SEGURIDAD EN LA RED

1. **Nivel/etapa al que se dirige la actividad:**
   Especialmente orientado a Estudiantes, Técnicos y profesionales, gerentes, administradores ytodo aquel relacionados con las áreas de Redes, Internet, Seguridad, Sistemas, Informática y tecnologíasafines, que quieran adquirir los conocimientos sobre Seguridad en la Red.

2. **Horas de duración:**
   150horas. La duración es sólo una estimación, ya que el alumno dispone de todo el temario desde el momento de su inscripción.

3. **Número máximo de participantes:**
   ON-LINE.

4. **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

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

6. **Material:**
   Se trata de un material específico propio, dirigido al cumplimiento del programa y con las tareasperfectamente estructuradas.
   Cada bloque formativo, en general, se compone de 4 apartados:
   - Teoría en HTML editable y descargable en formato .pdf
   - Videos reproducibles y descargables
   - Prácticas o laboratorios planteados y resueltos
   - Preguntas de autoevaluación
   - Opcional: Archivos adicionales como presentaciones gráficas y temarios adicionales relacionados.

OBJETIVOS:

- El estudiante estará en capacidad de desarrollar una infraestructura deseguridad.
- 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.

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 losdiversos módulos. Será, así, necesario analizar las posibles amenazas que pueden atacar a nuestroentorno y veremos por encima que herramientas o soluciones se podrían aplicar para evitarlo. Deberemospoder 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 mejorentendimiento sobre los otros puntos que se tratarán durante el curso.

Lecciones:

- 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 laconfiguración de diversos apartados de seguridad en entornos con equipos tanto a nivel capa de enlacecomo de capa de 3.

Lecciones:

- 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 desus propias normas para establecer comunicaciones seguras, por lo que es útil estudiar en qué consiste ycómo utilizarla.

Lecciones:

- 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 sededica a la seguridad, las VPN. Como también los distintos protocolos de los que se pueda hacer usocuando se crea las conexiones cifradas. También se analizarán los diversos tipos de VPN y en quésituaciones se les puede sacar más rendimiento.

Lecciones:

- 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