Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 1

Mastering Security Basics — Fundamentos de Seguridad

Este material es un **resumen conceptual elaborado con palabras propias**, pensado como guía de apoyo para estudiar junto al libro original en inglés *CompTIA Security+: Get Certified Get Ahead — SY0-701 Study Guide* (Joe Shelley & Darril Gibson). No es una traducción ni una reproducción del texto original; cubre los mismos temas, organizados en el mismo orden, para facilitar el repaso en español.

Incluye: resumen por secciones, glosario de términos clave (inglés ↔ español) y preguntas de práctica para autoevaluación.

1. Metas Fundamentales de Seguridad: la Tríada CIA

Toda la seguridad de la información gira en torno a tres objetivos centrales, conocidos como la **Tríada CIA** (Confidentiality, Integrity, Availability). Cualquier amenaza, ataque o control de seguridad que estudies a lo largo del temario se puede relacionar con al menos uno de estos tres pilares.

Confidencialidad (Confidentiality)

Evita la divulgación no autorizada de información: que solo las personas autorizadas puedan ver un dato. Se logra principalmente con dos mecanismos:

- **Cifrado (encryption):** transforma los datos en algo ilegible para quien no tenga la clave de descifrado. Es la herramienta más efectiva para proteger la confidencialidad, tanto de datos en tránsito (por ejemplo, un correo) como de datos almacenados.
- **Controles de acceso (access controls):** se basan en tres pasos — *identificación* (quién dices ser, ej. usuario), *autenticación* (demostrás que sos quien decís, ej. contraseña) y *autorización* (qué se te permite hacer una vez autenticado, ej. permisos).

Integridad (Integrity)

Garantiza que los datos no hayan sido alterados de forma no autorizada o accidental (por errores humanos, fallas de sistema o malware). La herramienta clave es el **hashing**: un algoritmo que genera una cadena de longitud fija a partir de un archivo o mensaje. Si el dato no cambia, el hash tampoco cambia. Comparando el hash original con uno calculado después, se puede detectar si hubo alguna modificación (aunque el hash no dice *qué* cambió, solo que algo cambió).

Disponibilidad (Availability)

Asegura que los sistemas y datos estén accesibles para los usuarios autorizados cuando los necesitan. Se logra principalmente mediante:

- **Redundancia y tolerancia a fallos:** eliminar puntos únicos de falla (SPOF). Ejemplos: RAID (discos redundantes), clústeres de failover (servidores redundantes), balanceo de carga y NIC teaming (red), UPS y generadores (energía).
- **Escalabilidad (scalability):** aumentar manualmente la capacidad. Escalado *vertical* = agregar más recursos a un servidor (más RAM/CPU). Escalado *horizontal* = agregar más servidores.
- **Elasticidad (elasticity):** el sistema agrega o quita recursos automáticamente según la demanda (muy típico en la nube).
- **Resiliencia (resiliency):** capacidad del sistema de recuperarse solo ante fallas, con el menor tiempo de inactividad posible (reintentos automáticos, backups probados, etc.).
- **Parchado (patching):** mantener el software actualizado para evitar errores y vulnerabilidades que afecten la disponibilidad.

Importante: aplicar seguridad siempre tiene un costo (recursos, dinero, rendimiento). Por ejemplo, cifrar todos los datos puede aumentar su tamaño hasta un 60%. Las organizaciones deben equilibrar el nivel de seguridad deseado contra el costo real que implica.

2. Conceptos Básicos de Riesgo

- **Riesgo (risk):** la probabilidad de que una amenaza explote una vulnerabilidad y provoque una pérdida.
- **Amenaza (threat):** cualquier circunstancia o evento con potencial de comprometer la confidencialidad, integridad o disponibilidad. Puede ser interna (empleado descontento) o externa, natural (huracán) o humana, intencional o accidental.
- **Vulnerabilidad (vulnerability):** una debilidad — en el hardware, software, configuración o incluso en los propios usuarios.
- **Mitigación de riesgo (risk mitigation):** reducir la probabilidad de que una amenaza explote una vulnerabilidad, o reducir el impacto si esto ocurre, mediante controles (también llamados contramedidas o salvaguardas).

3. Selección de Controles de Seguridad

CompTIA clasifica los controles de seguridad de dos maneras distintas y complementarias: por **categoría** (cómo funciona el control) y por **tipo** (qué objetivo persigue). Un mismo control puede tener una categoría y un tipo a la vez — por ejemplo, un firewall es un control técnico (categoría) y preventivo (tipo).

