



Presentación del Curso

**Curso de Formador de Formadores
CCNA Cyber Ops**



Tabla de contenido

DESCRIPCIÓN GENERAL	3
PÚBLICO OBJETIVO	3
OBJETIVOS DE APRENDIZAJE	3
DURACIÓN.....	4
CONTENIDOS	4
COMPETENCIAS PREVIAS	6
RECURSOS.....	6
ASPECTOS METODOLÓGICOS.....	6
CRITERIOS DE APROBACIÓN	7
CERTIFICADO	7
PERFIL DEL FACILITADOR.....	7



CURSO DE FORMADOR DE FORMADORES CCNA CYBER OPS

Descripción general

El presente curso se desarrollará en la modalidad presencial, el cual le permitirá prepararse y acreditarse como Formador de Formadores de CCNA CYBER OPS bajo la modalidad definida por la Academia de Networking de Cisco.

Para ser Formador de Formadores en CCNA CYBER OPS, debe conocer el temario de CCNA CYBERSECURITY OPERATIONS, el cual ofrece una cobertura integral y completa de ciberseguridad en la red, y en los que aprenderá sobre:

- Desarrollar las clases del curso correspondiente utilizando la plataforma "Netacad".
- Guiar al estudiante en el desarrollo de los laboratorios.
- Lograr la formación exitosa del estudiante en el mundo de la Ciberseguridad.

El curso es apropiado para el público en general de muchos niveles de educación y tipos de instituciones, como escuelas secundarias, institutos de enseñanza superior, universidades, escuelas técnicas y de formación profesional, y centros comunitarios, que brindará numerosas oportunidades de experiencia práctica y desarrollo de destrezas profesionales.

También usted podrá desarrollar un pensamiento crítico y habilidades para resolver problemas mediante programas de monitoreo y detección de a la red.

Con esta capacitación le permitirá ser uno de las pocas personas que es **formador de formadores del curso de CCNA CYBER OPS de la Academy Networking Cisco.**

Público Objetivo

El curso de FORMADOR DE FORMADORES CCNA CYBER OPS, está dirigido a todas los profesionales de Tecnologías de la Información, Ingeniería Electrónica, Ingeniería en Sistemas o afines, que desean instruir los conocimientos la Academy Networking Cisco.

Objetivos de aprendizaje

Objetivo general:

- Proveer un entrenamiento teórico y práctico utilizando herramientas, lineamientos y procedimientos para monitorear, detectar y contener ataques de red, así como el desarrollo de exámenes y actividades orientadas a la docencia de acuerdo con el perfil requerido para un instructor Cisco.

Objetivos específicos:

Los participantes que finalicen el curso de Formador de Formadores CCNA CYBER OPS serán capaces de:

- Desarrollar las clases del curso correspondiente utilizando la plataforma "Netacad".
- Guiar al estudiante en el desarrollo de los laboratorios.
- Lograr la formación exitosa del estudiante en el mundo de la Ciberseguridad.

Duración

El curso tiene una duración de 70 horas.

Contenidos

CAPÍTULO 1: LA CIBERSEGURIDAD Y EL CENTRO DE OPERACIONES DE SEGURIDAD

- 1.1. El peligro
- 1.2. Soldados en la guerra contra la ciberdelincuencia

CAPÍTULO 2: SISTEMA OPERATIVO WINDOWS

- 2.1. Descripción General de Windows
- 2.2. Administración de Windows

CAPÍTULO 3: SISTEMA OPERATIVO LINUX

- 3.1. Descripción general de Linux
- 3.2. Administración de Linux
- 3.3. Hosts de Linux

CAPÍTULO 4: PROTOCOLOS Y SERVICIOS DE RED

- 4.1. Protocolos de red
- 4.2. Protocolo de Ethernet y protocolo de Internet IP
- 4.3. Verificación de conectividad
- 4.4. Protocolo de resolución de direcciones
- 4.5. La capa de transporte
- 4.6. Servicios de red

CAPÍTULO 5: INFRAESTRUCTURA DE LA RED

- 5.1. Dispositivos de comunicación de red
- 5.2. Infraestructura de seguridad de red

- 5.3. Representaciones de red

CAPÍTULO 6: PRINCIPIOS DE LA SEGURIDAD DE REDES

- 6.1. Los atacantes de y sus herramientas
- 6.2. Amenazas y ataques comunes

CAPÍTULO 7: UNA MIRADA MÁS DETALLADA A LOS ATAQUES A LA RED

- 7.1. Monitoreo de red y herramientas
- 7.2. Ataque a las bases
- 7.3. Un ataque a lo que hacemos

CAPÍTULO 8: PROTEGER LA RED

- 8.1. ¿Qué es la defensa?
- 8.2. Control de acceso
- 8.3. Inteligencia contra amenazas

