

2. Design security operations, identity, and compliance capabilities

25–30%

Design solutions for security operations

- Microsoft Defender XDR correlaciona señales de puntos de conexión, identidades, correo y aplicaciones y aplica respuesta automática, mientras que Microsoft Sentinel es el SIEM y SOAR que recopila datos multinube y de terceros. Incorporar Sentinel al portal de Defender ofrece una cola de incidentes unificada, correlación entre Microsoft Purview Audit registra en el registro de auditoría unificado las operaciones de usuarios y administradores de los servicios de Microsoft, con directivas de retención por servicio, actividad o usuario y acceso por API para un SIEM. En Azure, la configuración de diagnóstico envía registros a Log Analytics, a almacenamiento inmutable o a Azure Arc representa servidores locales y de otras nubes como recursos de Azure, y el Azure Monitor Agent envía sus datos a Microsoft Sentinel según reglas de recopilación de datos. Sentinel ingiere registros de AWS desde S3 con OIDC y de GCP mediante Pub/Sub, y Defender for Cloud conecta AWS y GCP sin agente para CSPM y protege servidores en cualquier entorno.
- Microsoft Sentinel aporta SOAR con reglas de automatización, que etiquetan, asignan o cierran incidentes y lanzan playbooks, y con playbooks basados en Azure Logic Apps que se integran con sistemas externos. Defender XDR añade investigación y respuesta automatizadas con veredicto por evidencia e interrupción automática de ataques.
- La guía de Microsoft pide un plan de respuesta con roles definidos (líder técnico, enlace de comunicaciones, registrador) y elegir entre limpiar sobre la marcha o una corrección conjunta cuando el adversario está atrincherado.

En Microsoft Sentinel, las búsquedas parten de una hipótesis, guardan marcadores y generan reglas e incidentes

Design solutions for identity and access management

- Microsoft Entra Agent ID da a cada agente de IA una identidad propia, distinta de las de usuarios y cargas de trabajo, con blueprints, propietarios técnicos y patrocinadores del negocio. El acceso condicional se dirige al sujeto del token: el usuario en el flujo on-behalf-of, la identidad de agente o su blueprint en el acceso de aplicación y la cuenta de usuario del agente cuando actúa como usuario.
- Global Secure Access combina Microsoft Entra Internet Access, una puerta de enlace web segura para Internet y SaaS, y Private Access, que sustituye la VPN con acceso por aplicación a recursos híbridos y multinube. Defender for Cloud Apps controla sesiones SaaS en el navegador, los puntos de conexión privados y Azure Bastion evitan exponer PaaS e IaaS, y la federación de identidades de carga de trabajo elimina secretos.
- En identidad híbrida, la sincronización de hash de contraseñas es el método más sencillo y conviene activarla siempre como respaldo y para detectar credenciales filtradas; la autenticación de paso a través aplica los estados de cuenta locales y AD FS cubre requisitos no nativos. Cloud Sync sincroniza bosques desconectados con agentes Microsoft Entra External ID cubre dos escenarios: colaboración B2B con invitados en el inquilino de personal y CIAM ligeros. En multinube, Microsoft Entra ID centraliza el inicio de sesión en AWS con acceso condicional y PIM para consumidores en un inquilino externo separado. La configuración de acceso entre inquilinos controla el acceso de entrada y salida y puede confiar en la MFA y los dispositivos del socio; la conexión directa B2B sirve para canales compartidos de Teams. Verified ID emite credenciales verificables firmadas con DID.
- El acceso condicional es el motor de directivas de confianza cero. La evaluación continua de acceso permite que Exchange, SharePoint y Teams rechacen tokens vigentes ante eventos críticos o cambios de ubicación. ID Protection calcula el riesgo de usuario y de inicio de sesión, que se usa en directivas de acceso condicional con

