SC-500 · CHEAT SHEET · CERTIFYDECK

# Microsoft Certified: Cloud and AI Security Engineer Associate

Contiene pesos oficiales y habilidades clave del temario de SC-500, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 120 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

## 1. Manage identity, access, and governance

20–25%

### Secure access to resources by using Microsoft Entra ID

- Privileged Identity Management ofrece acceso just-in-time: una asignación apta exige activar el rol (con MFA, justificación, incidencia o aprobación) y una activa concede los permisos sin acción. La configuración se define por rol; la directiva de acceso condicional de un contexto de autenticación se destina a los usuarios aptos, no al rol, porque durante la activación aún no lo tienen.
- Una directiva de acceso condicional es un si-entonces de asignaciones (usuarios, recursos, red, condiciones) y controles de concesión o sesión, que se evalúa tras el primer factor. Todas las directivas aplicables deben cumplirse y un bloqueo detiene la evaluación. El modo de solo informe evalúa sin aplicar ni pedir nada, y Require password change no se combina con otros controles.
- Las claves de acceso (FIDO2) pueden estar vinculadas al dispositivo (Microsoft Authenticator, llaves FIDO2) o sincronizadas; con atestación solo se admiten las vinculadas. Temporary Access Pass es un código de tiempo limitado para registrar métodos sin contraseña. Las fuerzas de autenticación del acceso condicional (MFA, sin contraseña, resistente al phishing) limitan qué combinaciones de métodos son válidas.
- Al registrar una aplicación se crea el objeto de aplicación (App registrations), plantilla global que solo existe en el inquilino de origen, y una entidad de servicio, su representación local que se crea en cada inquilino donde se usa (Enterprise applications). En la entidad de servicio se asignan usuarios y roles; la asignación de grupos no se propaga a grupos anidados.
- Los permisos delegados actúan en nombre de un usuario y solo alcanzan lo que este puede ver; los permisos de aplicación (roles de aplicación) dan acceso sin usuario y solo los consiente un administrador. Se recomienda limitar el consentimiento de usuario a editores verificados y permisos de bajo impacto, y habilitar el flujo de consentimiento de administrador para las solicitudes.

### Secure secrets and keys by using Azure Key Vault

- Implementa un almacén de claves por aplicación, región y entorno para reducir el radio de impacto, y no lo uses como almacén de datos ni de configuración. Al crearlo, habilita el modelo de permisos de Azure RBAC y la protección de purga. Si se elimina, queda en eliminación temporal: el nombre sigue reservado y recuperarlo no restaura las asignaciones de roles.
- La eliminación temporal permite recuperar almacenes y objetos durante un periodo de retención que solo se fija al crear el almacén; una vez habilitada no se desactiva. La protección de purga, irreversible, impide purgar antes de que acabe la retención y la exigen servicios como Storage con claves administradas por el cliente. Completa la configuración con registro, Event Grid y Defender for Key Vault.
- Key Vault tiene un plano de control (gestionar el almacén, siempre con Azure RBAC) y un plano de datos (claves, secretos y certificados), autorizado con Azure RBAC, el modelo recomendado, o con directivas de acceso heredadas. Usa roles como Key Vault Secrets User en el ámbito del almacén; Key Vault Contributor no da acceso a datos y, con directivas de acceso, puede concederse ese acceso.
- El cortafuegos de Key Vault está deshabilitado por defecto; al habilitarlo puedes permitir IP públicas, subredes con el punto de conexión de servicio Microsoft.KeyVault o solo puntos de conexión privados deshabilitando el acceso público. La excepción de servicios de confianza solo admite los servicios de la lista (Azure DevOps no está en ella) y sigue vigente aunque el acceso público esté deshabilitado.
- La directiva de rotación de claves crea versiones nuevas con material nuevo; los servicios deben usar el URI sin versión y mantener habilitadas ambas versiones hasta volver a encapsular las claves de datos. Los certificados de Key Vault crean una clave y un secreto con su nombre, se gestionan con una directiva (autoRenew o emailContacts) y no deben guardarse como secretos.

