Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 5

Securing Hosts and Data — Asegurando Hosts y Datos

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; cubre los mismos temas, en el mismo orden, para facilitar el repaso en español.

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

1. Virtualización

- **Hipervisor:** software que crea, ejecuta y administra máquinas virtuales (VMs). **Host:** el sistema físico que aloja las VMs. **Guest:** el sistema operativo que corre dentro de la VM.
- **Escalabilidad (scalability):** proceso manual de asignar más recursos a una VM (suele requerir reinicio). **Elasticidad (elasticity):** ajuste automático de recursos según la carga, sin reinicio.
- **Thin client / VDI:** un thin client se conecta a un servidor para ejecutar un escritorio o apps. La infraestructura de escritorio virtual (VDI) aloja el sistema operativo de escritorio del usuario en un servidor, accesible incluso desde móviles.
- **Contenedores:** virtualización que ejecuta apps aisladas compartiendo el kernel del sistema operativo del host (más eficiente que un hipervisor tradicional, pero todos los contenedores deben usar el mismo SO que el host).

VM escape: ataque donde el atacante logra salir de la máquina virtual y acceder al host — la mejor protección es mantener parchados tanto el host como los guests. **VM sprawl:** ocurre cuando hay demasiadas VMs sin gestión adecuada (sin parches, consumiendo recursos innecesarios). **Resource reuse:** riesgo de que datos queden en la infraestructura compartida de la nube después de que un cliente termine de usarla.

Replicación: copiar los archivos de una VM a otro servidor físico como respaldo (restauración en minutos). **Snapshot:** captura del estado de una VM en un momento dado; permite revertir cambios si algo sale mal (ej. antes de aplicar un parche riesgoso).

2. Implementación de Sistemas Seguros

2.1 Seguridad de endpoints

- **Antivirus:** control básico que detecta virus, gusanos, troyanos y otro código malicioso.
- **EDR (Endpoint Detection and Response):** detecta y responde a amenazas en el endpoint usando análisis de comportamiento.
- **XDR (Extended Detection and Response):** extiende el concepto de EDR a más tipos de dispositivos (red, nube, IoT), dando una visión más completa.
- **HIPS (Host Intrusion Prevention System):** aplica prevención de intrusiones a un solo host, usando análisis de comportamiento, monitoreo de integridad de archivos y control de aplicaciones.

2.2 Hardening y gestión de configuración

El **hardening** consiste en asegurar un sistema más allá de su instalación por defecto: deshabilitar servicios y puertos innecesarios, desinstalar software que no se usa, cambiar contraseñas por defecto y aplicar cifrado de disco. La **gestión de configuración** ayuda a desplegar sistemas con configuraciones seguras y a mantenerlas en el tiempo.

Línea base segura (secure baseline): se trabaja en 3 pasos — *establecer* la configuración inicial, *desplegarla* en los sistemas, y *mantenerla* actualizada conforme cambian las necesidades y el panorama de seguridad.

Imágenes maestras (master images): se crea un sistema base, se configura y endurece, se prueba exhaustivamente, y luego se captura como imagen para desplegarla en múltiples equipos. Beneficios: punto de partida seguro y reducción del costo total de propiedad (TCO).

2.3 Gestión de parches y de cambios

La **gestión de parches (patch management)** asegura que sistemas, aplicaciones y firmware estén actualizados: identificar, descargar, probar (en un sandbox), desplegar y verificar los parches. La **gestión de cambios (change management)** exige aprobación y documentación antes de modificar cualquier sistema, para evitar interrupciones no intencionales — casi todos los desastres autoinfligidos en redes vienen de cambios hechos sin este proceso.

- **Lista de aplicaciones permitidas (allow list):** solo se permite ejecutar el software autorizado; todo lo demás queda bloqueado (más restrictivo).
- **Lista de aplicaciones bloqueadas (block list):** se bloquea software específico; el resto se permite.

3. Cifrado de Disco y Hardware de Seguridad

Tecnología	Qué es
FDE (Full Disk Encryption)	Cifra todo el disco (ej. BitLocker, FileVault, VeraCrypt).
SED (Self-Encrypting Drive)	Disco con circuitería de cifrado incorporada.
TPM (Trusted Platform Module)	Chip en la placa madre que guarda claves criptográficas, soporta arranque seguro y atestación remota. Incluye una clave de cifrado grabada de fábrica que aporta una 'raíz de confianza de hardware' (hardware root of trust).
HSM (Hardware Security Module)	Dispositivo removible/externo dedicado a generar, almacenar y gestionar claves criptográficas. A diferencia del TPM, no está integrado a la placa; existen incluso HSM en formato microSD.

