proponemos un enfoque integral de acercamiento a la seguridad de la información que viaja por su red, considerando elementos tales: Switches, Routers, Firewall, IPS/IDS, Gateway Antivirus, etc. De tal manera que se pueda combinar efectivamente la seguridad de la información en los diferentes sistemas hoy disponibles, sin afectar el desempeño de la red y mejorando a su vez la disponibilidad. Todo lo anterior conforma una estrategia integrada para la seguridad en su red.

OBJETIVO

En este curso teórico, sobre el tema seguridad en redes es complementado con una sesión de practica sobre un caso de estudio de la vida real, en donde se analiza los posibles retardos introducidos en una red por los dispositivos de seguridad, se busca generar en los asistentes, la motivación y el conocimiento necesarios para emprender un proceso continuo de mejoramiento de la seguridad de sus redes de voz y datos corporativas, con el objetivo de mejorar la seguridad de la red y por ende la seguridad de la información.

REQUISITOS

- ✚ Conocimiento del protocolo IP.
- ✚ Familiaridad con cálculos numéricos básicos para evaluación de desempeño.
- ✚ Participación en proyectos de diseño de redes seguras.
- ✚ Manejo de terminología básica del ingles técnico.

ORIENTADO A:

- + Ing de sistemas responsables de redes de datos.
- + Gerentes de tecnología.
- + Ingenieros electrónicos desempeñándose en el área de redes.
- + Administradores de la red
- + Oficiales de seguridad
- + Administradores de la seguridad de la red

VALOR DEL CURSO SEGURIDAD EN REDES:

El valor del curso seguridad en redes para máximo 6 participantes es de:

3000 U\$ (No IVA incluido y no gastos de viaje).

DURACION CURSO SEGURIDAD EN REDES

20 horas.

CONFERENCISTA: EL Ing Rodrigo Ferrer (rodrigo.ferrer@sisteseg.com) es egresado de la universidad de los Andes como ingeniero Eléctrico, en donde también ha realizado estudios de postgrado y especialización en telecomunicaciones y gestión de sistemas de información. Se ha desempeñado laboralmente en empresas de seguridad en redes tales como: 3com, Extreme Networks, Sonicwall, y Sisteseg, desempeñándose como Network Consultant para la región andina y como académico en varias universidades del país y ha participado en proyectos de consultoría a nivel nacional y en la región andina sobre modelos de seguridad y planes de continuidad del negocio. Posee la certificación CISSP (Certified Information System Security Profesional) del International Information Systems Security Certification Consortium (www.isc2.org), también la certificación CISA de ISACA y ABCP del DRI, CSSA, CST Sonicwall y COBIT f.c.

Como complemento a su formación tecnológica, ha realizado también realizado estudios de educación continuada en la Universidad de Cambridge en UK y actualmente está finalizando la Maestría en Filosofía, en la Universidad Javeriana con la tesis "La pregunta por la técnica".

DESCRIPCION DEL CURSO SEGURIDAD EN REDES:

MODULO I:

- + Introducción al concepto de seguridad en redes y seguridad de la información.
 - o Confidencialidad
 - o Integridad
 - o Disponibilidad y Desempeño
- + Seguridad en las redes y su relación con los estándares ISO 27001, ISO 17799, COBIT, BS25999 e ITIL.
- + ¿Qué es un verdadero análisis de riesgo?
- + Posibilidad de cuantificar el análisis de riesgo.
- + Desempeño y seguridad en la red.(Contradicción aparente)
- + Arquitectura de hardware de los dispositivos de seguridad en redes.

CURSO SEGURIDAD EN LA RED

-
- ✚ Análisis de disponibilidad, desempeño y seguridad para:
 - Routers
 - Switches
 - Firewalls tipo:
 - Packet filtering
 - Stateful
 - Proxy
 - Influencia del sistema operativo en los firewalls
 - IDS/IPS
 - Gateway Antivirus
 - Protección correo electrónico.(Mail Security)
 - SSL VPN
 - Dispositivos anti-spyware
 - ✚ Conectividad usando redes VPN.(IPSEC, SSL)
 - Análisis de desempeño para la seguridad en la red usando VPN
 - Recomendaciones para mejorar tiempos de respuesta
 - ✚ Optimización de la red y sus respectivos elementos.
 - En el procesamiento
 - Por medio del Tráfico diferenciado
 - Considerando planeamiento de capacidad en aplicaciones tipo WEB y en la Transferencia de archivos sobre el protocolo TCP.

MODULO II

- ✚ ¿Qué es una verdadera arquitectura de seguridad?
- ✚ Fundamentos para el diseño de una arquitectura de seguridad
- ✚ Seguridad física para garantizar la seguridad de la información.
 - Recomendaciones sobre seguridad física para el centro de cómputo.(NFPA 75, EIA/TIA 942)
 - Estrategias para el manejo del riesgo
 - Controles ISO 27001 para la seguridad física
- ✚ Importancia de los controles administrativos.
 - Políticas, procedimientos y estándares de configuración
 - Planes de contingencia para la red
- ✚ Conclusiones.
 - Estrategia integrada de seguridad en la red.
 - Controles Lógicos, físicos y administrativos
 - Seguridad sin sacrificar el desempeño o la disponibilidad
 - La seguridad en la red y su influencia en la seguridad de la información.

MODULO III (CASO DE ESTUDIO):

- ✚ Red con servidores FTP o WEB, Switches, Routers, Firewall.
- ✚ Switches nivel 3.

-
- ✚ Enlaces WAN y LAN.
 - ✚ Conectividad VPN para mejorar la seguridad en la red.
 - ✚ Se busca calcular los retardos para una aplicación FTP, con elementos de seguridad de esta forma se busca llegar a poseer una metodología de diseño de la seguridad en la red y la seguridad de la información.
 - ✚ Discutir las posibles alternativas para una arquitectura que mejore la seguridad en la red y la seguridad de la información.
 - ✚ Tener en cuenta el tema de la disponibilidad al diseñar una arquitectura de seguridad y siempre pensar en proponer estrategias para la recuperación ante una falla menor o mayor.
 - ✚ Ejemplo de configuración de un firewall tipo *stateful*.