### Implement governance to enforce security and regulatory compliance

- Cada definición de Azure Policy tiene un solo efecto: deny rechaza creaciones o actualizaciones con un 403, denyAction bloquea eliminaciones, audit y auditIfNotExists informan, y modify y deployIfNotExists pueden corregir recursos existentes con una tarea de corrección y una identidad administrada. Las asignaciones superpuestas se evalúan por separado y el resultado es el más restrictivo; agrupa definiciones en iniciativas para asignarlas juntas.
- El panel de cumplimiento normativo de Defender for Cloud evalúa los recursos frente a los controles de cada estándar asignado (iniciativas de Azure Policy); MCSB viene activado y los demás estándares requieren un plan de pago. Los controles automáticos enlazan con la corrección, los manuales se atestiguan con pruebas, y los datos se pueden descargar como informe, exportar de forma continua o usar para lanzar automatizaciones.
- Defender for Cloud evalúa los recursos frente a estándares de seguridad (MCSB de forma predeterminada, estándares normativos y estándares personalizados) y genera recomendaciones con pasos de corrección. Con Defender CSPM puedes crear recomendaciones personalizadas en KQL para Azure, AWS y GCP y reglas de gobernanza que asignan propietario y fecha límite; las exenciones marcan recursos como mitigados o con riesgo aceptado.
- Los bloqueos de recursos protegen suscripciones, grupos de recursos y recursos: CanNotDelete (Eliminar) permite leer y modificar pero no eliminar, y ReadOnly (Solo lectura) impide además las actualizaciones. Prevalecen sobre los permisos de cualquier usuario, se heredan del ámbito primario, solo afectan al plano de control y crearlos requiere acceso a Microsoft.Authorization/locks, como el de Owner o User Access Administrator.
- Una asignación de roles de Azure combina una entidad de seguridad (usuario, grupo, entidad de servicio o identidad administrada), un rol y un ámbito (grupo de administración, suscripción, grupo de recursos o recurso) que heredan los ámbitos inferiores. Elige primero el rol de función de trabajo más restrictivo y reserva Owner, Contributor, User Access Administrator y Role Based Access Control Administrator, que son roles con privilegios.

## 2. Secure storage, databases, and networking

25–30%

### Implement security for storage accounts

- Una cuenta de almacenamiento se refuerza con la transferencia segura (rechaza HTTP), una versión mínima de TLS, sin acceso anónimo (AllowBlobPublicAccess en false prevalece sobre los contenedores) y sin clave compartida, requisito del acceso condicional. El cifrado de infraestructura solo se activa al crear la cuenta, y las claves administradas por el cliente exigen eliminación temporal y protección de purga en el almacén.
- El cortafuegos de Azure Storage admite reglas de red virtual, reglas de red IP (solo direcciones públicas y sin efecto en la misma región), reglas de instancia de recurso y excepciones de servicios de confianza. Las reglas solo actúan con la acción predeterminada en Deny y solo afectan al plano de datos. Las instancias de recurso y excepciones siguen vigentes aunque se deshabilite el acceso público.
- Defender for Storage ofrece supervisión de actividad sin habilitar registros, detección de amenazas a datos confidenciales y análisis de malware al cargar o a petición. Se habilita por suscripción o por cuenta, y una cuenta puede invalidar la configuración de la suscripción. Los resultados llegan como etiquetas de índice, alertas, eventos de Event Grid o registros de Log Analytics, y los blobs malintencionados pueden eliminarse temporalmente.
- El acceso a datos se concede con roles de datos de Azure RBAC (Storage Blob Data Reader, Contributor, Owner, Delegator) y SAS. El SAS de delegación de usuario se firma con credenciales de Entra y se revoca al revocar las claves de delegación; los SAS de servicio pueden asociarse a una directiva de acceso almacenada para revocarlos. Una directiva de expiración de SAS con Block deniega los SAS fuera de su límite.

### Implement security for databases

- En Azure SQL, el firewall IP de nivel de servidor y de base de datos (este solo con T-SQL), las reglas de red virtual y los puntos de conexión privados controlan el acceso entrante; Allow Azure services admite cualquier recurso de Azure. Deshabilitar el acceso público deja solo los puntos de conexión privados. La autenticación solo de Microsoft Entra bloquea la de SQL y exige antes un administrador de Entra.
- La auditoría de Azure SQL Database se define en el servidor (se aplica a todas las bases de datos) o en cada base de datos, y envía registros a almacenamiento, Log Analytics o Event Hubs; detrás de un firewall exige identidad administrada. En SQL Managed Instance se usa una configuración de diagnóstico y CREATE SERVER AUDIT TO EXTERNAL_MONITOR. Las operaciones de soporte de Microsoft se auditan por separado.
- Defender for Databases agrupa cuatro planes: Azure SQL Databases (evaluación de vulnerabilidades y Advanced Threat Protection), SQL Servers on Machines (máquinas virtuales con SQL e instancias de Azure Arc), Open-Source Relational Databases (PostgreSQL, MySQL y Amazon RDS) y Azure Cosmos DB. Activar el plan Databases habilita los cuatro; para proteger solo algunas máquinas con SQL se deshabilita en la suscripción y se habilita por recurso.

