

COMPTIA · PLUS SERIES

VERSIÓN 1

CompTIA SecOT+ V1

Examen SOT-001

La certificación para proteger y gestionar los sistemas de tecnología operativa (OT) en la manufactura y la infraestructura crítica.

¿Por qué debería asistir?

CompTIA SecOT+ valida las habilidades para asegurar y gestionar sistemas de tecnología operativa (OT) en la manufactura y la infraestructura crítica. Está dirigida a profesionales con experiencia que necesitan dominar la evaluación de riesgos, el cumplimiento, la inteligencia de amenazas, la arquitectura y la respuesta a incidentes en entornos industriales. CompTIA prevé su lanzamiento en diciembre de 2026 y ya está disponible en preventa.

Durante el curso, los participantes aprenden los fundamentos de seguridad física, control y arquitectura propios de OT; a evaluar riesgos, gestionar programas de cumplimiento y alinear la ciberseguridad con los objetivos del negocio; a analizar y responder a amenazas con marcos específicos de OT y lecciones de ataques históricos como Stuxnet; a construir, endurecer y operar arquitecturas OT seguras; a gestionar activos, vulnerabilidades y el monitoreo de seguridad en entornos industriales, y a ejecutar la respuesta a incidentes físicos y ciberfísicos. El programa cubre los 6 dominios del examen SOT-001.

5 días	6	Plus	Prácticos	Avanzado
DURACIÓN	DOMINIOS OFICIALES	SERIE	LABORATORIOS	NIVEL



¿Quién debería participar?

Ingenieros de control y automatización
Profesionales que operan PLC, HMI y sistemas SCADA en plantas e instalaciones.

Especialistas en ciberseguridad OT/ICS
Profesionales que protegen redes y sistemas industriales e infraestructura crítica.

Equipos de TI que convergen con OT
Personal de seguridad de TI que asume responsabilidades sobre entornos industriales.

Responsables de riesgo y continuidad
Profesionales que gestionan el riesgo, el cumplimiento y la continuidad operativa.

Objetivos de aprendizaje

- Aplicar prácticas de seguridad física y comprender la convergencia IT/OT, los PLC, HMI y SCADA.
- Distinguir protocolos OT como Modbus, DNP3, BACnet y Profinet, y las infraestructuras heredadas y modernas.
- Evaluar riesgos, gestionar programas de cumplimiento y alinear la ciberseguridad con el negocio.
- Analizar amenazas OT con marcos como MITRE ATT&CK, el Modelo Diamante y la Cyber Kill Chain.
- Diseñar, endurecer y operar arquitecturas OT seguras con defensa en profundidad.
- Gestionar inventarios de activos, vulnerabilidades, parches y monitoreo en entornos industriales.
- Ejecutar la respuesta a incidentes OT, incluidos los eventos físicos y ciberfísicos.
- Integrar la respuesta física y cibernética con marcos como PICERL e ICS4ICS.

Áreas de habilidad

Seguridad física OT | Convergencia IT/OT | PLC, HMI y SCADA | Protocolos industriales | Gestión de riesgos | Cumplimiento | Inteligencia de amenazas | Arquitectura segura | Segmentación | Gestión de activos | Vulnerabilidades OT | Respuesta a incidentes

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 Fundamentos de sistemas OT y seguridad física** Bloqueo y etiquetado, análisis de riesgos del trabajo y EPP; convergencia IT/OT, PLC, HMI y SCADA; teoría de control; protocolos seriales, Ethernet e inalámbricos; infraestructura heredada, embebida y moderna.
Dominios **2 · 3** Día 2	**2 Gestión de riesgos OT** Gobierno, riesgo y cumplimiento; gestión del programa; evaluación, monitoreo y tratamiento de riesgos; gestión de cambios. **3 Inteligencia de amenazas OT** Marcos (Modelo Diamante, MITRE ATT&CK, Cyber Kill Chain); incidentes históricos como Stuxnet e Industroyer; actores, vectores e IoC.
Dominio 4 Día 3	**4 Arquitectura, diseño e ingeniería de ciberseguridad OT** Principios de arquitectura segura y defensa en profundidad; seguridad física; controles de hardware, hosts y aplicaciones; segmentación, firewalls e IDS/IPS; autenticación, MFA, PKI y acceso remoto seguro.
Dominio 5 Día 4	**5 Operaciones de seguridad OT** Inventario de activos y software y gestión de la configuración; análisis de registros, SIEM y SOAR; priorización y aplicación de parches; validación de vulnerabilidades; seguridad de dispositivos portátiles.
Dominio 6 Día 5	**6 Gestión de incidentes OT** Marcos PICERL e ICS4ICS; respuesta física y cibernética integrada; planes, playbooks y ejercicios; triaje, cadena de custodia y causa raíz; contención, erradicación y recuperación. **✔ Repaso integral y preparación para el examen** Repaso por dominio y preparación para el examen SOT-001.

El contenido sigue los 6 dominios oficiales publicados por CompTIA para el examen SecOT+ SOT-001 (V1). CompTIA aún no publica el peso de cada dominio.

Examen y certificación

Título	CompTIA SecOT+ – Versión 1
Código	SOT-001
Lanzamiento	Diciembre de 2026 (preventa disponible)
Preguntas	Por confirmar (CompTIA aún no lo publica)
Formato	Por confirmar (CompTIA aún no lo publica)
Duración	Por confirmar (CompTIA aún no lo publica)
Aprobación	Por confirmar (CompTIA aún no lo publica)
Idioma	Inglés
Plataforma	Pearson VUE (centro de pruebas o en línea con OnVUE)

Requisitos de elegibilidad

- No hay requisitos obligatorios. CompTIA recomienda al menos 3 años de experiencia práctica en entornos OT y 2 años implementando soluciones de ciberseguridad OT.

Ruta profesional CompTIA

SecOT+ lleva la ciberseguridad a la tecnología operativa: se apoya en los conocimientos de redes y seguridad de Network+ y Security+, y aporta la especialización industrial y de infraestructura crítica 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