SY0-801 · CHEAT SHEET · CERTIFYDECK

CompTIA Security+

Dominios, pesos oficiales y habilidades clave del temario de SY0-801, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 90 min Nota de corte: 750/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. General Security Concepts

16–16%

1.1 Explain security concepts and controls.

- La defensa en profundidad superpone barreras de personas, tecnología y operaciones para que lo que se escapa a una capa lo detenga otra. La tríada CIA protege confidencialidad, integridad y disponibilidad; AAA separa autenticación, autorización y contabilidad (registro de lo que se hizo). El no repudio impide negar una acción, el mínimo privilegio limita permisos y Zero Trust decide cada acceso sin confianza implícita.
- Las categorías de control dicen quién o qué aplica el control. Los técnicos los ejecutan mecanismos de hardware, software o firmware (firewalls, bloqueo de cuentas); los de gestión se centran en gestionar el riesgo y el programa de seguridad (evaluaciones de riesgos, políticas); los operativos los ejecutan personas (formación, procedimientos del centro de soporte) y los físicos protegen instalaciones y equipos.
- Los tipos de control describen cuándo y cómo actúa un control: el preventivo impide el incidente (bloqueo USB, IPS), el disuasorio desanima al atacante (carteles), el de detección descubre lo ocurrido (IDS, revisión de registros), el correctivo recupera la situación (restaurar copias), el directivo indica qué hacer (políticas) y el compensatorio da una protección comparable cuando el control habitual no puede aplicarse.

1.2 Given a scenario, demonstrate the impact of change management processes on security.

- Un cambio se solicita, se registra, se analiza su impacto en la seguridad, se prueba y lo aprueba el comité asesor de cambios (CAB), que recibe el plan y los resultados de las pruebas. La solicitud indica propietario, partes interesadas a las que avisar, ventana de mantenimiento y plan de reversión. Los cambios detectados se concilian comprobando si había una solicitud aprobada y si ocurrieron en la ventana prevista.
- Un cambio tiene consecuencias técnicas que hay que prever: el software nuevo debe añadirse a la lista de permitidos si se aplica denegar todo y permitir por excepción; las dependencias con otros sistemas forman parte del análisis de impacto; las aplicaciones heredadas pueden fallar con configuraciones bastionadas; y quien ejecuta el cambio se limita a las actividades aprobadas, con avisos si habrá reinicios o tiempo de inactividad.
- Un cambio no termina al desplegarse: hay que actualizar diagramas de red, diseños técnicos, configuración base, inventario, plan de seguridad y los procedimientos que usan el soporte y los usuarios. Esto vale también para los cambios estándar preaprobados. La configuración base anterior y los registros de aprobación se conservan sin modificarlos para la trazabilidad, las auditorías y una posible reversión.
- El control de versiones guarda el código, la configuración como código y las configuraciones base en un repositorio que registra cada cambio y la cuenta que lo hizo. Conservar las versiones anteriores permite volver a una configuración aprobada y ayuda en auditorías y respuesta a incidentes. Como el historial lo guarda todo, un secreto confirmado sigue expuesto aunque se borre después: hay que revocarlo y rotarlo.

1.3 Explain the importance of using appropriate cryptographic solutions.

- En una PKI cada identidad tiene un par de claves: la pública puede compartirse y sirve para cifrar datos dirigidos al propietario y verificar sus firmas; la privada nunca se publica y sirve para firmar y descifrar. El depósito de claves conserva la clave privada asociada a un certificado de cifrado para poder recuperar los datos si el usuario la pierde o deja la organización.
- La autoridad de certificación emite y revoca certificados; su raíz es el punto de partida de la confianza. La CRL es una lista firmada y periódica de certificados revocados, y OCSP consulta el estado de uno en concreto con información más oportuna. La CSR lleva la clave pública firmada con la privada. Un certificado autofirmado depende de distribuirse con seguridad, y un comodín cubre una sola etiqueta a la izquierda.
- El cifrado simétrico (AES) usa la misma clave para cifrar y descifrar y se emplea para grandes volúmenes; el asimétrico (RSA, ECC) sirve para establecer claves y firmar en esquemas híbridos. El cifrado de disco, partición o volumen protege frente al robo del equipo apagado, pero no con el sistema en marcha; el de base de datos o registro protege valores concretos. TLS 1.3 solo admite intercambios con secreto perfecto hacia delante.
- La firma digital se genera con la clave privada del firmante y se verifica con su clave pública; demuestra el origen y la integridad de los datos y aporta no repudio, porque solo el firmante posee la clave privada. Un HMAC usa una clave compartida y no ofrece no repudio. La firma de código con certificados de una CA reconocida permite a los sistemas operativos comprobar quién publicó un ejecutable y si se ha alterado.
- La sal es un valor aleatorio y único que se combina con cada contraseña antes de calcular el hash con un esquema lento de hash de contraseñas. Hace que contraseñas iguales den hashes distintos e inutiliza las tablas arcoíris precalculadas. Se guarda junto al hash y no tiene que ser secreta; el valor secreto que se guarda aparte es la pimienta (pepper). La lentitud la aporta el factor de coste, no la sal.

