SC-900 · CHEAT SHEET · CERTIFYDECK

Microsoft Certified: Security, Compliance, and Identity Fundamentals

Dominios, pesos oficiales y habilidades clave del temario de SC-900, para repasar antes del examen.

Nivel: Beginner Duración: 45 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Describe the concepts of security, compliance, and identity

10–15%

Describe security and compliance concepts

- En un entorno local la organización gestiona toda la pila; al pasar a IaaS, PaaS y SaaS el proveedor asume cada vez más capas (hosts y red, después sistema operativo y entorno de ejecución, y en SaaS toda la aplicación). Pase lo que pase el proveedor siempre es responsable de los datos, los dispositivos y la configuración.
- La defensa en profundidad usa varias capas de control (identidad, borde, red, host, aplicación y datos). Si una capa falla, las siguientes siguen protegiendo. Cada capa tiene sus propios controles.
- Confianza cero trata cada solicitud como hostil hasta verificarla. Se basa en tres principios: verificar de forma explícita, usar acceso con privilegios mínimos y asumir que ya ha habido una brecha. Se aplica a identidad, dispositivo, red, aplicación y datos.
- El cifrado hace ilegibles los datos sin la clave correcta. Se usa en tránsito (TLS) y en reposo, con claves gestionadas por el cliente o por el proveedor. Las claves deben custodiarse aparte, rotarse y revocarse.
- Cumplimiento es seguir leyes y estándares aplicables, que fija mínimos y no equivale a seguridad). Conceptos clave: residencia de los datos, soberanía de los datos y privacidad desde el diseño.

Define identity concepts

- Sobre aplicaciones en la nube, trabajo remoto, dispositivos personales y acceso de socios, el perímetro de red ya no es una frontera fiable, y la pregunta pasa a ser quién o qué realiza cada solicitud. Por eso la identidad es el nuevo perímetro. Hay personas, de dispositivos, cargas de trabajo y agentes de IA.
- La autenticación demuestra quién es cada uno. Se basa en algo que sabes, algo que tienes o algo que eres. La autenticación multifactor exige dos o más factores distintos y protege aunque el primero se vea comprometido.
- La autorización determina qué puede hacer cada identidad. Se basa en roles, permisos y atributos, y se evalúa después de una autenticación correcta.
- El principio de privilegio mínimo concede solo el acceso necesario, solo cuando hace falta y solo durante el tiempo justo. Reduce el daño que puede causar una cuenta comprometida.
- La seguridad de cero confianza aplica este principio a cada solicitud, sin dar nada por sentado.
- Un proveedor de identidades (IdP) crea, almacena y administra identidades y ofrece autenticación, autorización y aplicación de políticas. Se basa en estándares como SAML, OAuth 2.0 y OpenID Connect.
- Microsoft Entra ID es el servicio de administración de identidades y accesos basado en la nube de Microsoft, base de la familia Microsoft Entra. Cada suscripción a Microsoft 365, Azure o Dynamics ya incluye un inquilino de Entra, que contiene al directorio con usuarios, grupos, dispositivos y registros de aplicaciones y actúa como límite de seguridad y administración. Puede sincronizarse con AD DS, pero es independiente.
- Las identidades híbridas amplían el control de acceso a los recursos locales. Se logra con aprovisionamiento, sincronización entre Active Directory y Microsoft Entra ID, Microsoft Entra Cloud Sync usa un agente ligero para ello. El inicio de sesión puede resolverse con sincronización de hash de contraseña, autenticación directa o federación con AD FS.
- Microsoft Entra ID ofrece contraseñas, métodos telefónicos (SMS y llamada de voz), tokens OATH, Pase de acceso temporal, código QR para trabajadores de primera línea y métodos sin contraseña como Windows Hello para empresas, claves de acceso (FIDO2), Microsoft Authenticator y autenticación basada en certificados. Algunos sirven como factor principal y otros solo como secundario; las claves de acceso y los certificados son resistentes al phishing.
- La autenticación multifactor exige dos o más factores: algo que se sabe, algo que se tiene y algo que se es. Aunque la contraseña sea débil o esté expuesta, el factor adicional es difícil de obtener o duplicar. Microsoft Entra solicita MFA durante el inicio de sesión. Las aplicaciones heredadas que no admiten la autenticación moderna no pueden usar MFA.
- La protección de contraseñas impide el uso de contraseñas débiles y vulnerables. Las listas globales incluyen términos comunes y patrones predecibles. Las listas personalizadas añaden términos específicos de la organización, como nombres de productos o ubicaciones. Se aplica durante el restablecimiento de contraseña y el cambio de contraseña.
- El autoservicio de restablecimiento de contraseña permite a los usuarios restablecer sus contraseñas sin intervención del soporte técnico. Reduce la carga de trabajo del servicio de asistencia y mejora la experiencia del usuario. Se basa en métodos de autenticación registrados, como el teléfono o la aplicación Authenticator.
- El bloqueo inteligente de Microsoft Entra protege las cuentas de usuario frente a intentos de contraseña no válidos. Usa algoritmos para distinguir entre atacantes y usuarios legítimos. Los usuarios bloqueados pueden desbloquearse automáticamente o mediante autoservicio.