Arranque seguro (secure boot) y atestación: el TPM verifica que los archivos de arranque no hayan sido modificados (ej. por malware) antes de permitir el inicio. La **atestación remota** hace lo mismo pero enviando el reporte a un sistema externo que confirma la integridad.

Decommissioning (baja de equipos): antes de dar de baja hardware, hay que borrar todos los datos, revocar credenciales/licencias y destruir o disponer el equipo de forma segura. El hardware *legacy* (obsoleto) o *end-of-life* (fin de vida, sin soporte del fabricante) representa mayor riesgo porque ya no recibe parches.

4. Protección de Datos

La **prevención de pérdida de datos (DLP)** bloquea la exfiltración de datos — la transferencia no autorizada de información fuera de la organización. Puede ser basada en red (examina todo el tráfico saliente buscando palabras clave o patrones, como el formato de un número de Seguro Social) o basada en software (instalada en cada equipo). También puede bloquear el uso de dispositivos USB.

- **Cifrado de bases de datos:** es más común cifrar solo columnas sensibles (ej. número de tarjeta de crédito) que la base entera, para no gastar recursos innecesariamente.
- **Enclave seguro / TEE (Trusted Execution Environment):** área aislada del sistema, basada en hardware (ej. Intel SGX), que procesa datos sensibles de forma segura incluso en un entorno potencialmente inseguro — protege los 'datos en uso'.

5. Conceptos de Computación en la Nube

5.1 Modelos de entrega (qué se ofrece)

Modelo	Qué provee el CSP	Ejemplo
SaaS	La aplicación completa, vía navegador.	Gmail, Google Workspace.
PaaS	Plataforma preconfigurada (SO + apps base); el proveedor la mantiene actualizada.	Hosting gestionado, computación 'serverless'.
IaaS	Solo el hardware; el cliente instala y mantiene todo lo demás.	Amazon EC2.

5.2 Modelos de despliegue (quién lo usa)

- **Pública:** disponible para cualquiera que pague (Amazon, Google, Microsoft).
- **Privada:** para uso exclusivo de una sola organización.
- **Comunitaria:** compartida por organizaciones con intereses o requisitos comunes.
- **Híbrida:** combina dos o más modelos de despliegue (ej. pública + privada).
- **Multi-nube:** distinto de híbrida — combina recursos de dos o más proveedores de nube (ej. AWS + Azure), aumentando la resiliencia pero también la complejidad.

5.3 Matriz de responsabilidad

La responsabilidad de seguridad y mantenimiento se reparte entre el proveedor (CSP) y el cliente según el modelo: en SaaS, el CSP asume casi toda la responsabilidad; en IaaS, el cliente asume mucha más (sistema operativo, middleware, runtime); PaaS queda en un punto intermedio.

5.4 Endurecimiento de entornos en la nube

- **CASB (Cloud Access Security Broker):** se ubica entre la red de la organización y el proveedor de nube; monitorea tráfico y aplica políticas de seguridad.
- **DLP en la nube:** aplica políticas sobre datos almacenados en la nube (ej. detectar y cifrar información personal identificable).
- **SWG de próxima generación:** combina proxy y firewall; filtra URLs, detecta malware y aplica DLP sobre el tráfico saliente hacia Internet.
- **Grupos de seguridad (security groups):** reglas de firewall que el cliente puede definir sobre sus propios recursos, sin tocar el firewall del proveedor directamente.
- **IaC (Infrastructure as Code):** gestionar y aprovisionar centros de datos mediante código (scripts), facilitando la automatización y la reutilización.
- **SDN (Software-Defined Networking):** separa el plano de datos del plano de control, reemplazando routers/switches físicos con virtualización. Cuando conecta sitios a través de una WAN, se llama SD-WAN.

Edge vs. fog computing: ambos procesan datos cerca de donde se generan (evitando la latencia de ir y volver a la nube). Edge computing procesa en un solo nodo/dispositivo; fog computing usa una red de varios nodos cercanos.

