

Seguridad en la Red (150 horas)

Especialmente orientado a Estudiantes, Técnicos y Profesionales, Gerentes, Administradores y todos aquellos relacionados con las áreas de Redes, Internet, Seguridad, Sistemas, Informática y tecnologías afines, que quieran adquirir los conocimientos sobre Seguridad en la Red.

Dirigido a: Especialmente orientado a Estudiantes, Técnicos y profesionales, gerentes, administradores y todo aquel relacionados con las áreas de Redes, Internet, Seguridad, Sistemas, Informática y tecnologías afines, que quieran adquirir los conocimientos sobre Seguridad en la Red.

Con este curso conseguirás: El estudiante estará en capacidad de desarrollar una infraestructura de seguridad. La consecución del título conlleva obtener el reconocimiento del Comité de Sistema de Seguridad Nacional (CNSS) nº 4011 que reconoce al estudiante como competente en las habilidades de la protección de seguridad de infraestructuras de redes.

Requisitos previos: El estudiante debe contar con la certificación de CCNA o conocimientos equivalentes, como lo son: Medios de transmisión. Dispositivo de Internet. Modelo OSI

Módulos:

Módulo 1: Principios de seguridad en redes - 30 Horas En este curso preparatorio para el CCNA Security, empezaremos con los principios básicos que conformarán el bloque que iremos estudiando durante los diversos módulos. Será, así, necesario analizar las posibles amenazas que pueden atacar a nuestro entorno y veremos por encima que herramientas o soluciones se podrían aplicar para evitarlo. Debemos poder ser capaces de analizar qué topologías no son seguras y qué posibles problemas pueden acarrear. Casi meramente teórico, lo importante es asentar los conocimientos que irán dando pie a un mejor entendimiento sobre los otros puntos que se tratarán durante el curso.

Unidad 1. Comprendiendo los principios de la Seguridad de Redes

Unidad 2. Desarrollo de una Red Segura

Unidad 3. Defensa del Perímetro

Módulo 2: Configuración de la seguridad - 40 Horas En este módulo se verán temas prácticos como la configuración de diversos apartados de seguridad en entornos con equipos tanto a nivel capa de enlace como de capa de 3.

Unidad 1. Configuración AAA

Unidad 2. Asegurando el Router

Unidad 3. Asegurando dispositivos de Capa 2

Unidad 4. Implementación de Seguridad de Equipos Terminales

Módulo 3: Extendiendo la seguridad a otros servicios - 40 Horas Servicios como la telefonía requieren de sus propias normas para establecer comunicaciones seguras, por lo que es útil estudiar en qué consiste y cómo utilizarla.

Unidad 1. Provisión de Seguridad SAN

Unidad 2. Explorando la seguridad en soluciones de Voz

Unidad 3. Uso de Cisco IOS Firewalls para defender la Red

Unidad 4. Uso de Cisco IOS IPS para asegurar la Red

Módulo 4: Las redes Privadas Virtuales - 40 Horas En este módulo se estudiará la tecnología que se dedica a la seguridad, las VPN. Como también los distintos protocolos de los que se pueda hacer uso cuando se crea las conexiones cifradas. También se analizarán los diversos tipos de VPN y en qué situaciones se les puede sacar más rendimiento.

Unidad 1. Implementación De Firmas Digitales y soluciones criptograficas

Unidad 2. Exploración de PKI y cifrado asimétrico. Confidencialidad

Unidad 3. Construcción de una solución VPN IPsec "Site-to-Site

El alumno marca su propio ritmo y en función de, tanto su nivel de partida, como su capacidad de aprendizaje, conseguirá finalizar antes el curso.

La duración descrita en horas es sólo una estimación, ya que el alumno dispone de todo el temario desde el momento de su inscripción.

Tutorización:

El alumno dispone de un servicio de correo electrónico con un tutor de primer nivel, para la resolución de dudas sobre contenidos y/o consultas complejas.

Otros datos de interés:

Material:

Se trata de un material específico propio, dirigido al cumplimiento del programa y con las tareas perfectamente estructuradas.

Cada bloque formativo, en general, se compone de 4 apartados:

- 1. Teoría en HTML editable y descargable en formato .pdf
- 2. Videos reproducibles y descargables
- 3. Prácticas o laboratorios planteados y resueltos
- 4. Preguntas de autoevaluación
- 5. Opcional: Archivos adicionales como presentaciones gráficas y temarios adicionales relacionados.