Describe authentication capabilities of Microsoft Entra ID

Describe access management capabilities of Microsoft Entra ID

- El acceso condicional es el motor de directivas de Microsoft Entra ID. Evalúa señales (usuario, ubicación, dispositivo, aplicación, riesgo) para decidir si se bloquea el acceso o se concede, quizá exigiendo MFA, un dispositivo compatible o un cambio de contraseña. Se aplica después de la autenticación principal.
- Los roles de Microsoft Entra controlan quién puede hacer qué en el inquilino. Se asignan a usuarios, grupos o entidades de servicio mediante ámbitos. Incluyen roles integrados y personalizados, y admiten controles de sesión.

Describe identity protection and governance capabilities of Microsoft Entra

- Microsoft Entra ID Governance ayuda a que las personas adecuadas tengan el acceso adecuado a los recursos adecuados mediante automatización, delegación y visibilidad. Cubre el ciclo de vida de la identidad (flujos de trabajo de incorporación, movimiento y baja), el acceso con privilegios (Privileged Identity Management) y las revisiones de acceso.
- Privileged Identity Management (PIM) administra, controla y supervisa el acceso con privilegios en Microsoft Entra ID y en otros servicios en la nube. Ofrece acceso just-in-time y limitado en el tiempo, aprobación, MFA, justificación y registros de auditoría.
- Microsoft Entra ID Protection detecta, investiga y corrige riesgos basados en identidad. Analiza señales como inicios de sesión sospechosos, credenciales filtradas y comportamientos anómalos. Puede activar directivas de acceso condicional o exigir acciones, como MFA o cambios de contraseña.

3. Describe the capabilities of Microsoft security solutions

35–40%

Describe core infrastructure security services in Azure

- Azure DDoS Protection defiende los recursos de Azure con direcciones IP públicas frente a ataques de denegación de servicio distribuido en las capas 3 y 4. Supervisa el tráfico de forma continua, ajusta sus umbrales automáticamente mediante perfiles de tráfico y ofrece métricas, análisis y alertas. Para proteger aplicaciones web en la capa 7 se combina con un firewall de aplicaciones web.
- Azure Firewall es un servicio de seguridad de red administrado en la nube: un firewall con estado, con alta disponibilidad integrada y escalabilidad en la nube. Filtra el tráfico por IP, puerto, protocolo y FQDN, usa inteligencia de amenazas, admite SNAT y DNAT y se administra de forma central con Azure Firewall Manager. Premium añade IDPS y TLS.
- Azure Web Application Firewall proporciona protección centralizada de las aplicaciones web frente a vulnerabilidades habituales, como la inyección de SQL y el scripting entre sitios. Se implementa con servicios como Application Gateway y Azure Front Door, usa reglas administradas y personalizadas, ofrece protección contra bots y puede funcionar en modo de detección o prevención.
- Una red virtual de Azure es una red privada y privada de red dedicada a tu suscripción, y se segmenta en subredes. Las subredes permiten aplicar reglas distintas a cada nivel, pero Azure enruta el tráfico entre ellas por defecto, así que se restringe con grupos de seguridad de red o aplicaciones virtuales de red. Varias redes virtuales se pueden conectar mediante peering.
- Un grupo de seguridad de red (NSG) filtra el tráfico entre recursos de Azure con reglas de permiso o denegación por origen, destino, puerto, protocolo y dirección. Las reglas se procesan por prioridad (el número más bajo primero) y el procesamiento se detiene en la primera coincidencia. Los NSG tienen estado y se pueden asociar a subredes o interfaces de red.

