Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 8

Using Risk Management Tools — Herramientas de Gestión de Riesgos

---

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. Entendiendo la Gestión de Riesgos

Riesgo es la probabilidad de que una amenaza explote una vulnerabilidad. Se evalúa con dos criterios: **impacto** (magnitud del daño) y **probabilidad/likelihood** (con qué frecuencia se espera que ocurra). No es posible eliminar el riesgo por completo, solo gestionarlo.

1.1 Amenazas

Una **amenaza** es cualquier circunstancia que pueda comprometer confidencialidad, integridad o disponibilidad. Pueden ser humanas maliciosas (atacantes), humanas accidentales (errores de usuarios o administradores) o ambientales (cortes de energía, huracanes, terremotos). Un **threat assessment** identifica y prioriza estas amenazas junto con su probabilidad e impacto potencial.

1.2 Tipos de riesgo

- **Interno / externo:** riesgos desde dentro de la organización vs. desde afuera.
- **Robo de propiedad intelectual:** pérdida de patentes, secretos comerciales, etc.
- **Cumplimiento de licencias de software:** usar más licencias de las compradas genera pérdidas económicas.
- **Sistemas legacy:** el riesgo principal es la falta de soporte y parches del fabricante.

1.3 Estrategias de gestión de riesgos

Estrategia	Descripción
Evitar (avoidance)	Dejar de ofrecer el servicio o participar en la actividad riesgosa.
Mitigar (mitigation)	Implementar controles que reducen la vulnerabilidad o el impacto.
Aceptar (acceptance)	Cuando el costo del control supera el costo del riesgo; puede requerir una excepción o exención de política.
Transferir (transference)	Compartir el riesgo con otra entidad, típicamente mediante un seguro (ej. ciberseguro).

■ Recordá esto!

No es posible eliminar el riesgo, pero sí gestionarlo. Se puede evitar un riesgo dejando de ofrecer un servicio; un seguro transfiere el riesgo a otra entidad; se mitiga implementando controles; y cuando el costo del control supera al del riesgo, la organización acepta el riesgo residual.

Riesgo inherente: el riesgo que existe antes de aplicar controles. **Riesgo residual:** el que queda después de mitigar. **Riesgo de control:** el riesgo de que los controles ya implementados no sean adecuados. **Apetito de riesgo (risk appetite):** cuánto riesgo está dispuesta a aceptar la organización — puede ser *expansionista* (alto riesgo por alta recompensa), *conservador* (prioriza estabilidad) o *neutral* (enfoque equilibrado). **Tolerancia al riesgo:** la capacidad de la organización para soportar el riesgo (distinto del apetito, que es la disposición a aceptarlo).

2. Tipos de Evaluación de Riesgos

Las evaluaciones pueden ser puntuales (ad hoc/one-time), recurrentes (ej. anuales) o continuas. Comienzan identificando el **valor del activo (AV)** para enfocar los esfuerzos en los activos de mayor valor.

2.1 Evaluación cuantitativa

Usa montos monetarios específicos. Fórmulas clave:

- **EF (Exposure Factor):** porcentaje del activo que se dañaría en cada ocurrencia.
- **SLE (Single Loss Expectancy) = AV × EF:** costo de una sola pérdida.
- **ARO (Annualized Rate of Occurrence):** cuántas veces se espera que ocurra por año.
- **ALE (Annualized Loss Expectancy) = SLE × ARO:** pérdida anual esperada.

Ejemplo: un equipo vale $1.000.000 (AV) y una inundación dañaría el 50% (EF=50%) → SLE = $500.000. Si se espera una inundación cada 10 años, ARO = 0,1 → ALE = $50.000/año. Regla práctica: si el costo del control es menor que el ahorro que genera, se compra; si es mayor, se acepta el riesgo.

2.2 Evaluación cualitativa

Usa juicios (bajo/medio/alto) en vez de números exactos, muchas veces mediante encuestas a expertos. Se puede asignar valores (1, 5, 10) a probabilidad e impacto y multiplicarlos para priorizar (ej. servidor web: alta probabilidad × alto impacto = 100; PC de biblioteca: baja × baja = 1).

■ Recordá esto!

La evaluación cuantitativa usa montos monetarios exactos: SLE = AV × EF; ARO indica la frecuencia anual; ALE = SLE × ARO. La evaluación cualitativa usa juicios para categorizar riesgos según probabilidad e impacto.