Design solutions for secure privileged access

- El modelo de acceso empresarial amplía el modelo de niveles de AD a planos de control, administración y datos/cargas, más las rutas de acceso de usuarios y aplicaciones, e impide que un plano inferior controle uno superior. El acceso con privilegios se protege de extremo a extremo con cuentas, dispositivos e intermediarios
- PIM da acceso just-in-time a roles de Microsoft Entra, de Azure y a grupos, con aprobación, justificación, MFA y auditoría; los grupos que elevan a roles deben ser asignables a roles y exigir aprobación. La administración de derechos agrupa recursos en paquetes de acceso con aprobación y caducidad, también para externos, y las revisiones de acceso recertifican periódicamente grupos, aplicaciones y roles.
- El modelo de niveles de AD DS separa el nivel 0 (controladores, AD FS, AD CS, Entra Connect y lo que los gestiona), el nivel 1 (servidores y aplicaciones) y el nivel 2 (dispositivos de usuario), con PAW por nivel y sin reutilizar credenciales entre niveles. Defender for Identity detecta reconocimiento, movimiento lateral y control total
- La administración de inquilinos en la nube se protege con cuentas con privilegios solo en la nube, PIM, MFA del dominio, y la recuperación del bosque parte de copias de confianza de varios controladores de escritura, resistente a phishing y al menos dos cuentas de emergencia con FIDO2 y Administrador global activo permanente.
- Azure Lighthouse delega suscripciones a proveedores con control del cliente, Defender for Cloud Apps evalúa la postura de las aplicaciones SaaS y el CIEM dentro de Defender CSPM para descubrir identidades humanas y de carga de trabajo con permisos excesivos o inactivas en Azure, AWS y Google Cloud. Hay que conectar cada nube y activar Permissions Management (CIEM); el explorador de seguridad y las rutas de ataque muestran quién llega

Design solutions for regulatory compliance

- Cada riesgo o requisito normativo se traduce en una directiva de gobernanza con identificador, riesgo asociado, declaración orientada a resultados y la herramienta que la impone. MCSB ofrece controles ya asignados a CIS, NIST y PCI DSS, y la imposición se automatiza con Azure Policy, Defender for Cloud, Purview y Entra ID Governance.
- Microsoft Purview cubre requisitos normativos con Compliance Manager (evaluaciones, acciones de mejora y pruebas multinube con Defender for Cloud), etiquetas de confidencialidad y DLP para proteger datos, y retención para conservar o eliminar contenido. Las etiquetas de retención actúan por elemento y viajan con él; si hay conflicto, Azure Policy evalúa las propiedades de los recursos frente a reglas JSON; las definiciones se agrupan en iniciativas y se asignan en grupos de administración para que las hereden las suscripciones. Los efectos deny, modify, deployIfNotExists y audit permiten bloquear, corregir o informar; las tareas de corrección arreglan recursos
- El panel de cumplimiento normativo de Defender for Cloud evalúa de forma continua los recursos de Azure, existentes con una identidad administrada, y las exenciones registran excepciones.
- AWS y GCP frente a estándares como MCSB, ISO 27001 o PCI DSS, agrupados en controles. Los controles no automatizables se atestiguan con evidencias, los informes sirven a los auditores y los datos se exportan, se automatizan con Logic Apps y aparecen en Compliance Manager.

3. Design security solutions for infrastructure

25–30%

Design solutions for security posture management in hybrid and multicloud environments

- Al activar Defender for Cloud se aplica Microsoft cloud security benchmark, cuyas recomendaciones integradas alimentan la puntuación de seguridad agrupadas en controles. Un control solo suma puntos cuando sus recursos cumplen todas sus recomendaciones; las recomendaciones en versión preliminar no cuentan, y Cloud Secure Score de Microsoft Secure Score, en el portal de Microsoft Defender, mide la postura de identidades, dispositivos, aplicaciones y datos de Microsoft 365 y ordena acciones recomendadas por puntos, dificultad e impacto. Las acciones resueltas con terceros o mitigaciones alternativas suman puntos y las de riesgo aceptado no; el acceso se delega con roles personalizados de Defender Unified RBAC.
- Defender for Cloud ofrece administración de la postura en Azure, AWS y Google Cloud mediante conectores nativos con credenciales federadas, y en servidores locales mediante Azure Arc. Defender CSPM añade análisis de rutas de ataque, explorador de seguridad, EASM y reglas de gobernanza, y las alertas se integran en el portal de Microsoft Defender.
- La protección de cargas de trabajo (CWPP) de Microsoft Defender for Cloud se activa por planes: Defender for Servers protege máquinas de Azure, AWS, GCP y locales, Defender for Storage analiza malware y detecta abuso de tokens SAS sin registros de diagnóstico; Defender for Containers aporta evaluación de vulnerabilidades, protección en tiempo de ejecución e implementación controlada, y Defender for APIs protege las API de API Management. Manager, de modo que se gobiernan con Azure Policy, RBAC y Defender for Cloud como cualquier recurso de Azure. Los conectores de AWS y GCP de Defender for Cloud implementan Arc automáticamente. Para recursos de