6. Despliegue Seguro de Dispositivos Móviles

6.1 Modelos de propiedad

Modelo	Quién es dueño	Detalle
Corporativo	La organización	Uso exclusivamente laboral.
COPE	La organización	El empleado también puede usarlo para fines personales.
BYOD	El empleado	Trae su propio dispositivo; más difícil de gestionar.
CYOD	El empleado	Elige entre una lista de dispositivos aprobados por IT.

6.2 MDM (Mobile Device Management)

Las herramientas MDM (a veces parte de un UEM más amplio) hacen cumplir políticas de seguridad en dispositivos móviles. Funciones clave:

- **Gestión de aplicaciones:** listas de apps permitidas/bloqueadas (MAM cuando es específico de apps).
- **Cifrado total del dispositivo / segmentación de almacenamiento / contenedorización:** aíslan y protegen los datos corporativos sin necesariamente cifrar los datos personales del usuario — clave en escenarios BYOD.
- **Bloqueo de pantalla y borrado remoto (remote wipe):** borra todos los datos de un dispositivo perdido o robado, si sigue conectado.
- **Geolocalización / geofencing / GPS tagging:** geolocalización ubica el dispositivo; geofencing crea un límite virtual (ej. una app solo funciona dentro de la oficina); GPS tagging agrega coordenadas a fotos (riesgo de privacidad si se publican).
- **Autenticación contextual (context-aware):** combina identidad, ubicación, red, hora del día y tipo de dispositivo para decidir si autenticar.

6.3 Riesgos y control de hardware/software

- **Jailbreaking (iOS) / Rooting (Android):** eliminan las restricciones del fabricante, permitiendo instalar apps de cualquier fuente — alto riesgo; el MDM suele bloquear el acceso a la red si detecta esto.
- **Sideloading:** instalar una app (formato APK en Android) copiándola directamente al dispositivo en vez de bajarla de la tienda oficial — riesgo si viene de fuentes no confiables.
- **Tethering / hotspot móvil / Wi-Fi Direct:** permiten a un dispositivo compartir o conectar Internet sin pasar por los controles de red de la organización, evadiendo firewalls y proxies.

7. Sistemas Embebidos, IoT e ICS/SCADA

Un **sistema embebido** es cualquier dispositivo con una función dedicada que usa una computadora para cumplirla (ej. una impresora multifunción). El **Internet de las Cosas (IoT)** agrupa tecnologías que interactúan con el mundo físico y se comunican vía Internet, Bluetooth u otras redes inalámbricas.

- **ICS (Industrial Control System):** sistemas de grandes instalaciones (plantas de energía, tratamiento de agua). **SCADA:** supervisa y envía comandos al ICS. Idealmente están en redes aisladas sin acceso a Internet, y si se conectan a la red corporativa, suele ser mediante una VLAN protegida por un NIPS.
- **SoC (System on Chip):** integra procesador, memoria y E/S en un solo chip, muy compacto y eficiente en energía.
- **RTOS (Real-Time Operating System):** sistema operativo diseñado para timing preciso y determinístico, crítico en dispositivos médicos y automotrices.

Limitaciones de los sistemas embebidos: capacidad de cómputo reducida, restricciones criptográficas (poco poder de procesamiento para cifrado fuerte), dependencia de energía/batería, dificultad de despliegue en ubicaciones remotas, costo, y a menudo la **imposibilidad de parchear** o la falta de parches disponibles del fabricante.

8. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
Hypervisor	Hipervisor	Software que crea y gestiona máquinas virtuales.
VM escape	Escape de VM	Ataque que accede al host desde una VM comprometida.
VM sprawl	Proliferación de VMs	VMs sin gestión ni parches adecuados.
Snapshot	Instantánea	Estado guardado de una VM para poder revertir cambios.
Hardening	Endurecimiento	Asegurar un sistema más allá de su configuración por defecto.
Master image	Imagen maestra	Plantilla segura para desplegar sistemas.
Patch management	Gestión de parches	Mantener sistemas actualizados con parches vigentes.
Change management	Gestión de cambios	Proceso formal de aprobación antes de modificar sistemas.
Application allow/block list	Lista de apps permitidas/bloqueadas	Controla qué software puede ejecutarse.
FDE / SED	Cifrado total de disco / disco autocifrado	Protegen todo el contenido del disco.
TPM / HSM	TPM / HSM	Chip integrado / dispositivo externo para gestión de claves criptográficas.
Data exfiltration	Exfiltración de datos	Transferencia no autorizada de datos fuera de la red.
DLP	Prevención de pérdida de datos	Detecta y bloquea la exfiltración de información.
Secure enclave / TEE	Enclave seguro	Área aislada de hardware para procesar datos sensibles.
SaaS / PaaS / IaaS	SaaS / PaaS / IaaS	Modelos de entrega de servicios en la nube.