2. Threats, Vulnerabilities, and Attacks

24–24%

2.1 Explain characteristics of threats and vulnerabilities.

- La inteligencia de amenazas es información sobre amenazas agregada, analizada y enriquecida para aportar contexto a las decisiones; un feed en bruto de indicadores no lo es por sí solo. En una evaluación de riesgos, la probabilidad estima cuándo puede explotarse una vulnerabilidad y el impacto cuánto daño causaría si ocurre; CVSS puntúa la gravedad técnica de una vulnerabilidad, no el riesgo de una organización concreta.
- CVSS asigna una puntuación de 0 a 10 a partir de métricas base sobre explotación y alcance, y completarlas correctamente es crucial porque de ellas depende la nota final. Las bandas cualitativas son Baja 0,1-3,9, Media 4,0-6,9, Alta 7,0-8,9 y Crítica 9,0-10,0. Para priorizar, CISA aconseja corregir primero lo que figura en el catálogo KEV con explotación activa demostrada.

2.2 Describe common threat actors and motivations.

- CISA define al insider como quien tiene o tuvo acceso autorizado a los recursos de la organización o conocimiento de ellos, incluidos contratistas y proveedores con acceso. La amenaza interna puede ser intencionada (maliciosa), por negligencia o accidental, como enviar por error un documento a un destinatario equivocado.
- La motivación explica qué busca el actor: beneficio económico, espionaje, notoriedad, venganza, extorsión o una causa ideológica o política, según CISA. Señala que muchas amenazas internas intencionadas quieren pasar desapercibidas y que a menudo no buscan notoriedad, a diferencia de los ataques externos.
- Los autores se distinguen por si son internos o externos, por sus recursos y financiación y por su nivel de sofisticación. NIST SP 800-30 evalúa a los adversarios por capacidad (conocimientos, recursos, oportunidades), intención y selección de objetivos. CISA describe además amenazas colusorias, en las que un insider colabora con actores externos a menudo ciberdelincuentes que lo reclutan para cometer fraude.

2.3 Describe threat vectors and sources.

- NIST define el APT como un adversario sofisticado y con muchos recursos que usa varios vectores (cibernético, físico, engaño) y persigue sus objetivos durante largos periodos, adaptándose a las defensas. CISA lo asocia a actores estatales con fines como espionaje, robo de datos o disrupción, y advierte que un mismo APT puede tener varios nombres según cada organización le asigna el suyo.
- Los vectores basados en mensajes llegan por correo, SMS, RCS, mensajería instantánea o herramientas de colaboración. El smishing usa SMS con urgencia para que la víctima pulse un enlace o instale malware. Con una cuenta externa como punto de partida, el atacante puede hacer spear phishing interno por el chat corporativo, aprovechando la confianza en remitentes conocidos para robar credenciales.
- Los vectores basados en imágenes ocultan el señuelo dentro de una imagen: el quishing usa códigos QR que llevan a sitios de phishing y saltan del equipo al móvil, evadiendo la inspección de URL. Los falsos CAPTCHA (ClickFix) piden al usuario pegar y ejecutar un comando, lo que pasa por alto el filtrado de correo, el sandbox del navegador y el control de aplicaciones y ayuda a frenarlos.
- Los adjuntos maliciosos (documentos con macros, PDF, HTML) comprimidos o cifrados para burlar el filtrado de correo se reconocen por el tipo de archivo inesperado y el señuelo de urgencia. El malware suele ocultarse en el interior y activarse al manipularlo, por lo que conviene deshabilitar las macros. Es la pasarela de correo la encargada de abrirlos, detonarlos en sandbox y analizar y eliminar los adjuntos maliciosos antes de entregarlos.
- El navegador es un vector por sus extensiones, el JavaScript, las cookies y las credenciales y el robo de sesión. Una cookie de sesión robada permite usar la aplicación web como el usuario y eludir parte de la MFA, porque la sesión ya está autenticada. Las extensiones maliciosas imitan nombres legítimos; se mitigan con listas de extensiones permitidas e instalando solo desde fuentes de confianza.

2.4 Explain types of vulnerabilities and attack surfaces.

- Un producto sin soporte ya no recibe actualizaciones de su fabricante, así que cada fallo nuevo queda sin corregir; CISA advierte que los dispositivos perimetrales sin soporte son objetivo de campañas de explotación y deben retirarse. Mientras no se sustituyen, NIST SP 800-40r4 los trata como activos aislados, con parcheo cuidadoso y mitigaciones compensatorias, porque no se pueden parchear con normalidad.
- La gestión de parches identifica, prioriza, obtiene, instala y verifica parches. Un parche puede necesitar reinicio o parada para surtir efecto, por lo que hay que verificar que se ha aplicado de verdad y vigilar que siga instalado. Si un fallo se explota activamente y aún no hay parche, NIST recomienda una mitigación de emergencia temporal, sustituida después por la corrección.
- Los sistemas obsoletos existen porque ya no cumplen los requisitos actuales: equipos heredados sin soporte, protocolos retirados y sin recursos para añadir seguridad, o protocolos retirados como TLS 1.0 y 1.1, que el IETF desaconseja por carecer de algunas garantías actuales. Hasta sustituirlos, deben protegerse con controles compensatorios, en lugar de dejarlos expuestos.
- Un activo gestionado es un activo conectado a la red que puede formar parte de los procesos de inventario, parches, configuración y supervisión, por lo que acumula vulnerabilidades sin que nadie las vea. El Control 1 de CIS pide descubrir, inventariar y gestionar todos los activos (equipos, red, IoT, servidores y nube) para detectar los no autorizados o no gestionados y retirarlos. NIST SP 800-123 recomienda eliminar, mejor que solo deshabilitar, los servicios innecesarios, y MITRE ATT&CK aconseja canalizar el acceso remoto por VPN u otros concentradores gestionados con MFA en lugar de exponerlo directamente.