Specify requirements for securing identity and digital endpoints

- Microsoft Defender for Endpoint protege servidores Windows Server y Linux; Defender for Servers lo integra en Defender for Cloud e incorpora automáticamente la extensión en máquinas de Azure y habilitadas para Arc. Con otro antimalware, Defender Antivirus debe quedar en modo pasivo. La ubicación de los datos se fija en la configuración.
- Para móviles se combinan directivas de cumplimiento de Intune con acceso condicional en dispositivos inscritos, inicial y el sensor de Linux usa eBPF, sin módulos de kernel.
- Directivas de protección de aplicaciones (que no requieren inscripción) y Defender for Endpoint en Android e iOS para protección web, detección de jailbreak y señales de riesgo. El marco de protección de datos tiene tres niveles.
- Los dispositivos IoT requieren hardware mínimo y a prueba de manipulaciones, secretos en HSM, credenciales únicas (X.509 en producción), actualizaciones seguras y TLS. Los dispositivos heredados se protegen con una puerta de enlace de campo como IoT Edge, y el lado de la nube usa Private Link, Microsoft Entra ID y RBAC. Los
- Microsoft Defender for IoT supervisa redes OT/ICS sin agentes mediante sensores de red conectados a puertos IoT empresariales (impresoras, cámaras) se supervisan con Defender for Endpoint y Defender for IoT.
- SPAN o TAP, que analizan el tráfico en el propio sensor con motores de infracciones de protocolo y de directiva, malware industrial, anomalías e incidentes operativos. Los sensores pueden estar conectados a la nube o administrarse localmente en entornos aislados, y se integran con Microsoft Sentinel.
- hay que resolver conflictos entre líneas base y no usar versiones preliminares en producción. Para servidores, Defender for Cloud evalúa la configuración del sistema operativo frente a las líneas base de Microsoft Cloud Security

Specify requirements for securing SaaS, PaaS, and IaaS services

- Microsoft cloud security benchmark (MCSB) es la línea base prescriptiva para Azure y multinube, con controles asignados a CIS, NIST y PCI-DSS, y Defender for Cloud la aplica por defecto a Azure, AWS y GCP. Las líneas base por servicio indican si cada característica está habilitada y quién la configura; SSPM de Defender for Cloud Apps
- La seguridad de IoT se divide en dispositivo, conexión, perímetro y nube. Se recomiendan certificados X.509 únicos, evalúa SaaS y la configuración de máquinas de Azure Policy impone ajustes del SO en IaaS.
- HSM para las claves, TLS 1.2, Private Link y Microsoft Entra ID con RBAC; los dispositivos heredados se protegen con una puerta de enlace de campo como IoT Edge. Microsoft Defender for IoT detecta dispositivos OT sin agente
- Para cargas web en App Service se recomienda WAF en Azure Front Door (global, en el perímetro) o en Application Gateway (regional), puntos de conexión privados, HTTPS y TLS 1.2 o superior, identidades administradas y referencias de Key Vault para los secretos. Defender for App Service se integra sin agentes y detecta amenazas y
- Defender for Containers cubre postura, evaluación de vulnerabilidades sin agente en registros de Azure, AWS y Google; protección en tiempo de ejecución integrada con Defender XDR y cadena de suministro con reglas de implementación controlada. El bloqueo de desviación binaria impide procesos externos en contenedores en ejecución. Se recomienda integrar Microsoft Entra ID y deshabilitar las cuentas locales, usar clústeres privados o
- En AKS se recomienda registros privados, examen en CI, Key Vault, mínimo privilegio y segmentación de red. intervalos de IP autorizados para el servidor de API, Microsoft Entra Workload ID para que los pods accedan a Azure sin secretos y Azure Policy para Kubernetes (Gatekeeper) en AKS y Arc. Las directivas de red limitan el

