Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 9

Implementing Controls to Protect Assets — Controles para Proteger Activos

---

Este material es un **resumen conceptual elaborado con palabras propias**, pensado como guía de apoyo para estudiar junto al libro original en inglés. No es una traducción ni una reproducción del texto original; sigue la misma estructura y orden de secciones del libro, incluyendo recuadros equivalentes a los 'Remember This!' originales, para facilitar el repaso en español.

Incluye: resumen por secciones, tablas comparativas, glosario EN↔ES y preguntas de práctica originales.

1. Comparando Controles de Seguridad Física

Un control físico es algo que se puede tocar (cerraduras, cercas, cámaras). Las organizaciones aplican controles en distintos límites: perímetro, edificios, áreas de trabajo seguras, salas de servidores y hardware individual. El **camuflaje industrial** (ej. usar vegetación para ocultar una cerca de seguridad) también es una técnica física.

1.1 Credenciales de acceso (badges)

Las **tarjetas de proximidad** se activan al acercarse a un lector, sin necesitar fuente de energía propia (usan un capacitor y una bobina que recibe carga del lector). Combinarlas con un PIN aporta autenticación multifactor (algo que tenés + algo que sabés).

■ Recordá esto!

Las tarjetas de proximidad son del tamaño de una tarjeta de crédito. El usuario la pasa cerca de un lector, que lee sus datos. Algunos puntos de acceso combinan tarjetas de proximidad con PIN para autenticación.

1.2 Personal de seguridad y videovigilancia

Los guardias pueden verificar credenciales, disuadir el tailgating y mantener registros de visitantes. Un sistema **CCTV** ofrece prueba confiable de la ubicación y actividad de una persona (a diferencia de un log digital, que puede ser burlado si alguien usa la tarjeta de otro). También puede usarse como **control compensatorio** mientras se implementa un sistema más robusto.

■ Recordá esto!

La videovigilancia da prueba confiable de la identidad y actividad de una persona. Muchas cámaras incluyen detección de movimiento y de objetos. Un sistema CCTV puede usarse como control compensatorio.

1.3 Sensores

Tipo	Detecta
Movimiento	Cambios de posición; se combina con luces e iluminación automática.
Ruido	Nivel de sonido o sonidos específicos (ej. vidrio rompiéndose).
Infrarrojo	Firmas de calor, útil incluso en oscuridad total.
Presión	Cambios de presión en pisos, puertas o ventanas.
Microondas	Movimiento mediante señales de microondas reflejadas.
Ultrasónico	Ondas sonoras de alta frecuencia; también mide distancia.

1.4 Cercas, iluminación, alarmas y barricadas

- **Cercas:** delimitan el perímetro; el acceso se controla en portones específicos.

- **Iluminación:** disuade a atacantes; se combina con sensores de movimiento para ahorrar energía sin sacrificar seguridad.
- **Alarmas:** de incendio (humo/calor) o antirrobo (puertas/ventanas/movimiento).
- **Bollards:** postes cortos de concreto/acero que bloquean vehículos sin impedir el paso de personas — protegen entradas de intentos de embestida.
- **Vestíbulo de control de acceso (mantrap):** dos puertas enclavadas que permiten el paso de una sola persona a la vez, previniendo el tailgating.

2. Gestión de Activos (Asset Management)

Rastrea activos de hardware, software y datos a lo largo de su ciclo de vida. Actividades clave:

- **Adquisición/procuración:** procedimientos para identificar la necesidad de nuevos activos y evaluarlos.
- **Asignación/contabilidad:** asignar cada activo a un dueño responsable y clasificarlo según sensibilidad y criticidad.
- **Monitoreo y rastreo de activos:** mantener un inventario actualizado, con enumeración periódica (auditorías) del inventario.

Una buena gestión de activos reduce el **system sprawl** (más sistemas de los necesarios, subutilizados) y ayuda a evitar activos no documentados. El seguimiento con **RFID** es común para hardware y dispositivos móviles.

3. Diversidad de Plataforma

La **defensa en profundidad** (seguridad por capas) implementa múltiples niveles de protección para que, si falla una capa, otras sigan protegiendo.

- **Diversidad de proveedores:** usar controles de distintos fabricantes (ej. dos firewalls de marcas distintas en una DMZ), para que una vulnerabilidad en uno no comprometa ambos a la vez.
- **Diversidad tecnológica:** usar tecnologías distintas para proteger un mismo entorno (ej. cerraduras biométricas + CCTV).
- **Diversidad de controles:** combinar controles técnicos, físicos, gerenciales y operacionales.

