

Cisco CCNA Cyberops Associate

Descrición

CCNA Cybersecurity Operations - CYBER OPS introduce os coñecementos e habilidades necesarias para asumir con éxito as tarefas, deberes e responsabilidades das/os analistas de seguridade de nivel asociado que traballan en centros de operacións de seguridade (SOC). Este curso introduce os conceptos de seguridade fundamentais e habilidades necesarias para supervisar, detectar, analizar e dar resposta á ciberdelincuencia, ciberespionaxe, ameazas internas, ameazas persistentes avanzadas, requisitos normativos e outros problemas de ciberseguridade aos que se enfrontan as organizacións. Así mesmo, fai fincapé na aplicación práctica das habilidades necesarias para manter e garantir a dispoñibilidade de seguridade operativa dos sistemas en rede.

A formación ten unha duración de 80 horas presenciais (40 presenciais e 40 en aula virtual síncrona).

HORARIO: De luns a venres de 16:30 a 20:30 horas.

. **Clases presenciais:** 25, 26, 27 de maio; 1, 4, 8, 11, 15, 18 de xuño

. **Clases virtuais:** 28, 29 de maio; 2, 3, 5, 9, 10, 12, 16, 17, 19 de xuño

Obxectivos

Unha vez rematado o curso, o alumnado adquirirá os coñecementos necesarios para:

- Comprender os principios, roles e responsabilidades involucrados nas operacións de ciberseguridade, así como as tecnoloxías, ferramentas, regulacións e estándares dispoñibles
 - Describir vulnerabilidades e ameazas comúns en dispositivos de usuario e infraestruturas de rede
 - Demostrar habilidades fundamentais aplicadas ao seguimento, detección, investigación, análise e resposta a incidentes de seguridade
 - Clasificar eventos intrusivos segundo categorías definidas por modelos de seguridade e establecer accións defensivas
 - Realizar con éxito as tarefas, deberes e responsabilidades dun analista de seguridade de nivel asociado nun Centro de Operacións de Seguridade (SOC)

Dirixido a

Dirixido a profesionais de IT (enseñeiras/os de Networking, administradoras/es de rede, etc.) que queiran iniciarse no tema da ciberseguridade, aumentando o seu coñecemento e experiencia nesta área de demanda crecente e nos procedementos empregados nun Centro de Operacións de Seguridade -SOC. Débense destacar os escenarios prácticos do curso baseados nas distribucións de Kali Linux e Security Onion, que incorporan ferramentas especializadas en probas de penetración e auditoría, así como ferramentas de análise, clasificación e monitorización de alertas.

Para un maior aproveitamento do curso, recoméndase que o alumnado teña coñecementos básicos de sistemas operativos Windows e/ou Linux, e un nivel de coñecementos previos en redes equivalente a ter completados os módulos 1 e 2 do curso CCNA R&S (conceptos básicos de redes, coñecemento de sistemas binarios e hexadecimais, conceptos básicos de programación e coñecemento de consultas básicas de SQL).

O manual e a certificación do curso están en inglés.

BENEFICIOS

Opción gratuita dun exame de certificación oficial

Diploma de asistencia

Perfil do docente

O persoal docente son instrutoras/es acreditadas/os polo programa Cisco Netacad e certificadas/os nas especialidades que imparten. Teñen máis de 5 anos de experiencia nesta área.

Cisco CCNA Cyberops Associate

PROGRAMA	Programación 2025/26
TIPO	CURSO
MATRÍCULA	Gratuíta
PERIODO INSCRICIÓN	01/04/2026 - 17/04/2026
PROBA DE SELECCIÓN	22/04/2026 (18:30)
CRITERIOS DE SELECCIÓN	Proba técnica presencial no CNTG en Santiago de Compostela
Nº PRAZAS	20 (Mínimo 10)
METODOLOXÍA	Presencial + virtual
TIPO DE EDICIÓN	Edición única tarde (desempregados/as e ocupados/as)
DURACIÓN	80 horas (36h presenciais, 44h virtuais)
DATA INICIO	25/05/2026
DATA FIN	19/06/2026
HORARIO	De luns a venres de 16:30 a 20:30 horas.
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	Understanding Cisco Cybersecurity Operations Fundamentals
MÓDULOS TRANSVERSAIS	Igualdade de 10 horas

TECNOLOXÍA

Cisco

Ciberseguridade/Ciberseguridad

PERIODO DOCENCIA

25/05/2026 - 19/06/2026

Temario

Módulo 1. Ciberseguridade: o Centro de Operacións de Seguridade – SOC

Módulo 2. Sistema operativo Windows

Módulo 3. Sistema operativo Linux

Módulo 4. Protocolos e servizos de rede

Módulo 5. Infraestrutura de rede

Módulo 6. Principios de seguridade en rede

Módulo 7. Ataques de rede: Unha inspección detallada

Módulo 8. Protección da rede

Módulo 9. Infraestrutura e Criptografía de clave pública

Módulo 10. Análise e seguridade de dispositivos finais

Módulo 11. Monitorización de seguridade

Módulo 12. Análise de datos de intrusionés

Módulo 13. Resposta e xestión de incidencias

