

La certificación para proteger y gobernar sistemas de inteligencia artificial y usar la IA para fortalecer las operaciones de ciberseguridad.

¿Por qué debería asistir?

CompTIA SecAI+ es la primera certificación de la Expansion Series de CompTIA. Cubre cómo asegurar y gobernar los sistemas de IA, cómo usar la IA en las operaciones de ciberseguridad y cómo adoptarla de forma responsable. Está pensada para profesionales de seguridad que ya cuentan con una base sólida y quieren especializarse en la intersección entre la IA y la ciberseguridad.

Durante el curso, los participantes aprenden a aplicar conceptos de IA para mejorar la postura de seguridad de la organización; a proteger los datos, los modelos y la infraestructura de IA con controles avanzados; a usar la IA para automatizar flujos de trabajo, acelerar la respuesta a incidentes y escalar las operaciones de seguridad; a aplicar marcos globales de gobierno, riesgo y cumplimiento a la adopción ética de la IA, y a defenderse de amenazas impulsadas por IA, como ataques adversarios, malware automatizado y el mal uso de la IA generativa. El programa cubre el 100 % de los objetivos del examen CY0-001.

5 días	4	Expansion	Prácticos	Avanzado
DURACIÓN	DOMINIOS OFICIALES	SERIE	LABORATORIOS	NIVEL



¿Quién debería participar?

Analistas e ingenieros de seguridad
Profesionales que protegen sistemas, datos y modelos de IA en la organización.

Equipos de SOC
Analistas que incorporan la IA a la detección, la correlación de alertas y la respuesta.

Arquitectos de seguridad y DevSecOps
Especialistas que integran la IA segura en pipelines y en la estrategia de seguridad.

Responsables de riesgo y cumplimiento
Profesionales de GRC que definen el uso ético y conforme de la IA.

Objetivos de aprendizaje

- Aplicar conceptos de IA para mejorar la postura de ciberseguridad de la organización.
- Reconocer amenazas impulsadas por IA: phishing automatizado, malware polimórfico y aprendizaje automático adversario.
- Proteger los datos, los modelos y la infraestructura de IA con controles avanzados.
- Asegurar los entornos de despliegue de IA locales, en la nube e híbridos.
- Usar la IA para automatizar flujos de trabajo y acelerar la detección y la respuesta a incidentes.
- Aplicar la IA al modelado de amenazas, el análisis de comportamiento y el monitoreo continuo.
- Aplicar marcos de gobierno, riesgo y cumplimiento como el NIST AI RMF y el RGPD a la adopción de la IA.
- Integrar la IA segura en los pipelines de DevSecOps y en la estrategia de seguridad empresarial.

Áreas de habilidad

Fundamentos de IA | Machine learning | Amenazas de IA | Ataques adversarios | Seguridad de modelos | Pipelines de datos | IA en el SOC | Automatización | Modelado de amenazas | NIST AI RMF | Ética de la IA | DevSecOps

Programa del curso

Duración: 5 días

Modalidades de formación

- **Presencial** — En aula, con instructor
- **Online** — En vivo, con instructor
- **Híbrida** — Aula y online combinadas

Módulo	Contenido
Dominio 1 **Día 1**	**1.0 Conceptos básicos de IA para ciberseguridad (17 %)** Principios y terminología de IA, machine learning, deep learning, NLP y automatización; aplicaciones de la IA en seguridad; amenazas impulsadas por IA: phishing automatizado, malware polimórfico y uso malicioso de la IA generativa.
Dominio 2 (parte 1) **Día 2**	**2.0 Seguridad de los sistemas de IA (40 %)** Controles de seguridad para proteger sistemas, datos y modelos de IA; seguridad de los entornos de despliegue locales, en la nube e híbridos.
Dominio 2 (parte 2) **Día 3**	**2.0 Seguridad de los sistemas de IA (cont.)** Mitigación de riesgos adversarios sobre los modelos, los pipelines de datos y las capas de inferencia.
Dominio 3 **Día 4**	**3.0 Seguridad asistida por IA (24 %)** Detección y respuesta con IA (anomalías, amenazas y remediación); automatización del triaje, la correlación de alertas y la orquestación; IA aplicada al modelado de amenazas y al monitoreo continuo.
Dominio 4 **Día 5**	**4.0 Gobierno, riesgo y cumplimiento de la IA (19 %)** Marcos regulatorios globales; GRC en todo el ciclo de vida de la IA; directrices éticas y normas como el RGPD y el NIST AI RMF. ✔ **Repaso integral y preparación para el examen** Repaso por dominio, práctica con preguntas basadas en desempeño y simulacro del examen CY0-001.

El contenido sigue los 4 dominios oficiales del examen CompTIA SecAI+ CY0-001 (V1); el porcentaje indica el peso de cada dominio en el examen.

Examen y certificación

Título	CompTIA SecAI+ – Versión 1
Código	CY0-001
Preguntas	Máximo 60
Formato	Opción múltiple y preguntas basadas en desempeño
Duración	60 minutos
Aprobación	600 (escala de 100–900)
Idioma	Inglés y japonés
Plataforma	Pearson VUE (centro de pruebas o en línea con OnVUE)

Requisitos de elegibilidad

- No hay requisitos obligatorios. CompTIA recomienda de 3 a 4 años de experiencia en TI, al menos 2 de ellos en ciberseguridad.
- Se recomienda contar con Security+, CySA+, PenTest+ o conocimientos equivalentes.

Ruta profesional CompTIA

SecAI+ es una certificación de especialización (Expansion Series) que amplía la ruta de ciberseguridad de CompTIA: se apoya en Security+ y en CySA+ o PenTest+ y aporta la seguridad de la inteligencia artificial antes del nivel experto, SecurityX.



Información general

- Material oficial de CompTIA, con laboratorios prácticos y preguntas de práctica.
- Instructor certificado y Savant Consultores como CompTIA Authorized Partner.
- Certificación acreditada por ANAB bajo la norma ISO/IEC 17024.
- Vigencia de 3 años, renovable mediante el programa de Educación Continua (CE) de CompTIA.

CompTIA Authorized Partner | ACADEMIC PARTNER

CompTIA SecAI+ CERTIFICATION Expansion Series