3.1 Ataques físicos

- **Card skimming / cloning:** capturar datos de la banda magnética de una tarjeta y clonarla; los chips (a diferencia de la banda) cifran los datos y son mucho más difíciles de clonar.
- **Fuerza bruta física (brute force):** intentar atravesar controles físicos directamente (ej. embestir una puerta con un vehículo, o probar todos los códigos de un teclado numérico).
- **Ataques ambientales:** interrumpir energía, alterar temperatura/humedad, o inundar instalaciones para dañar equipos.

4. Redundancia y Tolerancia a Fallos

Un **punto único de falla (SPOF)** es cualquier componente cuya falla provoca la caída de todo el sistema — puede ser hardware o incluso una persona (si solo ella sabe hacer una tarea crítica).

■ Recordá esto!

Un punto único de falla es cualquier componente cuya falla causa la falla de todo el sistema. RAID, balanceo de carga, UPS y generadores eliminan muchos puntos únicos de falla. Si solo una persona sabe realizar una tarea, esa persona puede ser un punto único de falla.

4.1 Redundancia de disco (RAID)

Nivel	Discos mínimos	Tolerancia a fallos
RAID-0 (striping)	2	Ninguna — solo mejora rendimiento.
RAID-1 (mirroring)	2	Sobrevive la falla de 1 disco.
RAID-5	3	Sobrevive la falla de 1 disco (usa paridad).
RAID-6	4	Sobrevive la falla de 2 discos (doble paridad).
RAID-10 (1+0)	4	Combina mirroring y striping; alta tolerancia y rendimiento.

4.2 Alta disponibilidad y balanceo de carga

Alta disponibilidad: el sistema permanece operativo con downtime casi nulo (ej. 'cinco nueves' = 99,999% = menos de 6 minutos de caída al año).

- **Balanceo activo/activo:** todos los servidores procesan solicitudes simultáneamente (clustering); mejora escalabilidad y disponibilidad.
- **Balanceo activo/pasivo:** un nodo activo y otro en espera (heartbeat entre ambos); si el activo falla, el pasivo toma el control.
- **Round-robin vs. afinidad de IP de origen:** round-robin reparte solicitudes en orden secuencial; la afinidad de IP mantiene al mismo cliente conectado al mismo servidor durante toda la sesión (session persistence).
- **NIC teaming:** agrupa varias tarjetas de red físicas en una sola virtual, sumando rendimiento y eliminando la NIC como punto único de falla.

4.3 Redundancia de energía

- **UPS:** energía de corto plazo, protege contra fluctuaciones y da tiempo para apagar de forma ordenada.
- **Fuente redundante (dual supply):** segunda fuente de poder, normalmente hot-swappable.
- **Generadores:** energía de largo plazo durante cortes extendidos.

- **PDU gestionados:** monitorean voltaje, corriente y consumo en los racks, reportando a una consola central.

5. Protegiendo Datos con Backups

La redundancia (ej. RAID) no reemplaza a los backups — si un incendio destruye el servidor, destruye también el RAID. Solo un backup separado protege contra ese escenario.

5.1 Medios y ubicación

- **Cinta, disco, NAS (nivel de archivo), SAN (nivel de bloque), nube.**
- **Offline (local) vs. online (nube):** offline da control y rapidez; online sobrevive a un desastre que destruya el sitio primario y suele cifrar automáticamente.

5.2 Tipos de backup

Tipo	Respalda	Tiempo de backup / restauración
Completo (full)	Todos los datos seleccionados.	Backup lento / restauración rápida (1 backup).
Diferencial	Todo lo cambiado desde el último backup completo.	Backup crece cada día / restauración necesita 2 backups (completo + último diferencial).
Incremental	Todo lo cambiado desde el último backup (completo o incremental).	Backup rápido y de tamaño estable / restauración necesita el completo + TODOS los incrementales en orden.
Snapshot / imagen	Estado de los datos en un momento específico.	Común en VMs; permite revertir cambios.

■ Recordá esto!

Con tiempo y dinero ilimitados, un backup completo diario da la recuperación más rápida. La estrategia completo/incremental minimiza el tiempo de backup diario. La estrategia completo/diferencial minimiza el tiempo de restauración.