2.5 Given a scenario, analyze indicators of malicious activity.

- Cada tipo de malware deja indicadores distintos: el ransomware cifra y renombra archivos y pide un rescate, el gusano se propaga solo por la red, la bomba lógica espera una condición para activarse, el rootkit oculta procesos y archivos para mantener acceso privilegiado, el spyware recopila información en secreto y el malware sin archivos se ejecuta en memoria sin dejar archivos en disco.
- Los ataques de red tienen patrones propios: un DDoS satura el ancho de banda desde muchos orígenes, un ataque en ruta se apoya en envenenamiento ARP o en degradar HTTPS a HTTP, y el envenenamiento de caché DNS hace que un resolvedor acepte respuestas falsificadas y las reparta a sus clientes. RFC 5452 recomienda aleatorizar IDs y puertos de origen para dificultar la falsificación.
- La ingeniería social se vale sobre todo de phishing por correos web falsos, smishing por SMS con enlaces y vishing por voz, a menudo con un identificador de llamada falsificado. CISA y MITRE ATT&CK señalan como indicador de compromiso el tráfico hacia dominios recién registrados, procesos extraños, marcas de tiempo alteradas, logs borrados, consumo excesivo de recursos, bloqueos de cuenta o viajes imposibles. MITRE ATT&CK describe cómo los atacantes manipulan fechas y registros para ocultarse.
- La evasión modifica el tráfico para que un proxy no lo reconozca como malicioso, y la ofuscación lo hace ilegible. Cuando la salida es un LLM inferencia a partir de entrada no confiable, el riesgo clásico es la inyección de prompts, que hace ignorar las normas de seguridad del modelo.

2.6 Summarize threats and vulnerabilities associated with artificial intelligence (AI) usage.

- Las amenazas de IA de este grupo afectan a la integridad del modelo: el envenenamiento manipula los datos de entrenamiento o ajuste fino para introducir sesgos o puertas traseras, y la inyección de prompts usa entradas directas o contenido externo para alterar su comportamiento y provocar fugas de datos. Se mitigan verificando el origen de los datos, separando el contenido no fiable y exigiendo aprobación humana en acciones de riesgo.
- Cuando la salida de un LLM se pasa a otro componente sin validar, el riesgo clásico es una inyección de shell provocada por ejecución remota de código, y ocurre igual si el modelo escribe en una base de datos. Un ejemplo típico es un chatbot que genera una consulta SQL a partir de la petición del usuario y la ejecuta sin filtrar.
- Otro caso es un LLM que devuelve HTML o JavaScript que el navegador interpreta, lo que provoca XSS. Hay que tratar al modelo como un usuario no fiable, validar su salida y codificarla según el contexto donde se use.

3. Security Architecture

19–19%

3.1 Compare and contrast security implications of different architecture models.

- Los modelos de despliegue en la nube se diferencian por quién los usa: la nube privada es de una sola organización, la comunitaria de un grupo con requisitos comunes, la pública está abierta a todos y la híbrida combina varias infraestructuras. Una red air-gapped no tiene conexión física con otras y solo intercambia datos de forma manual, a diferencia de la segmentación lógica con VLAN o cortafuegos.
- Al comparar arquitecturas hay que tener en cuenta la responsabilidad: en IaaS el cliente gestiona sistemas operativos, almacenamiento y aplicaciones, mientras que en PaaS el proveedor se ocupa del sistema operativo.
- La resiliencia es la capacidad de seguir operando en condiciones adversas, aunque sea degradado, y recuperarse en un plazo acorde con la misión, la disponibilidad es el acceso puntual y fiable a la información.
- Entre las consideraciones de negocio de una arquitectura están la soberanía de los datos, porque los datos quedan sujetos a las leyes del lugar donde se tratan y el RGPD limita las transferencias a terceros países, y la escalabilidad, que la nube ofrece mediante la elasticidad rápida para aprovisionar y liberar capacidad según la demanda.

3.2 Given a scenario, manage the security architecture to best protect the infrastructure.

- La ubicación de los dispositivos define las zonas de seguridad: los servidores públicos van en una DMZ o subred filtrada, que da acceso restringido desde el exterior y protege la red interna. La superficie de ataque es el conjunto de puntos por los que un atacante puede entrar o extraer datos, y se reduce desactivando servicios, puertos y software innecesarios.
- En Zero Trust ningún usuario ni activo es de confianza por estar en la red: cada acceso se concede por sesión según una política dinámica que tiene en cuenta la identidad y el estado del dispositivo. El motor de políticas decide, el administrador de políticas ejecuta la decisión y el punto de aplicación de políticas habilita, supervisa y termina las conexiones con el recurso.
- Las comunicaciones seguras incluyen decidir qué tráfico va por la VPN: el túnel dividido solo protege el tráfico interno e impide inspeccionar el resto, por lo que conviene deshabilitarlo en redes no fiables. La gestión fuera de banda usa rutas dedicadas para administrar los dispositivos de red, separa ese tráfico del de usuario y permite corregir sin que un atacante en la red de producción lo vea.
- La gestión de identidades aplica el mínimo privilegio también a las cuentas de servicio: una gMSA tiene una contraseña generada y rotada automáticamente por el directorio, lo que dificulta ataques como el Kerberoasting. La acumulación de privilegios aparece cuando alguien cambia de puesto y conserva los permisos anteriores; se evita con revisiones periódicas de accesos y retirando los permisos innecesarios.
- Los modos de fallo definen qué hace un sistema cuando falla: el fallo seguro (cerrado) conserva el estado seguro aunque se interrumpa el servicio, el fail-safe prioriza evitar daños a personas o bienes aunque se pierda seguridad, y el fallo suave detiene solo las funciones no esenciales. La elección depende de si el requisito prioriza la seguridad de la información o la de las personas.

