CompTIA Cybersecurity Analyst (CySA+)

Descrición

Aprende a detectar, analizar e protexer infraestruturas críticas utilizando ferramentas de detección e análise de ameazas.

Adquire as tácticas e ferramentas necesarias para xestionar riscos de ciberseguridade, identificar distintos tipos de ameazas comúns, avaliar a seguridade dunha organización, recompilar e analizar intelixencia de ciberseguridade e xestionar incidentes a medida que ocorren. É un enfoque integral da seguridade dirixido a quen está na primeira liña de defensa.

Este curso está deseñado para axudar aos estudantes para prepararse para o exame de certificación CompTIA CySA+ – Cybersecurity Analyst+

A certificación **CompTIA CySA+** é unha acreditación global, independente do fabricante, que cobre coñecementos e habilidades de nivel intermedio requiridos nos roles de analista de seguridade da información. Axuda a identificar a capacidade dun profesional de ciberseguridade para defender proactivamente unha organización mediante monitorización segura, identificación de ameazas, resposta a incidentes e traballo en equipo. O exame CompTIA CySA+ garante que o candidato posúe os coñecementos e habilidades necesarios para:

- Identificar e investigar actividades sospeitosas en redes, endpoints e contornas cloud para descubrir posibles ameazas de seguridade.
- Identificar, priorizar e mitigar vulnerabilidades utilizando enfoques de xestión de vulnerabilidades baseados en riscos.
- Investigar e responder a incidentes de ciberseguridade utilizando procesos estruturados de resposta a incidentes e técnicas reais.
- Utilizar conceptos modernos de operacións de seguridade, incluíndo intelixencia de ameazas, *threat hunting*, automatización e operacións de seguridade asistidas por IA.

Obxectivos

- Identificar e investigar actividade sospeitosa en redes, endpoints e contornas cloud para descubrir posibles ameazas de seguridade.
- Monitorizar e analizar datos utilizando ferramentas estándar do sector, como plataformas SIEM e EDR.
- Identificar, priorizar e mitigar vulnerabilidades mediante enfoques baseados en riscos.
- Investigar e responder a incidentes de seguridade utilizando procesos estruturados e técnicas aplicadas en contornas reais.
- Comunicar claramente achados e riscos de seguridade ás partes interesadas mediante informes e paneis de control (dashboards).
- Aplicar prácticas de seguridade en contornas cloud e híbridos, garantindo operacións eficientes e efectivas.

Dirixido a

- Analista de Seguridade Informática (IT Security Analyst)
- Analista do Centro de Operacións de Seguridade (SOC Analyst)
- Analista de Vulnerabilidades (Vulnerability Analyst)
- Especialista en Ciberseguridade (Cybersecurity Specialist)
- Analista de Intelixencia de Ameazas (Threat Intelligence Analyst)
- Enxeñeiro de Seguridade (Security Engineer)

BENEFICIOS Opción gratuita dun exame de certificación oficial

Diploma de asistencia

Perfil do docente

Consultor e instrutor con máis de 20 anos de experiencia no sector TIC. Certificado en tecnoloxías Microsoft e CompTIA, especializado en ciberseguridade, redes e telecomunicacións. Conta cunha ampla experiencia na impartición de formación técnica orientada a certificacións oficiais, así como no deseño, implementación e administración de infraestruturas de sistemas, redes e comunicacións, e no desenvolvemento de proxectos de seguridade informática en contornas empresariais e educativas.

PROGRAMA Programación 2026/27

TIPO CURSO

MATRÍCULA Gratuíta

CompTIA Cybersecurity Analyst (CySA+)

PERIODO INSCRICIÓN	01/10/2026 - 15/10/2026
PROBA DE SELECCIÓN	16/10/2026 (00:00)
CRITERIOS DE SELECCIÓN	Proba técnica presencial no CNTG en Santiago de Compostela
Nº PRAZAS	20 (Mínimo 10)
METODOLOXÍA	Virtual
TIPO DE EDICIÓN	Edición única tarde (desempregados/as e ocupados/as)
DURACIÓN	35 horas
DATA INICIO	23/11/2026
DATA FIN	04/12/2026
HORARIO	De luns a vernes de 16:30 a 20:00 horas.
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	Cybersecurity Analyst+ (CS0-004)
MÓDULOS TRANSVERSAIS	Igualdade de 5 horas
TECNOLOXÍA	Ciberseguridade/Ciberseguridad CompTIA
PERIODO DOCENCIA	23/11/2026 - 04/12/2026

Temario

Módulos do Curso

- Identificación dos fundamentos das operacións de seguridade
- Aplicación de estratexias de xestión de riscos
- Xestión da seguridade e configuración de sistemas
- Comparación de arquitecturas de sistemas
- Aplicación da xestión de accesos
- Intelixencia de ameazas e threat hunting
- Avaliación de vulnerabilidades de rede
- Xestión da resposta a incidentes e comunicación
- Execución de plans de resposta a incidentes
- Análises de actividade maliciosa
- Automatización da análise de datos
- Mellora de procesos mediante automatización
- Avaliación de vulnerabilidades en aplicacións
- Seguridade en aplicacións

LABS

- Live Lab: Operar unha estación de traballo SOC
- Applied Live Lab: Avaliar a superficie de ataque e o hardening do sistema
- Live Lab: Despregar unha aplicación na nube mediante CI/CD
- Live Lab: Despregar unha aplicación en contedores mediante CI/CD
- Live Lab: Configurar autenticación federada e PAM
- Applied Live Lab: Aplicar protección de datos e seguridade en endpoints
- Live Lab: Configurar un honeypot
- Live Lab: Implementar intelixencia de ameazas
- Applied Live Lab: Analizar escaneos de vulnerabilidades
- Live Lab: Configurar rexistro centralizado (centralized logging)
- Live Lab: Utilizar un playbook para resposta a incidentes
- Live Lab: Rexistrar evidencias dun caso
- Live Lab: Crear consultas de análises de rexistros (log analysis queries)
- Live Lab: Configurar un sandbox
- Applied Live Lab: Analizar actividade anómala nun host
- Indicadores de compromiso en redes
- Applied Live Lab: Analizar actividade anómala na rede
- Indicadores en aplicacións e servizos web
- Live Lab: Analizar correos de phishing
- Challenge Live Lab: Resolver casos de resposta a incidentes
- Live Lab: Implementar unha solución de automatización
- Live Lab: Realizar rule tuning
- Live Lab: Engadir IA a un playbook de resposta a incidentes
- Applied Live Lab: Analizar vulnerabilidades en infraestrutura cloud
- Applied ALive Lab: Analizar vulnerabilidades en servizos web
- Live Lab: Integrar escaneo de seguridade nunha pipeline CI/CD
- Challenge Live Lab: Resolver vulnerabilidades en cloud e aplicacións