

MICROSOFT CERTIFIED · FUNDAMENTALS

AZ-900

Study Guide — Azure Fundamentals

Guía intensiva de preparación · Versión 2026

Temario base

Skills measured — actualización oficial del 14 de enero de 2026

Perfil objetivo

Técnico ASIR / sysadmin con experiencia Linux, redes, Docker, virtualización, AD

Formato

Cram guide — repaso intensivo, no curso introductorio

Dominios oficiales

Cloud Concepts (25-30%) · Azure Architecture & Services (35-40%) · Azure Management & Governance (30-35%)

Índice

1. Introducción al examen
2. Conceptos Cloud (25-30%)
3. Arquitectura de Azure
4. Compute y redes
5. Storage
6. Identidad, acceso y seguridad
7. Gestión de costes
8. Gobernanza y cumplimiento
9. Herramientas de gestión y despliegue
10. Monitorización
11. Fuera de temario: BD, IA, Analítica, IoT
12. Comparativas clave
13. Preguntas trampa
14. Chuleta final (repaso de última hora) 14bis. Glosario rápido A-Z 14ter. Simulacro rápido (15 preguntas)
15. Checklist final

1. Introducción al examen

1.1 Qué evalúa realmente AZ-900

AZ-900 **no** evalúa tu capacidad de administrar Azure. Evalúa si sabes **describir** conceptos, servicios y herramientas. El verbo que aparece en cada objetivo oficial es casi siempre “**Describe...**” — no “Configure...”, no “Implement...”. Esto cambia tu estrategia de estudio: memoriza *para qué sirve cada cosa y cuándo se usa*, no la sintaxis ni los pasos de configuración.

🔔 **Consejo MCT:** si una pregunta te obliga a recordar un parámetro de CLI o un paso concreto de un asistente de creación, probablemente estés ante una pregunta mal formulada o desactualizada de un banco de preguntas no oficial. El examen real es conceptual.

1.2 Formato del examen

Parámetro	Valor aproximado
Preguntas	~40-60 (varía por formulario, Microsoft no publica cifra exacta)
Duración	~45-60 min de examen (con tiempo total en sala algo mayor)
Puntuación	Escala 1-1000, aprobado ≥ 700
Tipo de preguntas	Opción única, opción múltiple, arrastrar-soltar, casos de estudio cortos, alguna simulación interactiva
Idiomas	Incluye español
Modalidad	Centro Pearson VUE o proctoring online
Caduca	Requiere renovación anual gratuita en Microsoft Learn (no expira “de por vida” desde el cambio de política)

⚠ La puntuación de aprobado (700) **no equivale a 70% de aciertos brutos** — las preguntas están ponderadas por dificultad. No lo calcules como un examen escolar clásico.

1.3 Los tres dominios oficiales



El dominio de **Arquitectura y Servicios** es el más pesado — invierte ahí la mayor parte de tu tiempo de estudio. Este documento sigue exactamente esta estructura oficial (no la de guías genéricas de terceros, que suelen incluir contenido ya retirado del temario).

1.4 Errores comunes de candidatos

Error	Por qué falla
Estudiar con dumps antiguos de 2019-2022	Incluyen Azure Blueprints (obsoleto), omiten Microsoft Purview y Azure Arc (nuevos), y sobredimensionan IA/BD/IoT que ya no están en el temario
Memorizar precios exactos	El examen pregunta <i>qué herramienta</i> estima costes, no cifras concretas
Confundir “quién administra qué” en el modelo de responsabilidad compartida	Es la pregunta trampa más repetida del examen — ver sección 13
Tratar RBAC y Azure Policy como sinónimos	Uno controla quién puede actuar, el otro controla qué configuración es válida
Ignorar Microsoft Entra ID por “ya conozco Active Directory”	Entra ID es un servicio de identidad cloud-native , no un AD replicado — las diferencias son material de examen

1.5 Plan de estudio intensivo (5 días)

Pensado para alguien con tu perfil técnico (ASIR, Linux, redes, Docker, virtualización) — no necesitas tiempo para conceptos básicos de IT, solo para el vocabulario y las particularidades de Azure.