3.3 Summarize concepts and strategies used to protect data.

- Los datos estructurados siguen un esquema predefinido de filas y campos, como una tabla de base de datos, mientras que los no estructurados, como texto libre, imágenes, audio y vídeo, carecen de una estructura explícita que relacione los datos con las personas. Por eso los datos no estructurados son más difíciles de localizar, clasificar y proteger con herramientas basadas en campos.
- Los datos tienen tres estados: en reposo cuando están almacenados en un dispositivo o soporte, en tránsito cuando se mueven entre sistemas o sedes, y en uso cuando se visualizan, modifican o procesan. Cada estado requiere controles distintos: cifrado de disco para el reposo y protocolos como TLS 1.3 o IPsec para el tránsito; TLS 1.0 y 1.1 están obsoletos.
- La clasificación asigna a cada dato un nivel según el daño que causaría su divulgación o pérdida. La información pública es la que la organización pone a disposición de todos; la sensible podría perjudicar la privacidad o las operaciones sin estar clasificada oficialmente, y los niveles como secreto o alto secreto solo se aplican a información designada como clasificada por seguridad nacional.
- Hay varios métodos para proteger datos según el uso que se les vaya a dar: el enmascaramiento oculta parte de un valor y no conserva su utilidad analítica, la seudonimización sustituye los identificadores por seudónimos y mantiene una vía controlada de revinculación, y la anonimización elimina la asociación con la persona. El cifrado y la tokenización sustituyen el valor completo.
- Los roles de protección de datos reparten responsabilidades: el propietario decide la clasificación y establece los controles de la información, el custodio los aplica en el día a día, el responsable del tratamiento determina fines y medios, y el encargado trata los datos por su cuenta. Según el RGPD, el encargado no puede recurrir a un subencargado sin autorización previa por escrito del responsable.

3.4 Explain the importance of resilience and recovery in security architecture.

- Los sitios alternativos se eligen según el tiempo de recuperación y el coste: el sitio frío solo tiene espacio, energía y controles ambientales; el templado añade equipos sin software ni datos actuales; el activo está plenamente operativo, y el espejo replica en tiempo real. Además, el sitio debe estar en una zona que no sufra los mismos riesgos naturales que el principal.
- La diversidad de plataformas, como usar distintos fabricantes, hardware o hipervisores, evita que una sola vulnerabilidad compartida provoque un fallo de modo común en todos los componentes. NIST advierte de que puede ser más aparente que real si los productos comparten componentes, y de que puede aumentar la superficie de ataque y los costes de gestión, por lo que debe analizarse.
- La redundancia elimina puntos únicos de fallo: el balanceo de carga reparte el tráfico, los clústeres permiten que otro nodo asuma el servicio y el escalado automático añade o quita capacidad según la demanda. En energía, las fuentes duales cubren el fallo de una fuente, el UPS da autonomía breve para un apagado ordenado y el generador cubre cortes largos.
- El almacenamiento resiliente combina RAID, replicación e instantáneas. La replicación síncrona copia en tiempo real al sitio de DR y evita perder escrituras confirmadas; la asíncrona introduce un retraso ligado al RPO. Las instantáneas son copias de un momento dado que dependen de los datos origen, por lo que no sustituyen a una copia separada.
- Una política de copias define su alcance (completas, incrementales o diferenciales), la frecuencia ligada al RPO y la retención. Las copias inmutables o sin conexión resisten al ransomware que borra o cifra las accesibles, y solo las pruebas de restauración y la verificación de integridad con hashes demuestran que se pueden recuperar.

4. Security Operations

27–27%

4.1 Given a scenario, apply mitigating controls, techniques, and solutions to secure the environment.

- La segmentación divide la red en zonas aisladas, con VLAN, subredes o redes físicas separadas, y controla el tráfico entre ellas con cortafuegos, routers o reglas en la nube. Reduce la superficie de ataque, frena el movimiento lateral y protege activos críticos como sistemas de pago o dispositivos IoT y OT.
- Los controles de acceso deciden quién y qué puede usar un recurso y con qué permisos. Las ACL enumeran las [illegible] El mínimo privilegio limita los permisos a lo necesario, por ejemplo obligando a los administradores a usar cuentas sin privilegios para el correo y la navegación.
- El bastionado [illegible] aplicar parches, [illegible] servicios, puertos y protocolos innecesarios [illegible] por defecto [illegible] como los CIS Benchmarks, sirven de línea base para configurar de forma coherente sistemas operativos y aplicaciones.
- El sandboxing ejecuta código no fiable en un entorno aislado y controlado, como una máquina virtual, un contenedor o el sandbox del navegador [illegible] y los sistemas de detección lo usan para analizar adjuntos y URL antes de entregarlos.
- La tecnología de engaño coloca señuelos [illegible] atacante: honeypots, honeynets, honeyfiles y honeytokens [illegible] falsas que generan alertas al usarse. Requieren aislamiento de producción.