El reporte de riesgos es sensible — solo ejecutivos y profesionales de seguridad deberían acceder a él, porque revela vulnerabilidades y controles en detalle, información valiosa para un atacante.

2.3 Análisis de riesgos

- **KRI (Key Risk Indicators):** métricas para monitorear el nivel de riesgo (ej. incidentes por mes, % de parches vencidos).
- **Registro de riesgos (risk register):** documento que lista riesgos conocidos, su probabilidad/impacto y asigna un *dueño del riesgo (risk owner)* responsable de gestionarlo.
- **Matriz de riesgo:** gráfico que ubica los riesgos según probabilidad e impacto.

2.4 Riesgos de la cadena de suministro

La cadena de suministro incluye todos los proveedores necesarios (hardware, software, servicios) para crear y distribuir un producto. Un atacante puede interrumpir la cadena atacando a un tercero en vez de a la organización directamente — un indicador clave es una disrupción inesperada en la cadena.

3. Comparando Herramientas de Escaneo y Pruebas

3.1 Escáneres de red

- **ARP ping scan:** detecta hosts activos mediante respuestas ARP.
- **SYN stealth scan:** envía un SYN a cada IP; si responde, hay un host activo (cierra con RST en vez de completar el handshake).
- **Escaneo de puertos:** identifica puertos abiertos (protocolo/servicio probable).
- **Escaneo de servicios:** va más allá, confirma qué servicio corre realmente en un puerto.
- **Detección de SO (fingerprinting):** analiza respuestas de paquetes (ej. tamaño de ventana TCP) para identificar el sistema operativo.

3.2 Escaneo de vulnerabilidades

Identifica vulnerabilidades, malas configuraciones y ausencia de controles, probando pasivamente los controles de seguridad — **no explota** nada.

- **CVE (Common Vulnerabilities and Exposures):** diccionario público de vulnerabilidades conocidas (mantenido por MITRE).
- **CVSS (Common Vulnerability Scoring System):** asigna severidad de 0 a 10.
- **SCAP:** facilita la comunicación entre escáneres y otras herramientas de seguridad.

Priorización de vulnerabilidades: clasificación (CVSS), variables del entorno, impacto en la industria/organización, y tolerancia/umbral de riesgo de la organización.

3.3 Confirmación de resultados: falsos positivos y negativos

	Vulnerabilidad real	No hay vulnerabilidad
El escáner la reporta	Verdadero positivo	Falso positivo
El escáner no la reporta	Falso negativo	Verdadero negativo

3.4 Escaneos con y sin credenciales

Un **escaneo credenciado** usa una cuenta válida y accede a información más profunda (ej. versiones de software instalado), con menos falsos positivos. Un **escaneo no credenciado** simula la perspectiva de un atacante sin acceso previo.

■ Recordá esto!

Un falso positivo indica una vulnerabilidad que no existe. Los escaneos credenciados obtienen información más detallada y precisa, con menos falsos positivos que los no credenciados.

4. Pruebas de Penetración (Penetration Testing)

A diferencia del escaneo de vulnerabilidades (pasivo), el pentest es **activo**: intenta explotar las vulnerabilidades encontradas. Requiere **consentimiento por escrito** y reglas de compromiso (rules of engagement) antes de comenzar — sin autorización, es un ataque, no una prueba.

Categoría	Enfoque
Física	Vulnerabilidades en seguridad física (cerraduras, ingeniería social, acceso a edificios).
Ofensiva	Simula un ataque real desde la perspectiva del atacante.
Defensiva	Evalúa la efectividad de los controles ya implementados.
Integrada	Combina física, ofensiva y defensiva para una evaluación completa.

4.1 Fases de un pentest

- **Reconocimiento pasivo:** OSINT (redes sociales, noticias, sitio web) sin interactuar con el objetivo — no es ilegal.
- **Reconocimiento activo:** herramientas que envían datos al objetivo y analizan respuestas (Nmap, Netcat, dnsenum, Nessus, hping, etc.) — casi siempre ilegal sin autorización.
- **Explotación inicial:** aprovechar una vulnerabilidad descubierta para obtener acceso.
- **Persistencia:** mantener presencia en la red (ej. backdoors) sin ser detectado.
- **Movimiento lateral:** usar el sistema comprometido para acceder a otros (ej. con WMI o PowerShell).
- **Escalamiento de privilegios:** obtener cada vez más permisos dentro de la red.
- **Pivoting:** usar un sistema ya comprometido para atacar otros sistemas.
- **Limpieza (cleanup):** eliminar cuentas, scripts y archivos creados durante la prueba.