Evaluate solutions for network security and Security Services Edge (SSE)

- Un diseño de red de confianza cero segmenta en macro y microsegmentos con controles propios de entrada y salida, prefiere la segmentación basada en identidad y usa topología en estrella con Azure Firewall en el concentrador (Premium añade IDPS e inspección TLS). En el límite con Internet se combinan DDoS Network Protection (capas 3 y 4) y WAF (capa 7), y los servicios PaaS se protegen con Private Link o un perímetro de seguridad de red, identidad. Filtra por categoría web, FQDN y URL mediante directivas agrupadas en perfiles de seguridad vinculados al acceso condicional; el perfil de línea base se aplica a todo el tráfico, también al de redes remotas. Sin inspección
- Internet Access para servicios de Microsoft usa el perfil de tráfico de Microsoft para aportar comprobación de red TLS evalúa el HTTPS por SNI; con ella descifra el tráfico para detectar malware y aplicar DLP.
- compatible en el acceso condicional (frena la reutilización de tokens sin listas de IP), restauración de la IP de origen para Entra ID y Graph, y Universal Tenant Restrictions, que aplica las restricciones de inquilino v2 en cualquier
- Microsoft Entra Private Access es el acceso a la red de confianza cero de Global Secure Access y sustituye la VPN. sistema operativo y navegador sin proxy para evitar el acceso a inquilinos externos no autorizados.
- Quick Access agrupa los FQDN e IP privados como transición, y las aplicaciones de Global Secure Access permiten segmentar por aplicación con su propio acceso condicional. Los conectores de red privada se instalan en Windows Server, solo abren conexiones salientes y se agrupan para dar alta disponibilidad.

4. Design security solutions for applications and data

20–25%

Evaluate solutions for securing Microsoft 365

- Microsoft Secure Score mide la postura de seguridad de Microsoft 365 en cuatro grupos (identidad, dispositivos, aplicaciones y datos) y permite compararla con organizaciones similares y fijar KPI. Las acciones suman puntos completos o parciales; el riesgo aceptado no suma y las resueltas por un tercero sí. Las vistas de licencia actual, alcanzable y planeada, la zona personalizada y la tendencia de regresión ayudan a priorizar e informar.
- Microsoft Defender for Office 365 protege el correo y la colaboración con Datos adjuntos seguros, Vínculos seguros y protección contra suplantación, y añade investigación, respuesta automatizada y simulación de ataques. Defender for Cloud Apps es un CASB que descubre aplicaciones SaaS y les asigna riesgo, aporta SSPM a Secure Score, controla sesiones en el explorador y gobierna aplicaciones OAuth. Ambos se integran en Microsoft Defender XDR.
- Microsoft Intune administra dispositivos (MDM) y aplicaciones (MAM) desde la nube y se apoya en Microsoft Entra ID para la identidad. Las directivas de cumplimiento comunican el estado del dispositivo al acceso condicional, que concede o bloquea el acceso; conviene marcar como no compatibles los dispositivos sin directiva. Las directivas de protección de aplicaciones protegen datos en dispositivos personales sin inscripción.
- Microsoft Purview protege los datos de Microsoft 365 con tipos de información confidencial, clasificadores, etiquetas de confidencialidad y cifrado (Double Key Encryption cuando solo la organización debe poder descifrar). DLP supervisa y protege datos en Exchange, SharePoint, OneDrive, Teams, dispositivos y recursos locales, empezando en modo de simulación. Insider Risk Management detecta riesgos internos y escala casos a eDiscovery.
- Microsoft 365 Copilot solo devuelve datos que el usuario ya puede ver, por lo que el exceso de uso compartido se amplifica; DSPM for AI lo detecta con evaluaciones de riesgo de datos. Las etiquetas con cifrado exigen VIEW y EXTRACT para que la IA use el contenido, DLP bloquea indicaciones con datos confidenciales e Insider Risk Management detecta usos de IA de riesgo. Auditoría, eDiscovery y retención cubren el cumplimiento.