4.2 Explain the security implications of proper hardware, software, and data asset management.

- El ciclo de vida de un activo empieza antes de la compra: en la planificación y la adquisición se definen requisitos [illegible] se registra con número de serie, ubicación y configuración base; durante la operación [illegible] exige una evaluación de riesgos previa.
- A cada [illegible] el SBOM del software [illegible] autorizados para evitar falsificaciones [illegible]
- Al retirarlo se sanean sus datos con clear, purge o destroy según la sensibilidad y el destino del soporte, y se da de baja del inventario.

4.3 Given a scenario, perform tasks associated with vulnerability management.

- Las vulnerabilidades se identifican con varios métodos complementarios: el análisis de vulnerabilidades de hosts y redes; el análisis estático del código fuente (SAST), que señala fallos como la inyección SQL con archivo y línea, y la CSPM, que vigila de forma continua la configuración y los permisos de los servicios de nube. SAST no ve problemas de configuración que no estén en el código.
- La puntuación base CVSS mide la gravedad intrínseca de una vulnerabilidad; para priorizar hay que completarla con métricas de amenaza, como la explotación activa, y de entorno, como la criticidad del sistema y los controles existentes. El catálogo KEV de la CISA señala lo que ya se explota, y en un informe de pentest se atiende primero lo que da control de sistemas críticos.
- Ante una vulnerabilidad se puede aceptar, mitigar, transferir o evitar el riesgo. Aplicar el parche o actualizar es lo único que elimina el fallo sin perder funcionalidad; si no hay parche, se mitiga con controles compensatorios como la segmentación de red. Las excepciones al plan de mantenimiento se documentan, se vigilan y se revisan con regularidad.
- Verificar una corrección significa comprobar que el parche está instalado y ha surtido efecto (a veces exige reiniciar), que los [illegible] mecanismo de prueba original; un resultado de otra herramienta o perfil no es comparable.
- Los informes de vulnerabilidades se adaptan a cada destinatario e incluyen un plazo de acción. Hacia fuera, una política de divulgación de vulnerabilidades indica dónde informar, qué sistemas y pruebas están autorizados y promete no emprender acciones legales contra la investigación de buena fe; un bug bounty añade pagos por hallazgos válidos.

4.4 Explain security alerting and monitoring concepts and tools.

- La monitorización cubre sistemas, aplicaciones e infraestructura. Los registros del sistema operativo recogen eventos del sistema y auditoría (inicios de sesión, accesos a archivos, cambios de cuentas) y sirven para investigar un host concreto. Los registros de aplicación muestran qué hizo cada usuario dentro de la aplicación, algo que en conexiones cifradas solo la propia aplicación puede registrar.
- Las actividades de monitorización incluyen agregar y normalizar registros en un punto central, generar alertas, analizar, archivar e informar. En el archivo, la retención es rutinaria y la preservación conserva registros que se eliminarían por su interés para una investigación. El ajuste de alertas (tuning) reduce falsos positivos sin crear falsos negativos y debe revisarse periódicamente.
- Las herramientas de monitorización incluyen benchmarks de configuración como los de CIS, el SIEM que centraliza y correlaciona registros, antivirus, DLP, analizadores de vulnerabilidades, orquestación y analizadores de paquetes. La recopilación sin agente evita instalar software en cada host, pero envía más datos sin filtrar y puede exigir credenciales; con agentes se filtra en origen a cambio de mantenerlos.
- NetFlow exporta registros de flujos (direcciones IP, recuentos de paquetes y bytes) sin el contenido de los paquetes. SNMP permite supervisar y gestionar dispositivos, y SNMPv3 añade autenticación y cifrado. Syslog transporta mensajes de eventos a un colector central. SCAP estandariza el formato de listas de comprobación y datos de vulnerabilidades (CVE, CPE, CVSS, OVAL, XCCDF) para evaluarlas automáticamente.
- Las alertas automáticas permiten reaccionar en minutos a eventos de interés, como la asignación de privilegios a una cuenta, en lugar de esperar a una revisión manual. Se basan en filtrar automáticamente los registros conocidos y [illegible] umbrales sobre una línea base de actividad normal, por ejemplo un aumento brusco del volumen de correo saliente.

