

COMPTIA · PLUS SERIES

VERSIÓN 8

CompTIA Security+ V8

Examen SY0-801

La certificación de ciberseguridad reconocida a nivel mundial que valida las habilidades prácticas para proteger sistemas y datos, y responder a amenazas.

¿Por qué debería asistir?

CompTIA Security+ es la certificación de referencia para iniciar y consolidar una carrera en ciberseguridad. Valida habilidades prácticas y aplicables desde el primer día para proteger sistemas y datos, responder a amenazas y ejecutar las funciones esenciales de seguridad en cualquier organización. La versión 8 (SY0-801) actualiza el programa con Zero Trust, automatización y orquestación, entornos de nube, híbridos y OT, y un objetivo dedicado a los riesgos de seguridad de la inteligencia artificial.

Durante el curso, los participantes aprenden a aplicar controles de seguridad por capas, gestión de accesos y criptografía; a identificar actores de amenaza, técnicas de ataque, vulnerabilidades e indicadores de actividad maliciosa; a proteger infraestructuras locales, híbridas y en la nube con un enfoque de resiliencia y continuidad; a monitorear, gestionar vulnerabilidades y responder a incidentes con registros, alertas y datos de seguridad, y a aplicar políticas, gestión de riesgos, cumplimiento y concienciación. El programa cubre el 100 % de los objetivos del examen SY0-801.

5 días	5	26	Prácticos	Intermedio
DURACIÓN	DOMINIOS OFICIALES	OBJETIVOS	LABORATORIOS	NIVEL



¿Quién debería participar?

Administradores de seguridad
Profesionales que implementan y mantienen controles de seguridad, accesos y monitoreo en la organización.

Administradores de sistemas y redes
Personal de infraestructura que necesita incorporar la seguridad en servidores, redes, nube y endpoints.

Analistas de SOC y mesa de ayuda
Técnicos de soporte y analistas junior que dan el siguiente paso hacia un rol de ciberseguridad.

Responsables de TI y cumplimiento
Coordinadores, auditores y personal de riesgo que necesitan una base técnica sólida en seguridad.

Objetivos de aprendizaje

- Aplicar controles de seguridad por capas, principios de Zero Trust, gestión de accesos y criptografía.
- Identificar actores de amenaza, técnicas de ataque, vulnerabilidades e indicadores de actividad maliciosa, incluidos los riesgos asociados a la IA.
- Proteger entornos en la nube, híbridos, locales y conectados, apoyando la resiliencia y la continuidad del negocio.
- Utilizar monitoreo, gestión de vulnerabilidades, herramientas de seguridad, automatización y prácticas de seguridad operativa.
- Gestionar autenticación, autorización, federación, MFA y controles de acceso seguro.
- Detectar, responder e investigar incidentes usando registros, alertas y datos de seguridad.
- Aplicar políticas de seguridad, gestión de riesgos, cumplimiento, auditoría y programas de concienciación.
- Evaluar el impacto de la gestión de cambios y de los terceros en la postura de seguridad.

Áreas de habilidad

Zero Trust | Criptografía | Amenazas y ataques | Riesgos de IA | Arquitectura en la nube y OT | Protección de datos | Resiliencia y recuperación | Gestión de vulnerabilidades | Monitoreo y alertas | Identidad y accesos | Respuesta a incidentes | Riesgo y cumplimiento

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 generales de seguridad (16 %)** Tipos de controles de seguridad y cómo se complementan entre sí; impacto de la gestión de cambios en la seguridad; soluciones criptográficas: cifrado, certificados, hashing, firmas digitales y gestión de claves.
Dominio 2 Día 2	**2.0 Amenazas, vulnerabilidades y ataques (24 %)** Actores de amenaza y sus motivaciones; vectores de amenaza y superficies de ataque; indicadores de actividad maliciosa; vulnerabilidades comunes y sus riesgos; riesgos de seguridad de los sistemas de IA: modelos, prompts, privacidad y exposición de datos.
Dominio 3 Día 3	**3.0 Arquitectura de seguridad (19 %)** Implicaciones de seguridad de los modelos de arquitectura, incluida la tecnología operativa (OT); principios de seguridad para la infraestructura empresarial; protección de datos durante todo su ciclo de vida; resiliencia y recuperación mediante respaldos, redundancia y pruebas.
Dominio 4 Día 4	**4.0 Operaciones de seguridad (27 %)** Técnicas de seguridad para endpoints, redes, aplicaciones y datos; ciclo de vida de los activos; indicadores de vulnerabilidad y mitigaciones; monitoreo y alertas; identidades y accesos, incluido el acceso privilegiado; automatización y orquestación; respuesta a incidentes y fuentes de datos para investigaciones.
Dominio 5 Día 5	**5.0 Gestión y supervisión del programa de seguridad (14 %)** Elementos de un programa de gobierno eficaz; procesos de gestión de riesgos; riesgos de terceros; requisitos de cumplimiento y privacidad; auditorías y evaluaciones; concienciación en seguridad. ✔ **Repaso integral y preparación para el examen** Repaso por dominio, práctica con preguntas basadas en desempeño (PBQ) y simulacro cronometrado del examen SY0-801.

El contenido sigue los 5 dominios y 26 objetivos oficiales del examen CompTIA Security+ SY0-801 (V8); el porcentaje indica el peso de cada dominio en el examen.

Examen y certificación

Título	CompTIA Security+ – Versión 8
Código	SY0-801
Lanzamiento	17 de noviembre de 2026 (fecha prevista por CompTIA)
Preguntas	Máximo 90
Formato	Opción múltiple y preguntas basadas en desempeño
Duración	90 minutos
Aprobación	750 (escala de 100–900)
Idioma	Inglés
Plataforma	Pearson VUE (centro de pruebas o en línea con OnVUE)

Requisitos de elegibilidad

- No hay requisitos obligatorios. CompTIA recomienda dos años de experiencia práctica como administrador de seguridad.
- Se recomienda contar con conocimientos equivalentes a CompTIA A+ y Network+.
- La versión anterior (SY0-701) sigue disponible hasta su retiro: 11 de junio de 2027 en inglés y 13 de agosto de 2027 en español, japonés, portugués y tailandés.

Ruta profesional CompTIA

Security+ es la certificación central de la ruta de ciberseguridad de CompTIA: consolida la base de soporte y redes, y abre el camino hacia los roles de analista, pentester y arquitecto de seguridad.



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 Security+ CERTIFICATION Plus Series