CAPÍTULO 9: LA CRIPTOGRAFÍA Y LA INFRAESTRUCTURA DE CLAVES PÚBLICAS

- 9.1. Criptografía
- 9.2. Infraestructura de claves públicas

CAPÍTULO 10: SEGURIDAD Y ANÁLISIS DE TERMINALES

- 10.1. Protección de terminales
- 10.2. Evaluación de vulnerabilidades de terminales

CAPÍTULO 11: MONITOREO DE LA SEGURIDAD

- 11.1. Tecnologías y protocolos
- 11.2. Archivos de registro

CAPÍTULO 12: ANÁLISIS DE DATOS DE INTRUSIONES

- 12.1. Evaluar alertas
- 12.2. Trabajar con datos de seguridad de la red
- 12.3. Informática forense digital

CAPÍTULO 13: RESPUESTA Y MANEJO ANTE INCIDENTES

- 13.1. Modelos de respuesta ante los incidentes
- 13.2. Manejo de incidentes

Competencias previas

Conocimientos: Es recomendable que los participantes de este curso, hayan aprobado el curso CCNA CYBERSECURITY OPERATIONS dentro de la Academia de Networking Cisco.

Habilidades o destrezas: Los participantes deben tener certificación activa de CCNA CYBERSECURITY OPERATIONS, uno o más años de experiencia profesional implementando y administrando soluciones de Cisco, en monitoreo, detección y respuesta a amenazas de ciberseguridad.

Valores: Los participantes deben establecer criterios éticos respecto al manejo y evaluación de los comportamientos observables de las personas.

Recursos

- Habilidades de navegación de PC y de Internet
- Tiempo para el desarrollo de las actividades de aprendizaje planificadas, así como para las actividades que realice de manera autónoma
- Disponer de una computadora con conexión a internet.
- Tener una cuenta de correo electrónico.

Aspectos metodológicos

- La capacitación se desarrollará en la modalidad presencial, para lo cual, se realizará un control de asistencia de los participantes en el horario establecido.
- Los contenidos del curso están a su disposición las 24 horas del día y los 7 días de la semana dentro del tiempo establecido para la duración del curso, por lo que, todos los participantes pueden organizar su propio horario de estudio.
- El curso es teórico – práctico, por cuanto el estudiante se apoyará en la plataforma de NetAcad, para lo cual se creará un nombre de usuario y contraseña para el acceso.
- Cada día se presentan contenidos que son estructurados con actividades individuales y colaborativas, recursos complementarios y herramientas que estarán disponibles en formatos para navegar.
- El seguimiento tutorial efectuado es constante y proactivo, lo que garantiza el éxito del proceso de aprendizaje.

Criterios de aprobación

El Programa de Capacitación Formador de Formadores CCNA CYBER OPS que administra ESPE INNOVATIVA EP es de aprobación, para lo cual se aplican las siguientes evaluaciones académicas por cada uno de los módulos:

Exámenes electrónicos por capítulo, estos exámenes pueden presentarlos en base a la planificación académica del instructor en el horario de las clases presenciales o fuera de ellas.

Prácticas de laboratorio por cada capítulo y práctica final (skills).

- Examen Final Teórico
- Examen Final Práctico
- Examen Feedback (Satisfacción del Cliente)

Todas las evaluaciones son calificadas sobre 100 puntos, por lo que para aprobar cada uno de los módulos el participante debe obtener una nota promedio de todas las evaluaciones descritas de 80/100 puntos y registrar una asistencia mínima del 80% a las sesiones presenciales.

Certificado

El participante que cumpla con los criterios de aprobación, recibirá un certificado:

- Certificado con el aval de la Universidad de las Fuerzas Armadas – ESPE, ESPE INNOVATIVA EP, SETEC.

Perfil del Facilitador

Formación académica

Pregrado:

Título de grado de tercer nivel en carreras como Ingeniería Electrónica, Sistemas, Tecnologías de la Información o afines.

Posgrado (De preferencia):

- Redes y Telecomunicaciones
- Gerencia de Sistemas y Tecnología Empresarial
- Gestión de la Seguridad de la Información
- Seguridad Informática y Hacking Ético

Otros:

- Certificación activa de Cisco CCNA CYBER OPS.

Experiencia relacionada:

- Desempeño profesional en el área de su especialidad
- Docencia en áreas relacionadas a su especialidad
- Instructor de cursos CCNA CYBER OPS en la Academy Networking Cisco.

Esta obra está bajo una licencia de [Creative Commons Reconocimiento-NoComercial-SinObraDerivada 3.0 Ecuador](https://creativecommons.org/licenses/by-nc-nd/3.0/ec/)