Describe security management capabilities of Azure

- Microsoft Defender for Cloud es una plataforma de protección de aplicaciones nativas de la nube (CNAPP) que protege recursos de Azure, AWS, GCP y locales. Combina administración de la posición de seguridad (CSPM), seguridad de DevOps y protección de cargas de trabajo (CWPP), y genera recomendaciones, alertas e incidentes que mejoran la seguridad en la nube.
- La administración de la posición de seguridad en la nube (CSPM) evalúa de forma continua los recursos de Azure, AWS y GCP y emite recomendaciones para reducir configuraciones incorrectas y riesgos. La puntuación segura resume la posición de seguridad: cuanto más alta, menor riesgo identificado. Las capacidades avanzadas, como la gobernanza de seguridad de Defender Cloud, incluyen estándares (puntos de referencia como el Microsoft cloud security benchmark, estándares de cumplimiento normativo y estándares personalizados) que definen controles y lógica de evaluación. Cuando un recurso no cumple un control, se genera una recomendación con los pasos de corrección, y el panel de cumplimiento normativo muestra el estado de cada estándar.
- La protección de cargas de trabajo en la nube se activa con planes de Defender para tipos de recurso concretos, como servidores, almacenamiento, bases de datos, contenedores, App Service o Key Vault. Estos planes aportan detecciones avanzadas que generan alertas de amenazas, y capacidades como el acceso Just-In-Time a máquinas virtuales o el examen de malware en almacenamiento.

Describe capabilities of Microsoft Sentinel

- Un SIEM recopila, agrega y analiza datos de aplicaciones, dispositivos, servidores y usuarios de toda la organización para detectar e investigar incidentes. SOAR actúa después: automatiza los flujos de respuesta a las alertas que genera el SIEM. Microsoft Sentinel es un SIEM nativo de la nube que además es plataforma SOAR, con reglas de automatización y libros de Azure Logic Apps.
- Las reglas de análisis de Microsoft Sentinel se ejecutan periódicamente sobre los datos recopilados y generan alertas, que se agrupan en incidentes. Hay reglas programadas, casi en tiempo real (NRT), de anomalías (que no generan alertas propias) y la detección Fusion de ataques de varias fases. La búsqueda de amenazas explora proactivamente lo que ninguna alerta ha señalado y UEBA detecta desviaciones de la línea base.

Describe threat protection with Microsoft Defender XDR

- Microsoft Defender XDR coordina de forma nativa la detección, la prevención, la investigación y la respuesta en puntos de conexión, identidades, correo y aplicaciones. Agrupa las alertas relacionadas en incidentes, permite buscar amenazas con consultas entre productos y puede contener ataques en curso mediante la interrupción automática.
- Microsoft Defender for Office 365 es la solución principal de seguridad de correo y colaboración de Microsoft 365 y se suma a las protecciones integradas de todos los buzones en la nube. Vínculos seguros verifica las URL al hacer clic, Datos adjuntos seguros detona los adjuntos en un entorno virtual y el entrenamiento de simulación de ataques ayuda a los usuarios a identificar y notificar los ataques de suplantación de identidad.
- Microsoft Defender for Endpoint es una plataforma de seguridad de puntos de conexión para prevenir, detectar, investigar y responder a amenazas avanzadas en Windows, macOS, Linux, Android e iOS. Incluye reducción de la superficie expuesta a ataques (prevención), protección de última generación, detección y respuesta de puntos de conexión (EDR) y funciones para gestionar vulnerabilidades.
- Microsoft Defender for Cloud Apps es un agente de seguridad de acceso a la nube (CASB) con funciones de CASB: Cloud Discovery descubre las aplicaciones en uso (TI en la sombra) y puntúa su riesgo, mientras que SSPM recomienda mejoras de configuración. Controla datos confidenciales, supervisa sesiones con el control de aplicaciones de acceso condicional y protege contra amenazas y ataques OAuth en aplicaciones.
- Microsoft Defender for Identity detecta, investiga y protege a las identidades usando señales de Active Directory local y de Microsoft Entra ID. Sus sensores se ejecutan en la infraestructura de identidad y envían solo las señales necesarias. Cubre reconocimiento, credenciales en peligro, movimiento lateral y dominio de AD, y evalúa la posición de seguridad, incluidas las rutas de movimiento lateral.

4. Describe the capabilities of Microsoft compliance solutions

20–25%

Describe Microsoft Service Trust Portal and privacy principles

- El Service Trust Portal es el sitio público de Microsoft para publicar informes de auditoría de auditores externos y documentos técnicos sobre cómo protegen los datos los servicios en la nube. Organiza el contenido en certificaciones y normativas, informes y documentos, recursos sectoriales y regionales y recursos de tu organización. Parte del contenido exige una cuenta de organización de Microsoft Entra.
- Microsoft explica su compromiso de privacidad en cuatro áreas: control de los datos, ubicación de los datos, seguridad de los datos y defensa de los datos. Puedes acceder a tus datos, modificarlos o eliminarlos, elegir dónde se almacenan y contar con cifrado en reposo y en tránsito. Microsoft no usa tus datos para publicidad y remite al cliente las solicitudes gubernamentales.