Inglés	Español	Definición breve
Multi-cloud	Multi-nube	Uso de recursos de dos o más proveedores de nube.
CASB	CASB	Intermediario de seguridad entre la red y el proveedor de nube.
IaC	Infraestructura como código	Gestión de infraestructura mediante scripts.
SDN / SD-WAN	Red definida por software	Separa el plano de datos del de control usando virtualización.
BYOD / COPE / CYOD	BYOD / COPE / CYOD	Modelos de propiedad de dispositivos móviles.
MDM	Gestión de dispositivos móviles	Aplica políticas de seguridad a móviles.
Jailbreaking / Rooting	Jailbreak / Rooteo	Eliminar restricciones del fabricante en iOS/Android.
Sideloading	Carga lateral	Instalar apps fuera de la tienda oficial.
ICS / SCADA	ICS / SCADA	Sistemas de control industrial y su supervisión.
RTOS	Sistema operativo en tiempo real	SO con timing preciso para sistemas embebidos.

9. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 5. Las respuestas están al final.

1. Una empresa tiene 9 servidores físicos subutilizados (menos del 20% de uso) y quiere consolidarlos en menos hardware. ¿Qué tecnología es la más adecuada?

2. Un administrador crea una VM para probar una aplicación y se olvida de avisar al equipo de IT, por lo que queda sin los parches de seguridad más recientes. ¿Cómo se llama este problema?

3. Antes de aplicar un parche riesgoso a una VM, un administrador guarda su estado actual para poder revertir los cambios si algo sale mal. ¿Qué herramienta está usando?

4. Una organización quiere dar a los nuevos empleados equipos ya configurados con todas las políticas de seguridad aplicadas, sin tener que configurar cada uno manualmente. ¿Qué técnica deberían usar?

5. Una empresa contrata un servicio en la nube donde solo recibe acceso al hardware (servidores, almacenamiento, red) y debe instalar y mantener todo lo demás ella misma. ¿Qué modelo de nube es?

6. Dos organizaciones combinan recursos de AWS y Microsoft Azure para aumentar la resiliencia de sus sistemas. ¿Es esto un despliegue híbrido o multi-nube?

7. Una empresa permite a los empleados usar sus propios celulares para trabajar, pero quiere asegurarse de que los datos corporativos estén cifrados sin cifrar los datos personales del usuario. ¿Qué técnica de MDM es la más adecuada?

8. Un usuario modificó su iPhone para poder instalar aplicaciones desde fuentes no oficiales, eliminando las restricciones de Apple. ¿Cómo se llama esta práctica?

9. Una planta de tratamiento de agua tiene un sistema que supervisa y envía comandos a los equipos industriales del lugar. ¿Cómo se llama este tipo de sistema?

10. Un dispositivo médico embebido necesita reaccionar a eventos dentro de un tiempo estrictamente definido para garantizar la seguridad del paciente. ¿Qué tipo de sistema operativo requiere?

Respuestas

1. Virtualización — permite alojar varias VMs en menos servidores físicos, aprovechando mejor los recursos.

2. VM sprawl (proliferación de VMs) — VMs no gestionadas ni parcheadas por falta de comunicación con IT.

3. Un snapshot (instantánea) — permite revertir la VM a un estado conocido y seguro.

4. Imágenes maestras (master images) — un punto de partida seguro y consistente para desplegar equipos.

5. IaaS (Infrastructure as Service) — el proveedor solo entrega el hardware.

6. Multi-nube — combina recursos de dos proveedores de nube distintos, a diferencia de híbrida que combina modelos de despliegue (ej. pública + privada).

7. Contenedorización — cifra y aísla los datos corporativos en un contenedor sin afectar los datos personales.

8. Jailbreaking — elimina las restricciones de software de un dispositivo Apple.

9. Un sistema SCADA (Supervisory Control and Data Acquisition), que controla el ICS de la planta.

10. Un RTOS (Real-Time Operating System) — garantiza tareas completadas dentro de un tiempo específico.