4.5 Given a scenario, apply concepts related to identity and access management.

- El alta de cuentas exige una solicitud aprobada y permisos basados en una autorización válida para las funciones del usuario. La baja debe estar ligada a los procesos de RR. HH.: se avisa a los gestores de cuentas ante bajas y traslados, se deshabilitan las cuentas que ya no se necesitan y se cambian las credenciales de las cuentas compartidas cuando alguien sale del grupo.
- Los permisos se asignan según el mínimo privilegio: solo el acceso necesario para las tareas actuales. Hay que revisarlos periódicamente y retirar los que sobran tras un traslado para evitar la acumulación de privilegios. La segregación de funciones reparte tareas incompatibles, como crear proveedores y aprobar pagos, entre roles distintos para impedir el fraude sin colusión.
- La verificación de identidad (identity proofing) recoge, valida y verifica información para confiar en la identidad que declara una persona: resolución de la identidad, validación de las pruebas y atributos, verificación de que el solicitante es su titular e inscripción. Los niveles IAL1 e IAL2 admiten procesos remotos; el IAL3 exige una sesión presencial con un agente formado y biometría.
- La federación transmite información de identidad y autenticación entre sistemas de dominios distintos: el proveedor de identidad (IdP) autentica al usuario y envía una aserción al usuario de confianza (RP) según un acuerdo de confianza. El RP valida la firma con la clave del IdP esperado, comprueba que es el destinatario y rechaza aserciones reutilizadas.
- El SSO permite usar una cuenta y sus autenticadores en varias aplicaciones, normalmente mediante un protocolo de federación. SAML intercambia aserciones XML entre socios; OAuth 2.0 concede a una aplicación de terceros acceso limitado mediante tokens, sin compartir la contraseña; LDAP da acceso al directorio y su bind simple con contraseña debe ir protegido con TLS (StartTLS).

4.6 Given a scenario, apply automation and orchestration solutions to secure operations.

- La automatización y los scripts se aplican al aprovisionamiento de usuarios (altas, cambios y bajas según RR. HH.), al aprovisionamiento de recursos, a la gestión del estado deseado (mantener la configuración aprobada), a la detección de anomalías y a la gestión de tickets, por ejemplo creando y asignando tickets automáticamente cuando salta cierto tipo de alerta.
- Antes de automatizar hay que valorar salvaguardas (aprobación humana para acciones de alto impacto), la lógica y la complejidad de los flujos, el coste, los riesgos de proceso como los falsos positivos que paran servicios, y el despliegue: los cambios automatizados se prueban, validan y documentan fuera de producción y siguen el control de cambios.
- La IA en operaciones de seguridad incluye agentes que ejecutan acciones mediante herramientas, chatbots que ayudan a los analistas, análisis predictivo y líneas base aumentadas con IA que aprenden el comportamiento normal. Los agentes necesitan permisos mínimos y aprobación humana para acciones de alto impacto, y las líneas base dependen de que los datos de entrenamiento estén limpios.
- La automatización busca resultados concretos: eficiencia y ahorro de tiempo, aplicar líneas base de configuración [illegible] la revisión humana de las decisiones.
- En CI/CD, la integración continua automatiza compilación y pruebas, la entrega continua [illegible] y deja manual el paso a producción, y el despliegue continuo automatiza también la producción. La canalización amplía la superficie de ataque, así que exige secretos fuera del código y en un gestor dedicado, mínimo privilegio, revisión de cambios e integridad de artefactos.

4.7 Summarize concepts associated with incident response activities.

- La preparación se hace antes del incidente: políticas con funciones y autoridades definidas (quién puede desconectar sistemas), procedimientos en forma de playbooks, formación del personal y pruebas del plan. Los ejercicios de simulación de mesa se basan en la discusión sin tocar sistemas, mientras que los ejercicios funcionales y las simulaciones ponen al equipo a actuar en un entorno simulado.
- La identificación detecta y confirma incidentes a partir de alertas y supervisión continua, avisos internos, avisos externos [illegible] para decidir si se declara un incidente.
- La investigación [illegible] y mantener la integridad de los datos. La cadena de custodia [illegible] normalmente se borrarían, y el e-discovery exige localizar y entregar la información solicitada en un litigio sin alterarla, suspendiendo su borrado programado.
- La contención impide que un incidente se extienda: cuarentena de malware, aislamiento de equipos en redes de remediación o detención de contenedores infectados. Debe coordinarse, usando canales fuera de banda si el atacante puede vigilar las comunicaciones, y conviene evitar apagar equipos salvo que no puedan desconectarse, porque se pierde la evidencia en memoria.
- En una extorsión, pagar a los atacantes no garantiza recuperar los archivos ni que los datos robados no se publiquen. Antes de decidir conviene consultar a las fuerzas de seguridad, que pueden conocer descifradores ya disponibles, y preservar la evidencia.

4.8 Given a scenario, use data, artifacts and sources to support a security investigation.

- Cada tipo de registro responde a preguntas distintas: los de autenticación muestran origen, usuario, resultado y hora de cada intento; los de auditoría, cambios de cuentas y accesos a archivos; los de aplicación, peticiones y respuestas; los de red, conexiones; los de acceso físico, entradas a instalaciones; y los metadatos, datos como autor o fecha de modificación de un archivo.
- Las fuentes de datos de una investigación se eligen según la pregunta: los registros NetFlow o IPFIX resumen quién habló con quién y cuántos bytes durante largos periodos; las capturas de paquetes guardan el contenido, pero poco tiempo; los análisis de vulnerabilidades muestran debilidades; la videovigilancia registra la presencia física; y los informes automáticos y paneles resumen lo que recogen las herramientas de seguridad.
- La integridad de archivos y registros permite confiar en ellos como evidencia. Los hash detectan cualquier cambio, el software de comprobación de integridad compara los hash de los archivos críticos, y los registros se protegen enviándolos a un sistema separado, limitando el acceso a las herramientas de auditoría y usando protección criptográfica como hash firmados.
- Una imagen del sistema conserva la evidencia: el volcado de memoria captura datos volátiles que se pierden al apagar, como malware residente en memoria; la copia bit a bit duplica todo el soporte, incluidos archivos borrados y espacio slack, y se verifica con hash; y la instantánea guarda el estado de una máquina virtual o un volumen en la nube en un momento dado.
- Una investigación implica a partes no técnicas: el departamento jurídico revisa planes y contratos y orienta cuando un incidente puede acabar en juicio o exige decisiones como retrasar la contención; recursos humanos interviene si se sospecha de un empleado; los auditores ayudan a estimar el impacto económico y la seguridad física facilita el acceso y la custodia de pruebas.

