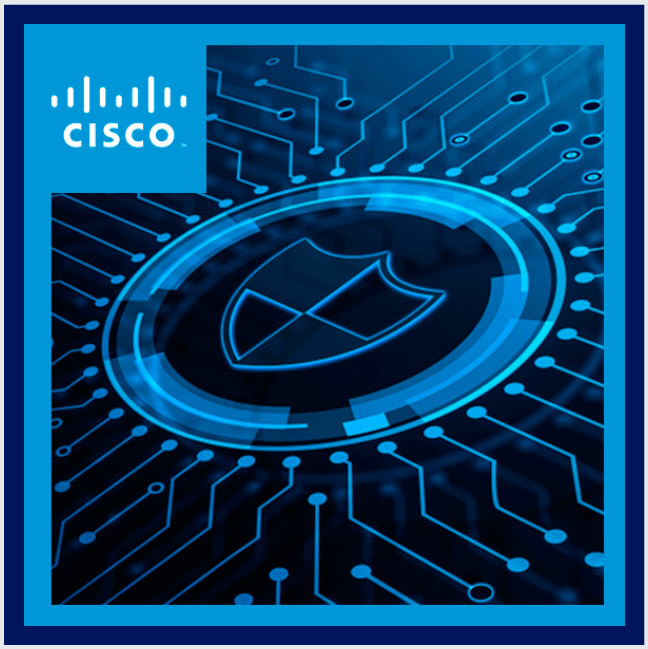
CCNA SECURITY

Código: CIS-011

Propuesta de Valor: HARDWARE - REDES - TELECOMUNICACIONES

Duración: 50 Horas Académicas



CCNA Security ayuda a los estudiantes a prepararse para las carreras de especialistas en seguridad en un nivel inicial a través de una comprensión profunda de los principios de seguridad de la red y de las herramientas y configuraciones necesarias para asegurar una red. El currículo proporciona una introducción a los conceptos de seguridad básicos y a las habilidades necesarias para la instalación, reparación y supervisión de dispositivos de red para mantener la integridad, confidencialidad y disponibilidad de los datos y dispositivos. Este curso enfatiza en la experiencia práctica junto con el aprendizaje en el aula y en línea.

AUDIENCIA

- Dirigido a estudiantes de nivel universitario o Profesionales en Ingeniería que buscan habilidades de redes de nivel empresarial, profesionales TI que desean expandir sus habilidades básicas en enrutamiento, conmutación y solución de problemas de red para avanzar en su carrera.
- Personal que haya ralizado y aprobado los 4 niveles de CCNA.
- O simplemente personas que desean obtener la certificación CCNA Security

PRE REQUISITOS

- Este curso está diseñado para estudiantes que tienen conocimientos y habilidades equivalentes a los aprendidos en Interconexión de dispositivos de red de Cisco Parte 1 (ICND1), Interconexión de dispositivos de red de Cisco Parte 2 (ICND2), conocimiento práctico del sistema operativo Windows y conocimiento de redes Cisco IOS. y conceptos.

OBJETIVOS

- Describir los componentes de una política de seguridad de red integral que se puede usar para contrarrestar las amenazas contra los sistemas de TI, dentro del contexto del ciclo de vida de la política de seguridad.
- Desarrollar e implementar contramedidas de seguridad destinadas a proteger los elementos de la red como parte de la infraestructura de la red.
- Implementar y mantener tecnologías de control y contención de amenazas para la seguridad del perímetro en redes pequeñas y medianas

- Describa las estrategias y tecnologías de conectividad seguras mediante VPN, así como la configuración de VPN de sitio a sitio y de acceso remoto utilizando las características de Cisco IOS.

CERTIFICACIÓN DISPONIBLE

Certificación emitida por COGNOS.

CONTENIDO

1. FUNDAMENTOS DE SEGURIDAD DE REDES

1.1. INTRODUCCION A LOS CONCEPTOS DE SEGURIDAD DE REDES
1.2. COMPRENDER LAS POLITICAS DE SEGURIDAD UTILIZANDO UN ENFOQUE DE CICLO DE VIDA
1.3. CONSTRUYENDO UNA ESTRATEGIA DE SEGURIDAD PARA REDES SIN FRONTERAS

2. PROTEGIENDO LA INFRAESTRUCTURA DE RED

2.1. INTRODUCCION A CISCO NETWORK FOUNDATION PROTECTION
2.2. PROTEGIENDO LA INFRAESTRUCTURA DE RED USANDO CISCO CONFIGURATION PROFESSIONAL
2.3. ASEGURANDO EL PLANO DE ADMINISTRACION EN DISPOSITIVOS CISCO IOS
2.4. CONFIGURACION DE AAA EN DISPOSITIVOS CISCO IOS UTILIZANDO CISCO SECURE ACS
2.5. ASEGURAR EL PLANO DE DATOS EN LOS SWITCHES CISCO CATALYST
2.6. ASEGURAR EL PLANO DE DATOS EN ENTORNOS IPV6

3. CONTROL DE AMENAZAS Y CONTENCION

3.1. PLANIFICACION DE UNA ESTRATEGIA DE CONTROL DE AMENAZAS
3.2. IMPLEMENTACION DE LISTAS DE CONTROL DE ACCESO PARA LA MITIGACION DE AMENAZAS
3.3. ENTENDER LOS FUNDAMENTOS DEL CORTAFUEGOS
3.4. IMPLEMENTACION DE FIREWALLS DE POLITICAS BASADAS EN LA ZONA DE CISCO IOS
3.5. CONFIGURACION DE POLITICAS BASICAS DE FIREWALL EN DISPOSITIVOS ASA DE CISCO
3.6. ENTENDER LOS FUNDAMENTOS DE IPS
3.7. IMPLEMENTANDO CISCO IOS IPS

4. CONECTIVIDAD SEGURA

4.1. ENTENDER LOS FUNDAMENTOS DE LAS TECNOLOGIAS VPN
4.2. INTRODUCCIóN A LA INFRAESTRUCTURA DE CLAVE PúBLICA
4.3. EXAMINANDO LOS FUNDAMENTOS DE IPSEC
4.4. IMPLEMENTACION DE VPN DE SITIO A SITIO EN LOS ROUTERS CISCO IOS
4.5. IMPLEMENTANDO SSL VPNS USANDO DISPOSITIVOS ASA DE CISCO

BENEFICIOS

Al finalizar el curso tendrá solidos conocimientos sobre los principios de seguridad de la red y de las herramientas y configuraciones necesarias para asegurar una red.