CompTIA Security X Certification

CompTIA SecurityX es la certificación de **máximo nivel** en la ruta de ciberseguridad de CompTIA. Valida habilidades de **arquitectura, ingeniería y operaciones de seguridad** para proteger entornos complejos **on-premises (locales)**, **cloud** e **híbridos**.

Es la evolución de CASP+ y está pensada para profesionales senior que desean demostrar dominio a nivel **Security Architect** o **Senior Security Engineer**.

Impartimos este curso **en aula virtual en directo**, con enfoque práctico, formadores certificados y materiales oficiales.

Objetivos

¿Qué aprenderás?
Al finalizar el curso estarás preparado para:

- **Arquitectar, integrar e implementar** soluciones seguras en infraestructuras complejas, alineando seguridad y objetivos de negocio.
- Aplicar **gobernanza, cumplimiento, gestión de riesgos y *threat modeling*** a escala corporativa.
- Utilizar **automatización, monitorización, detección y respuesta a incidentes** para sostener operaciones de seguridad resilientes.
- Endurecer sistemas y **diseñar arquitecturas** seguras (incluida criptografía y tendencias emergentes como IA) tanto en **cloud** como en **local/híbrido**.
- Prepararte para el examen **SecurityX CAS-005**, cuyos dominios son: GRC (20%), Arquitectura (27%), Ingeniería (31%) y Operaciones (22%).

¿Por qué debería hacer este curso?

- **Nivel más alto de CompTIA en ciberseguridad**, con reconocimiento internacional e **independiente del fabricante**.
- **Relevancia estratégica:** mapea a 19 roles NICE y a 19 roles DCWF, y está **aprobada por DoD 8140.03M**; cumple ISO/ ANSI 17024.
- **Transición de CASP+ a SecurityX:** el **cambio de nombre** no afecta al estatus de quienes ya tenían CASP+; se emite automáticamente la nueva **insignia**.

¿Qué valor me aporta a mí?

- Te posiciona para **roles senior** que lideran arquitectura y operaciones en entornos complejos.
- Mejora tu **empleabilidad y reputación** por su foco en integración técnica, diseño seguro y GRC.
- Indicadores salariales (EE. UU. orientativos): mediana anunciada de **150.270 $** para Security Architects, con rangos de **106.240–197.380 $** según experiencia. *(Referencia sectorial; no constituye garantía en España.)*

¿En qué beneficia a mi empresa que yo lo haga?

- Acelera la **madurez de seguridad** y la alineación con **cumplimiento normativo** (GRC).
- Capacita para **automatizar, monitorizar y operar** seguridad con detección y respuesta eficaces, reduciendo tiempo de exposición.
- Refuerza la **resiliencia** en cloud y en entornos locales, aportando visión de **arquitectura** y **ingeniería** de seguridad de extremo a extremo.

Audiencia

- **Security Architects** y **Senior Security Engineers** que lideran la postura de seguridad de la empresa.
- **Information Security Officers** que necesitan validar capacidades a nivel corporativo.
- Profesionales con **10+ años en IT** (mín. 5 en seguridad)

Requisitos previos

- Recomendado: **10 años de experiencia práctica en IT** (5 en seguridad) y dominio equivalente a **Network+, Security+, CySA+, Cloud+, PenTest+**.
- Si no cumples al 100% te asesoramos sobre **itinerarios previos** o un plan de refuerzo.

Metodología

Aula virtual en directo.

Duración

5 días

Temario del curso

1. **Módulo 1: Introducción a Copilot**
   - Preevaluación
2. **Módulo 2: Resumiendo la Gobernanza, Riesgo y Cumplimiento**
   - Implementar componentes de gobernanza apropiados
   - Explicar el cumplimiento legal
   - Aplicar estrategias de gestión de riesgos
3. **Módulo 3: Implementación de Arquitectura y Diseño**
   - Aplicar el desarrollo de Software
   - Integración de la arquitectura de software
   - Apoyar la resiliencia operativa
   - Implementar infraestructura en la nube
   - Integrar conceptos de confianza cero
   - Solución de problemas usando AAA y IAM
4. **Módulo 4: Comprendiendo la Ingeniería de Seguridad**
   - Mejora de la seguridad de los endpoints
   - Configurar la infraestructura de red

- Iniciar la automatización de la seguridad
- Aplicar conceptos de criptografía

5. **Módulo 5: Aplicación de las Operaciones de Seguridad y la Respuesta a Incidentes**

- Realizar modelado de amenazas
- Examinar la monitorización de la seguridad
- Analizar métodos de ataque conocidos y mitigaciones asociadas
- Aplicar herramientas y tecnologías de caza de amenazas
- Evaluar el análisis y la respuesta a incidentes