Design solutions for securing applications

- Para evaluar una cartera de aplicaciones, Microsoft Defender for Cloud (CNAPP) aporta CSPM con puntuación de seguridad, recomendaciones y cumplimiento normativo multinube, análisis de rutas de ataque para priorizar por exposición y seguridad de DevOps del código a la nube. Defender for Cloud Apps cubre las aplicaciones SaaS.
- Conviene clasificar las aplicaciones por sensibilidad de datos, exposición y criticidad.
- El modelado de amenazas identifica amenazas en la fase de diseño, cuando mitigarlas es más barato. Se crea un diagrama de flujo de datos con entidades, procesos, almacenes y límites de confianza, se aplica STRIDE a cada elemento, se priorizan las mitigaciones y se valida el resultado. Microsoft Threat Modeling Tool automatiza parte del proceso, y el modelo se actualiza cuando cambia la arquitectura.
- Una estrategia de ciclo de vida completo integra la seguridad desde los requisitos, documentando las contrapartidas y la aceptación de riesgos, hasta el diseño con modelado de amenazas y servicios administrados de Azure. Sigue con SAST y DAST en CI/CD, agentes de compilación limpios, secretos segmentados, entornos separados y exposición progresiva, y en producción con catálogos versionados, parches y retirada de recursos sin uso.
- Los estándares de desarrollo seguro se basan en las 10 prácticas de Microsoft SDL (gobernanza, modelado de amenazas, criptografía, cadena de suministro, entorno de ingeniería, pruebas, formación) y en los controles DevOps Security de MCSB: SAST con varios analizadores, análisis de secretos con protección de inserción, SBOM y Dependabot, secretos en Key Vault y federación de identidades de carga de trabajo.
- Asignar tecnologías a requisitos evita huecos. Microsoft Entra ID y External ID para usuarios, identidades administradas y federación para cargas de trabajo, Azure WAF en Front Door o Application Gateway contra el OWASP Top 10, API Management en modo interno para aislar API, DDoS Protection para ataques volumétricos, Key Vault para secretos y los planes de Defender for Cloud para detectar amenazas.

Design solutions for securing an organization's data

- Microsoft Purview clasifica con tipos de información confidencial (patrones), coincidencia exacta de datos, clasificadores entrenables, huella digital de documentos y OCR para imágenes. DSPM de Purview responde qué datos hay, dónde están, quién accede y cómo se protegen. Azure SQL incluye Data Discovery & Classification, que recomienda columnas, etiqueta y permite auditar el acceso a datos etiquetados.
- Microsoft recomienda empezar con un marco de clasificación y una taxonomía de etiquetas; después, clasificar y etiquetar, cifrar y controlar el acceso, y más tarde DLP, riesgo interno y minimización de datos. Frente a ransomware, las copias se priorizan empezando por los sistemas de identidad, se protegen con almacenamiento inmutable o sin conexión, y MFA, y la lista de copias es la de restauración.
- Azure cifra los datos en reposo por defecto con claves de la plataforma; las claves administradas por el cliente se guardan en Key Vault o en Managed HSM (de un solo inquilino y con dominio de seguridad propio). El cifrado de infraestructura de Azure Storage añade una segunda capa con otra clave y solo se activa al crear la cuenta. En tránsito se usan TLS, MAC sobre centros de datos y VPN con IPsec.
- Para los datos que usa la IA, Microsoft Purview DSPM para IA detecta el uso compartido excesivo, aplica directivas de DLP que impiden a Copilot resumir contenido con ciertas etiquetas y supervisa sitios de IA de terceros. Microsoft Defender for Cloud añade la postura de seguridad de IA en Defender CSPM (inventario, recomendaciones, rutas de ataque multinube) y alertas en tiempo real contra jailbreak y fuga de datos.
- Azure SQL combina autenticación de Microsoft Entra, TDE en reposo, Always Encrypted frente a administradores, enmascaramiento dinámico, seguridad de nivel de fila y ledger para demostrar integridad. Synapse añade seguridad de nivel de objeto, fila y columna en los grupos de SQL dedicados. En Cosmos DB se recomiendan acceso privado, RBAC del plano de datos, identidades separadas por plano y copia continua.