### Implement security for Azure network services

- Un grupo de seguridad de red filtra el tráfico con reglas con estado que se procesan por prioridad; en la entrada se evalúa primero el de la subred y después el de la interfaz, y ambos deben permitir el tráfico. Los grupos de seguridad de aplicaciones agrupan interfaces de una misma red virtual para escribir reglas sin direcciones IP, y las etiquetas de servicio sustituyen a los prefijos de los servicios de Azure.
- Azure Virtual Network Manager aplica reglas de administración de seguridad a grupos de red dentro de su ámbito, y se evalúan antes que los grupos de seguridad de red. Allow deja que el grupo de seguridad de red decida, mientras que Always Allow y Deny terminan la evaluación; las excepciones se crean con reglas de prioridad más alta, y la configuración solo surte efecto al desplegarla en las regiones.
- Un hub virtual protegido es un hub de Virtual WAN con directivas de seguridad y enrutamiento de Azure Firewall Manager, sin rutas definidas por el usuario. La intención de enrutamiento envía al cortafuegos, NVA o SaaS del hub el tráfico de internet, el privado o ambos; es la única forma de inspeccionar el tráfico entre hubs y la ruta 0.0.0.0/0 no se propaga entre hubs.
- Las conexiones VPN de sitio a sitio y de red virtual a red virtual admiten una directiva IPsec/IKE personalizada por conexión con algoritmos y grupos DH concretos. En punto a sitio se elige entre certificados, RADIUS o Microsoft Entra ID, que solo funciona con OpenVPN y Azure VPN Client y permite acceso condicional y MFA; los certificados de cliente se revocan por huella digital.
- Microsoft Entra Private Access sustituye a la VPN: el cliente de Global Secure Access tuneliza hacia los FQDN e IP privados de Quick Access o de aplicaciones de Global Secure Access, y los conectores de red privada en Windows Server abren solo conexiones salientes. Cada aplicación es una aplicación empresarial con usuarios asignados y directivas de acceso condicional; un segmento por aplicación tiene prioridad sobre Quick Access.

## 3. Secure compute

20–25%

### Implement security for AI

- Los informes de gobernanza de acceso a datos de SharePoint combinan instantáneas (permisos de sitio, permisos por usuario o grupo, etiquetas de confidencialidad) con informes de actividad (vínculos de uso compartido y contenido compartido con Everyone except external users). Las evaluaciones de riesgo de datos de DSPM detectan el uso compartido excesivo y proponen correcciones como Restricted Content Discovery o el etiquetado automático.
- DSPM de Microsoft Purview se centra en los datos: qué hay, dónde está, quién accede y cómo se protege, también en aplicaciones y agentes de IA. AI observability hace inventario de aplicaciones y agentes de IA y de su riesgo, el explorador de actividades muestra las solicitudes y respuestas con información confidencial, y los objetivos de seguridad de datos guían la corrección con DLP y etiquetas.
- La protección en tiempo real de Microsoft Defender evalúa las invocaciones de herramientas de los agentes de Copilot Studio durante la ejecución y puede bloquearlas antes de que se ejecuten. La regla predeterminada solo audita; las reglas personalizadas bloquean por tipo de detección y agente, y lo auditado o bloqueado queda en BehaviorInfo para la búsqueda avanzada en Defender XDR.
- El acceso condicional para agentes evalúa el sujeto del token: el usuario en el flujo en nombre de, la identidad del agente o su plano técnico en el acceso solo de aplicación, y la cuenta de usuario del agente cuando actúa como usuario. Cada sujeto necesita su propia directiva, y apuntar a un plano técnico o a atributos de seguridad personalizados cubre también los agentes futuros.
- El radio de impacto de una identidad de agente es el alcance de recursos, datos y capacidades a los que llegaría un atacante si la comprometiera, y depende de sus permisos, sus orígenes de conocimiento y las acciones de su plano técnico. Las rutas de ataque muestran la explotación paso a paso; el riesgo se reduce limitando permisos (por ejemplo, Sites.Selected), orígenes y acciones.