4.2 Nivel de conocimiento del entorno

Tipo	Conocimiento previo
Entorno desconocido (unknown / black box)	Cero conocimiento previo, igual que un atacante real.
Entorno conocido (known / white box)	Conocimiento total: documentación, código fuente, credenciales.
Entorno parcialmente conocido (partially known / gray box)	Conocimiento parcial del sistema o red.

Intrusivo vs. no intrusivo: el pentest es intrusivo (invasivo) — puede interrumpir servicios. El escaneo de vulnerabilidades es no intrusivo — mucho más seguro de ejecutar sin afectar operaciones.

4.3 Programas de divulgación responsable

Los **programas de divulgación responsable** permiten reportar vulnerabilidades encontradas a la organización correspondiente antes de que sean explotadas. Los **programas de bug bounty** son una variante que ofrece recompensas monetarias por reportes válidos, creando un modelo de expertos externos buscando vulnerabilidades ('crowdsourcing').

5. Respondiendo a Vulnerabilidades

El método más común es **aplicar el parche**. Cuando no hay parche disponible, las opciones son:

- **Control compensatorio:** control secundario que previene la explotación (ej. un WAF frente a una vulnerabilidad SQLi conocida).
- **Segmentación:** aislar el sistema vulnerable en una red separada.
- **Excepción/exención de política:** permitir que el sistema siga operando pese a no cumplir la política — idealmente junto con otras medidas, no solo.

Validación de la remediación: tras corregir, se debe volver a escanear (rescan) para confirmar que la vulnerabilidad ya no existe, y documentar todo para futuras auditorías.

6. Captura de Tráfico de Red

Un **analizador de protocolos (sniffer)** como Wireshark captura y analiza paquetes, útil para solucionar problemas de comunicación o detectar manipulación de paquetes. Puede revelar credenciales en texto plano si el protocolo (ej. SMB) no las cifra.

- **Tcpreplay:** edita capturas de paquetes y las reenvía por la red — útil para probar si un IDS detecta ataques conocidos.
- **Tcpdump:** analizador de protocolos por línea de comandos (case-sensitive).
- **NetFlow:** recopila estadísticas de tráfico IP (no el contenido/payload) en routers y switches, y las envía a un colector para análisis.

7. Marcos y Estándares (Frameworks)

7.1 Normas ISO

- **ISO 27001:** requisitos de un sistema de gestión de seguridad de la información (ISMS).
- **ISO 27002:** guía de mejores prácticas, complementaria a la 27001.
- **ISO 27701:** extensión enfocada en gestión de información privada (PII), compatible con el RGPD/GDPR.
- **ISO 31000:** familia de estándares sobre gestión de riesgos.

7.2 Marcos específicos de industria y NIST

PCI DSS: estándar obligatorio para organizaciones que manejan tarjetas de crédito. **CIS:** ofrece guías gratuitas de mejores prácticas. **NIST RMF** (SP 800-37): marco de 7 pasos — Preparar, Categorizar, Seleccionar, Implementar, Evaluar, Autorizar, Monitorear. **NIST CSF:** incluye Núcleo (identificar, proteger, detectar, responder, recuperar), Niveles (Tier 1-4) y Perfiles (actual vs. objetivo) para identificar brechas.

8. Auditorías y Evaluaciones

Una **auditoría** es una evaluación formal de políticas, procedimientos y operaciones; confirma que los controles de seguridad son adecuados y efectivos. Una **evaluación (assessment)** es una revisión menos formal (escaneos, pentests, revisiones de controles).

- **Auditoría externa:** realizada por una firma independiente.
- **Auditoría interna:** realizada por un equipo propio de la organización, dirigido por el comité de auditoría.
- **Análisis de brechas (gap analysis):** compara los requisitos de un estándar (ej. ISO 27001) contra las operaciones reales de la organización, identificando oportunidades de mejora.
- **Attestation:** declaración formal del auditor confirmando que los controles están implementados y funcionan correctamente.

9. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
Risk / threat / vulnerability	Riesgo / amenaza / vulnerabilidad	Probabilidad de explotación / peligro potencial / debilidad.
Residual risk	Riesgo residual	El que queda tras aplicar controles.
Risk appetite / tolerance	Apetito / tolerancia al riesgo	Disposición a aceptar riesgo / capacidad de soportarlo.
SLE / ARO / ALE	SLE / ARO / ALE	Pérdida por evento / frecuencia anual / pérdida anual esperada.
Risk register	Registro de riesgos	Documento con riesgos identificados, dueños y puntajes.
Supply chain	Cadena de suministro	Proveedores necesarios para crear y distribuir un producto.
Vulnerability scan	Escaneo de vulnerabilidades	Identificación pasiva de debilidades, sin explotarlas.
CVE / CVSS	CVE / CVSS	Diccionario de vulnerabilidades / sistema de puntaje de severidad.
False positive / negative	Falso positivo / negativo	Reporte incorrecto de vulnerabilidad / vulnerabilidad no detectada.
Credentialed scan	Escaneo credenciado	Escaneo realizado con una cuenta válida.
Penetration testing	Prueba de penetración (pentest)	Prueba activa que explota vulnerabilidades.
Rules of engagement	Reglas de compromiso	Límites acordados antes de un pentest.
Reconnaissance	Reconocimiento	Fase de recopilación de información sobre el objetivo.
Lateral movement / pivoting	Movimiento lateral / pivoting	Uso de un sistema comprometido para acceder a otros.
Known/unknown/partially known environment	Entorno conocido/desconocido/parcial	Nivel de conocimiento previo del probador.
Bug bounty program	Programa de recompensas por errores	Incentivo monetario por reportar vulnerabilidades.

Inglés	Español	Definición breve
Compensating control	Control compensatorio	Control alternativo cuando no se puede aplicar el principal.
NetFlow	NetFlow	Estadísticas de tráfico IP recolectadas por routers/switches.
Gap analysis	Análisis de brechas	Comparación entre un estándar y las operaciones reales.
Attestation	Attestation (certificación)	Declaración formal del auditor sobre la efectividad de los controles.

10. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 8. Las respuestas están al final.

1. Un servidor valorado en $8.000 sufre 4 fallas al año, cada una con una pérdida del 25%. ¿Cuál es el ALE?

2. Un escaneo de vulnerabilidades reporta que un servidor le falta un parche, pero en realidad el parche sí está instalado. ¿Cómo se llama este error?

3. Un equipo de seguridad realiza un escaneo usando las credenciales de una cuenta administrativa para obtener información detallada del software instalado. ¿Qué tipo de escaneo es?

4. Un evaluador quiere simular exactamente lo que vería un atacante externo, sin ningún conocimiento previo del sistema. ¿Qué tipo de entorno de prueba debería usar?

5. Un probador de penetración, tras comprometer la computadora de un empleado, la usa para intentar acceder a otros sistemas de la red. ¿Cómo se llama esta técnica?

6. Una organización decide no aplicar un parche que rompe una aplicación crítica, pero protege el sistema colocándolo detrás de un firewall de aplicaciones web. ¿Qué tipo de respuesta a la vulnerabilidad es esta?

7. Un analista revisa estadísticas de tráfico IP recolectadas por los routers de la red, sin ver el contenido de los paquetes. ¿Qué herramienta está usando?

8. Una empresa que maneja pagos con tarjetas de crédito necesita cumplir con un estándar específico de la industria. ¿Cuál es?

9. Un equipo de auditoría interna compara los requisitos de ISO 27001 con las operaciones actuales de la empresa para identificar dónde no se cumple el estándar. ¿Cómo se llama este proceso?

10. Una organización ofrece recompensas monetarias a investigadores externos que reporten vulnerabilidades válidas en su software. ¿Cómo se llama este tipo de programa?

Respuestas

1. SLE = $8.000 × 25% = $2.000; ALE = SLE × ARO = $2.000 × 4 = $8.000 por año.

2. Un falso positivo — el escáner reportó una vulnerabilidad que no existe.

3. Un escaneo credenciado (credentialed scan).

4. Entorno desconocido (unknown environment / black box).

5. Movimiento lateral (lateral movement), o más específicamente pivoting si usa ese sistema como puente.

6. Un control compensatorio (compensating control).

7. NetFlow.

8. PCI DSS (Payment Card Industry Data Security Standard).

9. Un análisis de brechas (gap analysis).

10. Un programa de bug bounty.