3.1 Categorías de control (cómo funcionan)

Categoría	Qué es	Ejemplos
Técnico (Technical)	Usa tecnología (hardware, software, firmware).	Cifrado, antivirus, IDS/IPS, firewalls, mínimo privilegio.
Gerencial (Managerial)	Administrativo, documentado en políticas de seguridad.	Evaluaciones de riesgo, evaluaciones de vulnerabilidades.
Operacional (Operational)	Lo ejecutan las personas en el día a día.	Capacitación, gestión de configuración, protección de medios.
Física (Physical)	Se puede tocar físicamente.	Cercas, guardias, cerraduras, iluminación, mantraps.

3.2 Tipos de control (qué objetivo persiguen)

Tipo	Objetivo	Ejemplos
Preventivo	Evitar que ocurra un incidente.	Hardening, capacitación, guardias, deshabilitar cuentas.
Disuasivo (Deterrent)	Desalentar a un posible atacante.	Carteles de advertencia, banners de inicio de sesión.

Detectivo	Detectar el incidente después de ocurrido.	Monitoreo de logs, SIEM, auditorías, cámaras, IDS.
Correctivo	Revertir el impacto tras el incidente.	Backups y recuperación, manejo de incidentes.
Compensatorio	Alternativa cuando el control principal no es viable.	Usar TOTP mientras se entrega una tarjeta inteligente.
Directivo	Dar instrucciones sobre cómo actuar.	Políticas, estándares, procedimientos, gestión de cambios.

Truco para el examen: pensá primero en la *categoría* (¿es tecnología, papeleo, gente o algo físico?) y después en el *tipo* (¿previene, detecta, corrige, disuade, compensa o dirige?). Muchas preguntas combinan ambos, por ejemplo: 'control técnico preventivo'.

4. Registro de Logs y Monitoreo de Seguridad

El monitoreo continuo es clave para detectar incidentes. El examen espera que sepas interpretar logs y entender cómo se centraliza esa información.

4.1 Fuentes de logs

- **Logs de Windows:** Security (eventos de éxito/fallo, auditoría), System (funcionamiento del SO), Application (eventos generados por programas). Se ven con el Visor de Eventos.
- **Logs de Linux:** se guardan en `/var/log/`. Destacan `syslog`/`messages` (eventos generales del sistema) y `secure` (autenticación y autorización, ej. intentos fallidos de SSH).
- **Logs de red:** firewalls (tráfico permitido/bloqueado), IDS/IPS (posibles intrusiones), capturas de paquetes con herramientas como Wireshark.
- **Logs de aplicaciones:** por ejemplo, logs de servidores web en formato estándar W3C (host, usuario, fecha, request, código de estado, bytes).
- **Metadatos (metadata):** información sobre los datos — por ejemplo, la ruta de un correo o la ubicación GPS y el modelo de cámara de una foto. Muy útil en investigaciones forenses.

4.2 SIEM (Security Information and Event Management)

Un SIEM centraliza la recolección, análisis y gestión de logs provenientes de sistemas, aplicaciones e infraestructura de red. Combina dos funciones: **SEM** (monitoreo y alertas en tiempo real) y **SIM** (almacenamiento a largo plazo y análisis de tendencias para cumplimiento normativo). Sus componentes típicos son:

- **Agregación de logs:** unifica el formato de logs que llegan de fuentes distintas.
- **Motor de correlación:** busca patrones y relaciones entre eventos para generar alertas.
- **Disparadores (triggers):** generan una acción automática al superar un umbral (ej. bloquear IP tras 5 intentos fallidos de login).
- **Ajuste de alertas (alert tuning):** calibrar la sensibilidad para minimizar falsos positivos (alarmas sin motivo real) y falsos negativos (ataques reales que no generan alarma).
- **Sincronización horaria (NTP):** esencial para que los logs de distintos servidores puedan compararse correctamente durante una investigación.
- **Archivado:** mover logs antiguos a almacenamiento más económico, sin perder la posibilidad de restaurarlos si se necesitan.
- **Dashboards:** paneles visuales con alertas, tendencias y correlaciones en tiempo real.
- **Análisis de comportamiento de usuario (UBA):** detecta patrones anómalos de actividad que podrían indicar intención maliciosa.

Syslog es el protocolo estándar que define el formato de los mensajes de log y cómo se transportan hacia un servidor centralizado (llamado *collector*). La mayoría de los SIEM usan este formato internamente.

5. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
CIA Triad	Tríada CIA	Confidencialidad, Integridad y Disponibilidad — los 3 pilares de la seguridad.
Confidentiality	Confidencialidad	Solo usuarios autorizados pueden ver la información.
Integrity	Integridad	Los datos no han sido alterados sin autorización.
Availability	Disponibilidad	Los sistemas/datos están accesibles cuando se necesitan.
Encryption	Cifrado	Transformar datos en formato ilegible sin la clave correcta.
Hashing	Hashing / función hash	Genera una huella digital fija para verificar integridad.
Identification	Identificación	Afirmar una identidad (ej. usuario).
Authentication	Autenticación	Probar que sos quien decís ser (ej. contraseña).
Authorization	Autorización	Definir qué se te permite hacer una vez autenticado.
Risk	Riesgo	Probabilidad de que una amenaza explote una vulnerabilidad.
Threat	Amenaza	Evento o circunstancia con potencial de causar daño.
Vulnerability	Vulnerabilidad	Una debilidad explotable en un sistema.
Risk mitigation	Mitigación de riesgo	Reducir la probabilidad o el impacto de un riesgo.
Security control	Control de seguridad	Medida (contramedida/salvaguarda) para reducir el riesgo.
Redundancy	Redundancia	Duplicación de componentes críticos.
Fault tolerance	Tolerancia a fallos	Capacidad de seguir operando ante una falla.
Single point of failure (SPOF)	Punto único de falla	Elemento cuya caída provoca la caída de todo el sistema.
Scalability	Escalabilidad	Capacidad de aumentar recursos manualmente.
Elasticity	Elasticidad	Ajuste automático de recursos según demanda.
Resiliency	Resiliencia	Capacidad de recuperarse solo ante fallas.
Least privilege	Mínimo privilegio	Otorgar solo los permisos estrictamente necesarios.
Hardening	Endurecimiento (hardening)	Reforzar la configuración por defecto de un sistema.

Inglés	Español	Definición breve
SIEM	SIEM	Sistema centralizado de gestión de eventos e información de seguridad.
Log aggregation	Agregación de logs	Unificar logs de distintas fuentes en un formato común.
Correlation engine	Motor de correlación	Detecta patrones entre eventos de log para generar alertas.
False positive / negative	Falso positivo / negativo	Alerta sin amenaza real / ausencia de alerta ante amenaza real.

6. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 1. Las respuestas están al final.

1. Un administrador cifra todos los correos que contienen información de tarjetas de crédito antes de enviarlos. ¿Qué meta de la Tríada CIA está protegiendo principalmente?

2. Una empresa calcula el hash de un archivo antes y después de transferirlo, y los compara. ¿Qué meta de seguridad está verificando?

3. Un sitio web usa múltiples servidores con balanceo de carga para evitar caídas ante picos de tráfico. ¿Qué concepto describe mejor esta estrategia?

4. Una organización en la nube agrega automáticamente servidores durante el Black Friday y los retira cuando baja la demanda. ¿Cómo se llama esta capacidad?

5. Un guardia de seguridad revisa las credenciales antes de dejar entrar a alguien a la sala de servidores. ¿Es un control físico, técnico, gerencial u operacional? ¿Y qué tipo de control es (preventivo, detectivo, etc.)?

6. Un cartel en la entrada de un edificio dice 'Área vigilada por cámaras 24/7'. ¿Qué tipo de control es?

7. Después de un ataque de ransomware, la empresa restaura los archivos desde una copia de seguridad. ¿Qué tipo de control se está aplicando?

8. Un SIEM genera una alerta automática al detectar 50 intentos fallidos de login en 2 minutos. ¿Qué componente del SIEM hizo posible detectar ese patrón?

9. Homer ingresa mal su contraseña una sola vez y el SIEM dispara una alerta de ataque. ¿Cómo se llama este error de configuración?

10. ¿Qué protocolo se usa comúnmente para sincronizar la hora entre todos los servidores que envían logs a un SIEM?

Respuestas

1. Confidencialidad — el cifrado protege que solo el destinatario autorizado pueda leer la información.

2. Integridad — el hashing detecta si los datos cambiaron durante la transferencia.

3. Redundancia / tolerancia a fallos (específicamente, redundancia de red mediante balanceo de carga).

4. Elasticidad — el ajuste automático de recursos según la demanda.

5. Es un control físico (categoría) y preventivo (tipo) — también podría considerarse disuasivo.

6. Control disuasivo (deterrent) — busca desalentar a un intruso antes de que actúe.

7. Control correctivo — revierte el impacto del incidente restaurando los datos.

8. El motor de correlación (correlation engine), que analiza eventos de log en busca de patrones.

9. Falso positivo — se generó una alerta sin que hubiera una amenaza real.

10. NTP (Network Time Protocol).