### Implement security for servers and virtual machines (VMs)

- El cifrado del lado del servidor de Azure Disk Storage está siempre activo, pero no cubre discos temporales ni cachés; el cifrado en el host sí lo hace, cifra el flujo hacia el almacenamiento y es la opción recomendada para máquinas virtuales nuevas. Las claves administradas por el cliente se aportan con un conjunto de cifrado de disco, y Azure Disk Encryption tiene prevista su retirada.
- Azure Bastion es un servicio PaaS que ofrece RDP y SSH sobre TLS a las máquinas virtuales por su IP privada, sin IP pública ni agente en ellas. Las implementaciones dedicadas usan una subred exclusiva llamada AzureBastionSubnet; si le aplicas un grupo de seguridad de red, debes incluir todas las reglas requeridas, y la subred de destino debe permitir 3389 o 22 desde Bastion.
- El acceso a la máquina virtual just-in-time de Defender for Cloud bloquea los puertos de administración con reglas de denegación en el grupo de seguridad de red o en Azure Firewall y los abre solo para la IP, los puertos y el tiempo aprobados. Requiere máquinas de Resource Manager con grupo de seguridad de red o firewall, comprueba los permisos de Azure RBAC del solicitante y no corta las conexiones ya establecidas al vencer.
- Azure Arc-enabled servers representa en Azure los servidores locales o de otras nubes mediante Azure Connected Machine agent, que les da un identificador de recurso y una identidad administrada. Así se aplican Azure Policy, configuración de máquinas, Defender for Cloud y Microsoft Sentinel; los controles locales del agente, como la lista de extensiones permitidas, prevalecen sobre las restricciones de la nube.
- Defender for Servers se habilita preferentemente a nivel de suscripción, el plan 1 puede activarse por recurso, pero el plan 2 solo se puede deshabilitar por recurso. Las máquinas locales se incorporan mejor como servidores habilitados para Azure Arc, y en AWS y GCP el conector multinube despliega Arc automáticamente; en EC2 requiere el agente SSM.

### Implement security for application platform services

- Microsoft Defender for Containers cubre la gestión de la postura (detección sin agente y refuerzo del plano de control), la evaluación de vulnerabilidades sin agente de imágenes y nodos, la protección en tiempo de ejecución con el sensor de Defender y la cadena de suministro con implementación controlada. Azure Policy for Kubernetes aplica reglas de admisión, y las alertas se investigan también en Microsoft Defender XDR.
- En AKS, la autorización de Microsoft Entra ID con Azure RBAC usa roles integrados como Azure Kubernetes Service RBAC Reader, Writer, Admin y Cluster Admin, asignables por espacio de nombres. Deshabilitar las cuentas locales elimina la puerta trasera --admin no auditable, y los intervalos IP autorizados limitan qué direcciones llegan al servidor de API público; no se usan en clústeres privados.
- Azure Container Registry controla el acceso con roles de Azure RBAC como AcrPull, AcrPush y AcrDelete,; el usuario administrador está deshabilitado de forma predeterminada. Para la red, las reglas IP se aplican al punto de conexión público y los puntos de conexión privados usan la zona privatelink.azurecr.io; al deshabilitar el acceso público, los servicios de confianza necesitan la omisión de reglas.
- En Azure Container Apps, el aislamiento de internet se logra con un entorno interno, y la visibilidad de entrada de cada aplicación (externa o interna) decide quién llega a ella; las restricciones IP permiten o deniegan rangos, pero no ambos a la vez. Azure Container Instances admite identidades administradas para acceder a Key Vault sin credenciales y, dentro de una red virtual, usa una puerta de enlace NAT para la salida.
- Azure Functions protege los puntos de conexión HTTP por capas: HTTPS, claves de acceso, autenticación de App Service, API Management, red virtual y aislamiento. Para la entrada se usan restricciones de acceso o un punto de conexión privado, y la integración con red virtual solo cubre la salida; los secretos se guardan como referencias de Key Vault o se sustituyen por identidades administradas.

## 4. Manage and monitor security posture

20–25%

### Manage security posture by using Defender for Cloud

- Defender CSPM amplía el plan gratuito con el grafo de seguridad en la nube: análisis de rutas de ataque desde puntos de entrada externos, explorador de seguridad para consultas propias, priorización de riesgos, protección de activos críticos, gobernanza y recomendaciones personalizadas con KQL. Las rutas de ataque requieren el examen sin agente o la evaluación de vulnerabilidades de Defender for Servers.
- Defender for Cloud representa los marcos de cumplimiento como estándares de seguridad formados por controles que agrupan recomendaciones; el MCSB viene activado y otros estándares requieren un plan de pago. El panel de cumplimiento normativo muestra el estado por control, admite atestaciones manuales, informes PDF, exportación continua a Log Analytics y automatizaciones con Logic Apps.
- Los planes de protección de cargas de trabajo de Defender for Cloud se activan por suscripción y algunos, como Defender for Storage o Defender for SQL, también por recurso. Defender for Servers Plan 2 añade a Plan 1 el examen sin agente, el acceso just-in-time y la supervisión de integridad de archivos; Plan 1 se puede habilitar por recurso, Plan 2 no.
- Defender for Cloud conecta AWS y GCP con conectores nativos que usan autenticación federada sin credenciales de larga duración; en AWS, un conector de cuenta de administración incorpora automáticamente las cuentas miembro. Las máquinas locales se conectan con servidores habilitados para Azure Arc, y los conectores de AWS y GCP despliegan Arc en las máquinas de esas nubes.
- Defender for Servers usa Microsoft Defender Vulnerability Management para examinar las máquinas en modo sin agente, con instantáneas de disco en Plan 2 o Defender CSPM, o basado en agente mediante la integración con Defender for Endpoint en Plan 1 o Plan 2. El examen viene activado; los discos con claves del cliente requieren permisos de Key Vault y los resultados se exportan con Azure Resource Graph.