5. Security Program Management and Oversight

14–14%

5.1 Explain the importance of governance, risk, and compliance artifacts.

- Las guías orientan sin imponer: los benchmarks (como los CIS Benchmarks) son recomendaciones de configuración prescriptivas y consensuadas para bastionar sistemas; los avisos de seguridad informan de vulnerabilidades nuevas con productos afectados y mitigaciones; y una arquitectura de referencia es un modelo conceptual neutral que sirve de base para diseñar arquitecturas concretas.
- Los estándares fijan requisitos obligatorios y medibles. Una línea base de controles es el conjunto mínimo de controles para un sistema de impacto bajo, moderado o alto; un estándar de contraseñas alineado con NIST SP 800-63B-4 prioriza la longitud y la lista de bloqueo y prohíbe reglas de composición, caducidad periódica sin compromiso y pistas. Los RFC son documentos de estándares del IETF.
- Los procedimientos (SOP, runbooks, playbooks) explican paso a paso cómo realizar un proceso técnico y se derivan de la política y el plan. Conviene documentarlos para los incidentes más comunes y para procesos urgentes, probarlos o ejercitarlos periódicamente para verificar que siguen siendo exactos y usarlos para formar al personal nuevo.
- El plan de continuidad del negocio (BCP) mantiene los procesos de negocio, como las nóminas, durante y después de una interrupción y puede limitarse a las funciones prioritarias. El plan de recuperación ante desastres (DRP) se centra en los sistemas: traslada su operación a un sitio alternativo cuando la instalación principal queda inaccesible, y luego cada sistema se recupera con su plan de contingencia.
- Las políticas recogen las reglas de alto nivel de la organización. Una política de divulgación de vulnerabilidades indica a investigadores externos el alcance, los métodos no autorizados, cómo informar y el compromiso de no actuar legalmente contra la investigación de buena fe; una política de eliminación de datos asocia cada nivel de clasificación a un método mínimo de saneamiento (borrado, purga o destrucción).

5.2 Explain the impact of risk management processes on the security of the organization.

- La identificación de riesgos empieza por inventariar los activos que sustentan la misión y valorarlos más allá de su coste de reposición, porque sin esa información no se puede cuantificar el impacto. Después se analizan amenazas, vulnerabilidades y consecuencias. Cada riesgo registrado tiene un propietario que responde de él y elige la respuesta, y no puede delegar su seguimiento en un gestor de riesgos.
- La categorización según FIPS 199 asigna a cada objetivo (confidencialidad, integridad, disponibilidad) un impacto potencial BAJO, MODERADO o ALTO, y un sistema toma el valor más alto de sus tipos de información en cada objetivo. Para puntuar, la escala semicuantitativa (0-100 en tramos) se traduce fácilmente a niveles cualitativos y permite comparar riesgos, aunque cada tramo debe estar bien definido.
- El análisis de riesgos combina probabilidad e impacto. La probabilidad de amenazas adversarias se basa en intención, capacidad y objetivos; la de amenazas no adversarias, en datos históricos y empíricos, teniendo en cuenta los controles ya desplegados. El análisis cualitativo usa niveles no numéricos que facilitan la comunicación, el cuantitativo usa cifras con significado propio y respalda mejor los análisis coste-beneficio.
- El registro de riesgos es el repositorio central de los riesgos actuales, tanto aceptados como en mitigación, con su descripción, probabilidad, impacto, respuesta, propietario y estado. Sirve para comunicar: los registros de cada área se normalizan y agregan en uno empresarial y se priorizan en un perfil para la dirección. Debe revisarse de forma continua, también los riesgos aceptados.
- Hay cuatro respuestas al riesgo: aceptarlo cuando está dentro de la tolerancia, evitarlo eliminando o cambiando la actividad o tecnología que lo genera; mitigarlo con controles que reduzcan probabilidad o impacto; y transferirlo o compartirlo con un tercero, que desplaza la responsabilidad pero no reduce la probabilidad ni las consecuencias.

5.3 Explain the processes associated with third-party risk.

- La gestión de terceros tiene límites: la dependencia de un proveedor (entornos propietarios, coste de migrar), la jurisdicción y la regulación aplicables, la falta de visibilidad sobre los controles del proveedor, la dependencia de una única fuente o región y los recursos disponibles. Se compensan con interfaces genéricas, planes de salida, auditorías independientes de terceros y supervisión continua.
- La selección de proveedores empieza con la diligencia debida: solicitudes de información (RFI) y cuestionarios para filtrar candidatos y conocer su postura de riesgo. Después se publica una declaración de trabajo con una solicitud de propuesta (RFP) o de presupuesto (RFQ), y las respuestas se evalúan con criterios de seguridad, vigilando que ningún evaluador tenga conflictos de intereses.
- Cada acuerdo cumple un papel: el SLA compromete al proveedor con niveles de rendimiento, responsabilidades e informes; la SOW detalla el trabajo y los entregables del contratista; el MOU recoge un entendimiento mutuo sin pagos ni dependencias, mientras que el MOA documenta apoyo con o sin reembolso, y el NDA delimita la información que no puede divulgarse.
- La supervisión de proveedores continúa después del contrato: un inventario o registro de proveedores con los productos, sistemas que los usan y su criticidad; revalidación periódica del cumplimiento de los requisitos de seguridad mediante certificaciones, visitas, evaluaciones de terceros o autodeclaraciones, con un rigor proporcional a la criticidad, y cláusulas contractuales sobre auditoría e intercambio de información.

