CCNA SECURITY

250 HORAS

DESCRIPCIÓN

Los alumnos que realicen esta formación Cisco se introducirán en las tecnologías claves de seguridad y aprenderán cómo

desarrollar políticas de seguridad.

empleados poseen las habilidades necesarias para desarrollar una infraestructura de seguridad.

Este curso proporcionará a los estudiantes los conocimientos y habilidades necesarias para especializarse en el mundo de

la seguridad de redes Cisco. Es un curso práctico, orientado a soluciones con casos prácticos reales.

El curso de CISCO CCNA Security, está diseñado para especializar a los estudiantes de Cisco Networking Academy en el

mundo de la seguridad de redes.

OBJETIVOS

Los alumnos que realicen esta formación Cisco se introducirán en las tecnologías claves de seguridad y aprenderán cómo

desarrollar políticas de seguridad.

empleados poseen las habilidades necesarias para desarrollar una infraestructura de seguridad.

Este curso proporcionará a los estudiantes los conocimientos y habilidades necesarias para especializarse en el mundo de

la seguridad de redes Cisco. Es un curso práctico, orientado a soluciones con casos prácticos reales.

El curso de CISCO CCNA Security, está diseñado para especializar a los estudiantes de Cisco Networking Academy en el

mundo de la seguridad de redes.

CONTENIDOS

UNIDAD 1: Amenazas de seguridad en las redes modernas: Principios fundamentales de las redes seguras – Gusanos, virus y troyanos – Metodologías de ataque.

UNIDAD 2: Seguridad de los dispositivos de red: Seguridad del router de borde – Asignación de roles administrativos – Monitoreo y administración de dispositivos – Auditorias de seguridad.

UNIDAD 3: Autenticación, autorización y contabilidad: Propósito de AAA – Configuración de AAA – Configuración de AAA basada en servidor.

UNIDAD 4: Implementación de tecnologías de cortafuegos: Listas de control de acceso – Tecnologías de cortafuegos – Control de acceso basado en contexto – Políticas de cortafuegos

UNIDAD 5: Implementación de la prevención de la intrusión: Tecnologías IPS – Implementación de IPS.

UNIDAD 6: seguridad de la red de área local: Seguridad de terminales – Consideraciones de seguridad de capa 2 – Gíreles, VoIP y consideraciones de seguridad SAN.

UNIDAD 7: Criptografía: Seguridad de las comunicaciones – Servicios criptográficos – Resúmenes, firmas digitales y autentificación – Encriptación simétrica y asimétrica.

UNIDAD 8: Implementación de las redes privadas virtuales: VPNs – Componentes y operaciones de las VPNs IPSEC – Implementación de VPNs site-to-site – Implementación de VPNs de acceso remoto – Implementación de SSLVPNs.

UNIDAD 9: Gestionar una red segura: Ciclo de vida de una red segura – Red de autodefensa – Construcción de una política integral de seguridad.