### Implement activity and event collection in Microsoft Sentinel

- Microsoft Sentinel se habilita sobre un área de trabajo de Log Analytics sin bloqueos de recursos y con plan de pago por uso o de compromiso; conviene un grupo de recursos dedicado y empezar con una sola área, añadiendo otras por región, inquilino o propiedad. En el portal de Defender hay un área principal, correlacionada con Defender XDR, y áreas secundarias; las consultas entre áreas usan workspace().
- Microsoft Sentinel usa roles de Azure, asignados preferiblemente en el grupo de recursos del área de trabajo: Reader para ver, Responder para administrar incidentes, Contributor para crear contenido e instalar soluciones, Playbook Operator para ejecutar cuadernos de estrategias y Logic App Contributor para editarlos. Las asignaciones son acumulativas y las reglas de automatización usan una cuenta de servicio con permisos explícitos.
- El centro de contenido de Microsoft Sentinel reúne soluciones, paquetes de conectores, reglas de análisis, consultas de búsqueda, analizadores, libros, listas de seguimiento y cuadernos de estrategias, y contenido independiente. Para usar un elemento de una solución hay que instalar la solución completa; las dependencias se instalan con Install with dependencies y el contenido activo creado no se sobrescribe al actualizar.
- Los conectores para recursos de Azure se basan en API, en la configuración de diagnóstico o en agentes. Los conectores de diagnóstico administrados por Azure Policy aplican una configuración a todos los recursos de un tipo en un ámbito; para los recursos existentes hay que crear una tarea de corrección. El conector de Defender for Cloud exige un plan de Defender, el rol Colaborador y ofrece sincronización bidireccional.
- Los conectores Syslog vía AMA y CEF vía AMA instalan Azure Monitor Agent en una máquina Linux, a menudo un reenviador, y filtran con reglas de recopilación de datos. El portal solo permite un nivel mínimo por instalación; la API admite niveles concretos. Un reenviador ajeno a Azure necesita Azure Arc. CEF va a CommonSecurityLog y syslog a Syslog; usar la misma instalación para ambos duplica datos.

### Implement Microsoft Security Copilot

- Las áreas de trabajo de Security Copilot segmentan el uso: cada una tiene su historial de sesiones, capacidad en SCU, roles Propietario y Colaborador, plugins y ubicación de almacenamiento de datos, que no se puede cambiar. Una capacidad solo sirve a un área de trabajo a la vez. Crear capacidad exige Colaborador o Propietario de Azure. El registro de auditoría y el enrutamiento de los agentes integrados son de todo el inquilino.
- Security Copilot tiene dos roles propios, Copilot owner y Copilot contributor, que no son roles de Microsoft Entra y no dan acceso a datos de seguridad: cada plugin exige sus roles, como Lector de Microsoft Sentinel. Algunos roles, como Administrador global o de seguridad, heredan el de propietario. Se recomienda asignar los roles a grupos asignables a roles y evitar dar roles privilegiados solo para usar Copilot.
- Los plugins amplían lo que Security Copilot y sus agentes pueden consultar o hacer, con autenticación en nombre del usuario para los de Microsoft. Los propietarios deciden quién agrega plugins personalizados para sí o para la organización y pueden restringir los preinstalados a propietarios, también en experiencias integradas. Los plugins con Set up se configuran por usuario y conviene validar los personalizados antes a nivel de usuario.
- Los agentes de Security Copilot automatizan tareas con desencadenadores, permisos, identidad y plugins; se recomienda crear una identidad de agente con Microsoft Entra Agent ID en lugar de usar una cuenta de usuario. Los agentes de partners que leen datos de productos de Microsoft requieren la aprobación de un Administrador global. Security Store gestiona la compra y la facturación, y el agente se configura y opera en Security Copilot.