5.4 Summarize elements of effective security compliance.

- Las Guías de Cumplimiento (ROE) de un equipo rojo definen el objetivo y lista de exclusión, actividades permitidas, manejo de datos, informes y firmas, además de los criterios para detener las pruebas si aparece un incidente o un intruso real.
- La formación de cumplimiento complementa la concienciación general con formación específica del puesto para quien maneja información sensible: se imparte antes de dar acceso a los sistemas y se repasa periódicamente.
- La supervisión del cumplimiento se apoya en pruebas documentadas. Las aceptaciones (acknowledgements) confirman que cada persona ha leído y acepta normas como las de conducta, antes de recibir acceso y de nuevo cuando cambian. Las declaraciones (attestations) afirman formalmente que se cumplen unos requisitos, como la AOC de PCI DSS, que resume los resultados de un ROC o un SAQ.
- El RGPD reconoce derechos al interesado: rectificación de datos inexactos, supresión o derecho al olvido, limitación del tratamiento (por ejemplo, mientras se verifica la exactitud impugnada) y oposición, además de retirar el consentimiento. El responsable determina los fines y medios del tratamiento, el encargado trata los datos por cuenta del responsable y siguiendo sus instrucciones.
- El cumplimiento legal afecta a la conservación de datos: los calendarios de retención deben atender las necesidades legales y regulatorias; ante un litigio previsto, la retención legal obliga a conservar sin alterar registros que normalmente se eliminarían, y el derecho de supresión del RGPD cede cuando una ley obliga a conservar ciertos datos. Obtener registros de terceros, como un ISP, suele exigir una orden judicial.

5.5 Explain concepts associated with audit and assessment activities.

- En una auditoría se recopilan evidencias examinando documentos y configuraciones, entrevistando a personas y probando controles, a menudo sobre una muestra representativa. Como referencias, MITRE ATT&CK documenta tácticas y técnicas del adversario, la Cyber Kill Chain ordena sus objetivos en fases y el Diamond Model ayuda a agrupar intrusiones relacionadas.
- El alcance de una evaluación fija qué sistemas se cubren, su tamaño y con qué frecuencia se evalúan. La frecuencia suele venir de requisitos de cumplimiento y del riesgo, y la prioridad combina la clasificación de impacto con la fecha de la última evaluación: si faltan recursos, se cubre primero lo prioritario y se reduce el alcance.
- Una auditoría interna la realiza por la propia organización (cumplimiento, comité de auditoría, autoevaluaciones), o externa, realizada por una segunda o tercera parte como un regulador o un auditor independiente.
- En una prueba de penetración los evaluadores intentan eludir las funciones de seguridad bajo reglas pactadas; según lo que sepan antes, el entorno es conocido, parcialmente conocido o desconocido. El reconocimiento pasivo observa el tráfico sin enviar sondas, mientras que el activo envía paquetes, es más rápido y puede activar alertas del IDS.
- El análisis de brechas compara el estado actual con el deseado, y el benchmarking lo compara con otras organizaciones o prácticas del sector.
- Las auditorías se apoyan en marcos y normas de distinto ámbito: del sector, como PCI DSS para los entornos con datos de tarjetas de pago; internacionales, como ISO/IEC 27001, que fija los requisitos de un sistema de gestión de la seguridad de la información certificable; y regionales, como el RGPD de la Unión Europea para los datos personales.

5.6 Given a scenario, apply security awareness concepts to improve organizational security.

- La formación en seguridad combina varios tipos: inicial, al incorporarse y antes de recibir acceso; continua, con sesiones periódicas y actualizaciones sobre amenazas recientes; dirigida, para grupos o funciones con más riesgo, como los que más fallan en simulaciones, y correctiva, impartida enseguida tras un hallazgo de auditoría o un incidente.
- La formación puede entregarse mediante un sistema de gestión del aprendizaje (LMS), que distribuye contenido y registra inscripción y finalización; portales de autoservicio con material a demanda; sesiones uno a uno, como la mentoría, o formatos uno a muchos, como clases presenciales o seminarios web en directo. Combinar varios mecanismos ayuda a mantener la atención.
- La eficacia de la concienciación se mide con métricas que van más allá de la asistencia o la finalización, como el porcentaje de usuarios que notifican un phishing simulado. Los informes de gestión presentan esas tendencias a la dirección, y la puntuación de riesgo del comportamiento ayuda a identificar a las personas con más riesgo humano para darles apoyo no punitivo.
- Los temas habituales de concienciación incluyen la ingeniería social y el phishing, el compromiso del correo empresarial (BEC), que verifica las peticiones de pago por un contacto ya conocido, la gestión de contraseñas, el trabajo remoto y BYOD, y los medios extraíbles: una memoria USB encontrada se entrega a seguridad o a TI sin conectarla.