Replicación: copia exacta de datos en tiempo real (o casi) hacia un sitio secundario. **Journaling:** registra cambios secuencialmente en un log separado, permitiendo recuperar el estado más reciente aplicando esos cambios sobre un backup anterior — clave en bases de datos.

5.3 Pruebas de backup y consideraciones geográficas

La única forma de validar un backup es hacer una **restauración de prueba**. Tanto si funciona como si falla, el resultado es valioso: revela si el proceso funciona o si hay un problema por corregir antes de una crisis real.

- **Sitio (offsite vs. onsite):** al menos una copia debe guardarse fuera del sitio principal, a una distancia adecuada (ni tan cerca que un desastre afecte ambas, ni tan lejos que dificulte la recuperación).

- **Soberanía de datos (data sovereignty):** si los backups se almacenan en otro país (ej. en la nube), quedan sujetos a las leyes de ese país.
- **Cifrado:** los backups deben cifrarse para proteger su confidencialidad si el medio físico se pierde o es robado.

6. Elementos de Continuidad de Negocio

El **plan de continuidad de negocio (BCP)** ayuda a predecir y planificar ante interrupciones de servicios críticos, incluyendo un **plan de recuperación ante desastres (DRP)**.

6.1 Análisis de impacto al negocio (BIA)

Identifica **funciones esenciales de la misión** y los **sistemas críticos** que las soportan, así como los **procesos de negocio vulnerables**. No recomienda soluciones, pero informa a la dirección para priorizar recursos. Evalúa impacto en vidas, propiedad, seguridad, finanzas y reputación.

■ Recordá esto!

El BIA identifica funciones esenciales de la misión y sistemas críticos, tiempos máximos de inactividad, escenarios que podrían afectarlos, y las pérdidas potenciales de un incidente.

6.2 RTO, RPO, MTBF y MTTR

Métrica	Qué mide
RTO (Recovery Time Objective)	Tiempo máximo aceptable para restaurar un sistema tras una interrupción.
RPO (Recovery Point Objective)	Cuánta pérdida de datos es aceptable (define la frecuencia mínima de backup).
MTBF (Mean Time Between Failures)	Tiempo promedio entre fallas; mide confiabilidad (más alto = mejor).
MTTR (Mean Time to Repair)	Tiempo promedio para restaurar un sistema tras una falla.

6.3 Sitios de recuperación

Tipo	Características
Sitio caliente (hot)	Operativo 24/7, con datos actualizados; toma el control casi de inmediato. El más caro, el más rápido.
Sitio frío (cold)	Solo energía y conectividad básica; hay que llevar todo el equipo. El más barato, el más lento y difícil de probar.
Sitio tibio (warm)	Compromiso entre caliente y frío — hardware presente, pero datos no siempre actualizados.

Al planificar la ubicación de los sitios de recuperación, hay que considerar la **dispersión geográfica** para que el mismo desastre no afecte a ambos sitios. En la restauración post-desastre, se recomienda volver primero las funciones *menos* críticas al sitio principal, para detectar problemas ocultos sin afectar las funciones esenciales.

6.4 Pruebas del plan

Tipo de prueba	Cómo funciona
Tabletop exercise	Basada en discusión; un coordinador presenta un escenario y los participantes explican cómo responderían.
Simulación	Ejercicio funcional en un entorno simulado, sin afectar el sistema real.
Procesamiento paralelo	Activa el sitio de recuperación y lo corre en paralelo con el principal para confirmar que funciona.
Fail over test	Apaga el sitio principal por completo para verificar que el de recuperación asume la carga (la prueba más completa y disruptiva).

6.5 Planificación de capacidad

Evalúa los recursos necesarios para sostener el crecimiento en tres áreas: **personas** (dotación y habilidades necesarias), **tecnología** (cómputo, almacenamiento, ancho de banda) e **infraestructura** (espacio físico, energía, refrigeración).

7. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
Access control vestibule (mantrap)	Vestíbulo de control de acceso	Dos puertas enclavadas que permiten el paso de una persona a la vez.
Bollards	Bollards / postes de seguridad	Barreras que bloquean vehículos sin impedir el paso peatonal.
CCTV	Circuito cerrado de televisión	Sistema de videovigilancia.
Asset management	Gestión de activos	Rastreo de hardware, software y datos durante su ciclo de vida.
Single point of failure (SPOF)	Punto único de falla	Componente cuya falla provoca la caída de todo el sistema.
RAID	RAID	Conjunto redundante de discos económicos, para tolerancia a fallos.
Load balancing	Balanceo de carga	Distribuye el procesamiento entre varios servidores.
Active/active - active/passive	Activo/activo - activo/pasivo	Configuraciones de balanceo de carga y redundancia.
NIC teaming	Agrupación de NICs	Combina varias tarjetas de red en una virtual.
UPS	SAI (sistema de alimentación ininterrumpida)	Energía de respaldo de corto plazo.
Full / differential / incremental backup	Backup completo / diferencial / incremental	Estrategias de respaldo de datos.
Replication / journaling	Replicación / journaling	Copia en tiempo real / registro secuencial de cambios.
Data sovereignty	Soberanía de datos	Sujeción de los datos a las leyes del país donde se almacenan.
Business Impact Analysis (BIA)	Análisis de impacto al negocio	Identifica funciones esenciales y sistemas críticos.
RTO / RPO	RTO / RPO	Tiempo máximo de inactividad / pérdida de datos aceptable.

Inglés	Español	Definición breve
MTBF / MTTR	MTBF / MTTR	Tiempo medio entre fallas / tiempo medio de reparación.
Hot / cold / warm site	Sitio caliente / frío / tibio	Tipos de sitios de recuperación ante desastres.
Disaster Recovery Plan (DRP)	Plan de recuperación ante desastres	Pasos para recuperar sistemas críticos tras un desastre.
Tabletop exercise	Ejercicio de mesa (tabletop)	Prueba de plan basada en discusión.
Failover test	Prueba de conmutación por error	Apaga el sitio principal para probar el de respaldo.

8. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 9. Las respuestas están al final.

1. Una empresa necesita tolerancia a la falla de hasta dos discos simultáneos en un servidor crítico. ¿Qué nivel de RAID es el mínimo adecuado?

2. Un centro de datos requiere que solo una persona pueda entrar a la vez, verificada por biometría, para prevenir el tailgating. ¿Qué control físico es?

3. Una empresa realiza un backup completo los domingos y backups incrementales el resto de los días. El sistema falla un jueves por la mañana. ¿Cuántos backups distintos se necesitan para restaurar?

4. La misma empresa, pero usando backups diferenciales en vez de incrementales. ¿Cuántos backups se necesitan para restaurar el jueves?

5. Un análisis determina que un sitio de e-commerce no puede estar caído más de 3 horas sin pérdidas inaceptables. ¿Qué métrica describe ese límite de 3 horas?

6. La misma empresa decide que puede tolerar perder como máximo 15 minutos de transacciones en caso de falla. ¿Qué métrica es?

7. Una organización mantiene un sitio con hardware ya instalado, pero sin datos actualizados, como compromiso entre costo y velocidad de recuperación. ¿Qué tipo de sitio es?

8. Un coordinador reúne a los líderes de departamento en una sala de conferencias y les presenta un escenario de ciberataque, pidiéndoles que describan cómo responderían. ¿Qué tipo de prueba es?

9. Una organización utiliza dos firewalls de distintos fabricantes en su subred filtrada para reducir el riesgo de que una misma vulnerabilidad afecte a ambos. ¿Qué principio de seguridad en capas es este?

10. Un backup se almacena en un proveedor de nube que tiene servidores en otro país. ¿Qué concepto legal describe la sujeción de esos datos a las leyes de ese país?

Respuestas

1. RAID-6 (o RAID-10, aunque RAID-6 es el mínimo pensado específicamente para 2 discos con solo 4 discos).

2. Un vestíbulo de control de acceso (access control vestibule / mantrap).

3. 4 backups: el completo del domingo más los 3 incrementales (lunes, martes, miércoles), en orden cronológico.

4. 2 backups: el completo del domingo más el último diferencial (el del miércoles, que ya incluye todos los cambios desde el domingo).

5. RTO (Recovery Time Objective) — tiempo máximo aceptable de inactividad.

6. RPO (Recovery Point Objective) — cantidad de datos que se puede permitir perder.

7. Un sitio tibio (warm site).

8. Un ejercicio de mesa (tabletop exercise) — basado en discusión, no en acción real.

9. Diversidad de proveedores (vendor diversity).

10. Soberanía de datos (data sovereignty).