Describe compliance management capabilities of Microsoft Purview

- El portal de Microsoft Purview es una experiencia unificada para las soluciones de seguridad de datos, gobierno de datos y riesgo y cumplimiento, con un único punto de entrada para configuración, búsqueda y permisos. La página principal muestra tarjetas de las soluciones según tus permisos y suscripción, y el estado de cumplimiento procedente de Compliance Manager.
- Compliance Manager ayuda a evaluar y gestionar el cumplimiento, también en entornos multinube. Se organiza en controles (de Microsoft, propios o compartidos), evaluaciones, normativas y acciones de mejora, que se pueden asignar, probar y respaldar con pruebas. Sus recomendaciones no garantizan el cumplimiento: la organización debe validar sus propios controles.
- La puntuación de cumplimiento mide el avance en la realización de las acciones de mejora recomendadas dentro de los controles. Cada acción aporta puntos según el riesgo: las preventivas obligatorias valen más que las discrecionales, y las detectivas y correctivas valen menos. Sirve para entender tu situación y priorizar, y la puntuación inicial parte de la línea de base de protección de datos de Microsoft 365.

Describe information protection, data lifecycle management, and data governance capabilities of Microsoft Purview

- Microsoft Purview identifica contenido confidencial con varios tipos de clasificadores: tipos de información confidencial basados en patrones, entidades con nombre, coincidencia exacta de datos con valores con hash, clasificadores entrenables que aprenden de ejemplos, huellas digitales de plantillas y OCR para imágenes. El Explorador de datos muestra los elementos clasificados.
- El explorador de contenido muestra una instantánea actual de los elementos que tienen una etiqueta de confidencialidad, una etiqueta de retención o un tipo de información confidencial, y permite ver su ubicación. El explorador de actividad ofrece una vista histórica de las acciones sobre el contenido etiquetado, a partir del registro de auditoría unificado, y no funciona en tiempo real.
- Las etiquetas de confidencialidad clasifican y protegen el contenido con cifrado y marcas como marcas de agua o encabezados, y se guardan en los metadatos, por lo que acompañan al archivo. Las directivas de etiquetas las publican para usuarios o grupos concretos y pueden fijar etiqueta predeterminada, etiquetado obligatorio y justificación al reducir la etiqueta.
- La prevención de pérdida de datos (DLP) usa directivas para identificar, supervisar y proteger elementos confidenciales, como números de tarjeta, en Exchange, SharePoint, OneDrive, Teams, dispositivos y repositorios locales. Según la ubicación, puede mostrar una sugerencia, bloquear con o sin invalidación o mover el archivo a cuarentena.
- La administración de registros ayuda a cumplir obligaciones legales y normativas gestionando la retención, la declaración de registros y la eliminación. Los registros se declaran con etiquetas de retención; un registro normativo es aún más estricto, porque nadie puede quitar su etiqueta. Incluye plan de archivos, retención basada en eventos y revisión de eliminación.

Describe insider risk, eDiscovery, and audit capabilities in Microsoft Purview

- La administración de riesgos internos correlaciona señales para detectar riesgos malintencionados o involuntarios, como el robo de datos por usuarios que se marchan o las fugas de información. Usa plantillas de directivas, genera alertas que se evalúan y se convierten en casos, y protege la privacidad con seudonimización. Los casos pueden escalarse a eDiscovery.
- eDiscovery identifica, conserva, revisa y exporta contenido de Exchange, Teams, OneDrive, SharePoint y otros servicios como prueba en investigaciones y casos legales. Un caso agrupa búsquedas, retenciones y conjuntos de revisión, y sus miembros controlan el acceso. Las retenciones evitan la eliminación durante la investigación y los conjuntos de revisión permiten filtrar y etiquetar.
- La auditoría de Purview registra en un registro unificado miles de operaciones de usuarios y administradores, que se pueden buscar por actividad, usuario e intervalo de fechas. Auditoría (estándar) está habilitada de forma predeterminada; Auditoría (Premium) añade directivas de retención, conocimientos inteligentes y mayor ancho de banda para la API de actividad de administración.