CompTIA Security+

Temario

Módulo 1: Conceptos Generales de Seguridad

📌 **Objetivo**: Comprender los principios básicos de seguridad en TI y los diferentes tipos de controles.
📌 **Duración**: 5 horas

1.1 Controles de Seguridad

- Categorías: Técnico, Gerencial, Operacional y Físico.
- Tipos: Preventivo, Disuasivo, Detectivo, Correctivo, Compensatorio, Direccional.

1.2 Fundamentos de Seguridad

- Confidencialidad, Integridad y Disponibilidad (**CIA**).
- No repudio y autenticación (AAA: Authentication, Authorization, Accounting).
- Modelos de autorización y análisis de brechas.
- Arquitectura **Zero Trust**.
- Seguridad física y medidas de control de acceso.

1.3 Gestión de Cambios y Seguridad

- Procesos de aprobación, análisis de impacto y documentación.
- Consideraciones técnicas: Listas blancas, restricciones, reinicios, dependencia de software heredado.

1.4 Criptografía y Seguridad de Datos

- PKI (Infraestructura de Clave Pública), cifrado simétrico y asimétrico.
- Algoritmos, longitudes de clave y hash.
- Técnicas avanzadas: Blockchain, enmascaramiento de datos, tokenización.

Módulo 2: Amenazas, Vulnerabilidades y Mitigaciones

📌 **Objetivo**: Identificar amenazas y vulnerabilidades, y aplicar estrategias de mitigación.
📌 **Duración**: 8 horas

2.1 Actores de Amenazas y Motivaciones

- Tipos: Nation-state, hackers éticos, amenazas internas, crimen organizado.
- Motivaciones: Espionaje, interrupción del servicio, lucro financiero, ideologías.

2.2 Vectores de Ataque y Superficies de Amenaza

- Ingeniería social (phishing, smishing, vishing, typosquatting).
- Explotación de vulnerabilidades en software y hardware.
- Redes inseguras y amenazas en la cadena de suministro.

2.3 Vulnerabilidades Comunes

- Inyección SQL, desbordamiento de búfer, malware, ataques en entornos cloud.
- Errores de configuración y problemas en dispositivos móviles.

2.4 Análisis de Indicadores de Ataques

- Bloqueos de cuentas, uso concurrente de sesiones, viajes imposibles.
- Impacto en los sistemas, tráfico sospechoso.

2.5 Estrategias de Mitigación

- Firewalls, listas de control de acceso (ACL), segmentación de redes.
- Implementación de parches, cifrado, endurecimiento de sistemas.

Módulo 3: Arquitectura de Seguridad

📌 **Objetivo**: Comprender la seguridad en infraestructuras de TI y aplicar principios de diseño seguro.

📌 **Duración**: 7 horas

3.1 Modelos de Arquitectura Segura

- Seguridad en la nube, microservicios, redes definidas por software (**SDN**).
- Segmentación lógica y física, contenedorización, virtualización.
- Sistemas embebidos y seguridad en IoT.

3.2 Protección de Infraestructura Empresarial

- Colocación de dispositivos, conectividad segura.
- Tipos de firewalls y sistemas de detección de intrusos (IDS/IPS).
- Implementación de VPNs y acceso remoto seguro.

3.3 Protección de Datos

- Clasificación de datos: Sensibles, confidenciales, públicos.
- Métodos de protección: Cifrado, hashing, enmascaramiento, tokenización.

3.4 Resiliencia y Recuperación

- Balanceo de carga vs. clustering.
- Copias de seguridad, recuperación ante desastres, redundancia geográfica.

Módulo 4: Operaciones de Seguridad

📌 **Objetivo**: Aplicar estrategias de seguridad en la gestión de infraestructura y respuesta a incidentes.

📌 **Duración**: 12 horas

4.1 Hardening y Seguridad de Infraestructura

- Configuración segura de dispositivos: IoT, servidores, redes inalámbricas.
- Seguridad en software: Validación de entrada, análisis estático y dinámico.

4.2 Gestión de Activos y Seguridad

- Control de hardware/software, eliminación segura de datos.
- Clasificación y monitoreo de activos.

4.3 Administración de Vulnerabilidades

- Métodos de identificación: Escaneos, pruebas de penetración.
- Evaluación de riesgos y remediación.

4.4 Monitoreo y Alertas de Seguridad

- Herramientas: SIEM, antivirus, NetFlow, escáneres de vulnerabilidades.

4.5 Gestión de Identidad y Acceso

- Autenticación multifactor (**MFA**), SSO, federación de identidades.
- Implementación de políticas de acceso y administración de contraseñas.

4.6 Automatización y Respuesta a Incidentes

- Implementación de seguridad automatizada.
- Procesos de respuesta a incidentes y análisis forense digital.

Módulo 5: Administración y Supervisión de Seguridad

📌 **Objetivo**: Comprender la gobernanza, cumplimiento y gestión de riesgos en ciberseguridad.

📌 **Duración**: 8 horas

5.1 Gobernanza en Seguridad

- Políticas de seguridad, estándares y cumplimiento normativo.
- Modelos de gobernanza y roles en seguridad.

5.2 Gestión de Riesgos

- Evaluación de riesgos, análisis cuantitativo y cualitativo.

- Estrategias: Transferencia, mitigación, aceptación.

5.3 Evaluación de Riesgos de Terceros

- Evaluación de proveedores, acuerdos de nivel de servicio (**SLA**).

5.4 Cumplimiento y Auditorías

- Requerimientos regulatorios, impactos de incumplimiento.
- Auditorías de seguridad y pruebas de penetración.

5.5 Concientización y Cultura de Seguridad

- Capacitación en seguridad, reconocimiento de amenazas.
- Políticas de uso de dispositivos y concienciación sobre ingeniería social.

Módulo 6: Simulaciones y Preparación para el Examen

📌 **Objetivo**: Preparar a los participantes para rendir el examen **CompTIA Security+ SY0-701**.
📌 **Duración**: 5 horas

- Simulación de examen con preguntas de opción múltiple.
- Estrategias para abordar preguntas del examen.
- Revisión y análisis de respuestas.