Día	Bloque	Contenido	Tiempo estimado
1	Cloud Concepts	Sección 2 completa + tabla de responsabilidad compartida hasta poder dibujarla de memoria	2-3 h
2	Arquitectura + Compute/Redes	Secciones 3 y 4 completas. Practica en el Portal: crea una VM real y localiza cada recurso que menciona 4.3	3-4 h
3	Storage + Identidad/Seguridad	Secciones 5 y 6. Memoriza la tabla de redundancia (12.4) y la de tiers	3 h
4	Costes + Gobernanza + Herramientas + Monitorización	Secciones 7, 8, 9, 10. Repasa comparativas RBAC vs Policy y Advisor vs Service Health	2-3 h
5	Repaso general	Sección 11 (solo lectura rápida), 12 (todas las comparativas), 13 (preguntas trampa) y examen de práctica oficial de Microsoft Learn	3 h + práctica

🔔 **La noche antes del examen:** relee únicamente la sección 14 (Chuleta final) y repasa la sección 16 (Checklist). No abras contenido nuevo.

1.6 Qué NO vas a encontrar apenas en el examen (y por qué)

El temario oficial vigente (enero 2026) **no incluye** como objetivos: bases de datos gestionadas (Azure SQL, Cosmos DB), servicios de IA (Azure OpenAI, Cognitive Services), analítica (Synapse, Databricks, Data Factory) ni IoT (IoT Hub, IoT Central, Digital Twins). Esos bloques pertenecen a DP-900, AI-900 y a certificaciones de rol. Tampoco se detalla Network Security Groups, Load Balancer, Application Gateway o Azure Firewall a nivel de configuración — eso es AZ-104. Este documento los trata en la sección 11 con la profundidad mínima necesaria para no sorprenderte si aparecen como distractores, pero no merecen horas de estudio.

2. Conceptos Cloud (25-30%)

2.1 Cloud computing: definición de examen

Cloud computing = entrega de recursos de computación (servidores, almacenamiento, bases de datos, redes, software) **bajo demanda**, a través de internet, con **pago por uso**.

Las cinco características que el examen espera que reconozcas:

Característica	Qué significa
Autoservicio bajo demanda	El usuario provisiona recursos sin intervención humana del proveedor
Acceso amplio a la red	Disponible desde cualquier dispositivo con conexión
Pool de recursos	Recursos compartidos multi-tenant, asignados dinámicamente
Elasticidad rápida	Los recursos escalan (arriba/abajo) casi al instante
Servicio medido	Pago basado en consumo real, con métricas y facturación transparente

2.2 Modelo de responsabilidad compartida ☆☆☆☆

Es **el tema más preguntado de todo el examen** bajo distintas formas. La regla de oro:

El diagrama muestra una tabla de responsabilidad compartida en la nube. Las columnas representan los modelos de servicio: IaaS, PaaS, SaaS y SaaS+. Las filas representan los componentes de la arquitectura: Datos e info, Dispositivos, Identidad, Aplicaciones, Runtime, Middleware, Sistema Operativo, Virtualización, Servicios Plataforma, Almacenamiento, Redes y Redes Privadas, y Recursos Plataforma. Una línea horizontal divide la responsabilidad entre el cliente (izquierda) y el proveedor (derecha). En IaaS, el cliente es responsable de Datos e info, Dispositivos e Identidad. En PaaS, el cliente es responsable de Datos e info, Dispositivos, Identidad y Aplicaciones. En SaaS, el cliente es responsable de Datos e info, Dispositivos, Identidad y Aplicaciones. En SaaS+, el cliente es responsable de Datos e info, Dispositivos, Identidad y Aplicaciones. El proveedor es responsable de todo lo que está a la derecha de la línea de responsabilidad.

Componente	IaaS	PaaS	SaaS	SaaS+
Datos e info	Cliente	Cliente	Cliente	Cliente
Dispositivos	Cliente	Cliente	Cliente	Cliente
Identidad	Cliente	Cliente	Cliente	Cliente
Aplicaciones	Proveedor	Proveedor	Proveedor	Proveedor
Runtime	Proveedor	Proveedor	Proveedor	Proveedor
Middleware	Proveedor	Proveedor	Proveedor	Proveedor
Sistema Operativo	Proveedor	Proveedor	Proveedor	Proveedor
Virtualización	Proveedor	Proveedor	Proveedor	Proveedor
Servicios Plataforma	Proveedor	Proveedor	Proveedor	Proveedor
Almacenamiento	Proveedor	Proveedor	Proveedor	Proveedor
Redes y Redes Privadas	Proveedor	Proveedor	Proveedor	Proveedor
Recursos Plataforma	Proveedor	Proveedor	Proveedor	Proveedor

☛ **Regla mnemotécnica:** cuanto más "as a Service" subes (IaaS → PaaS → SaaS), **menos capas gestionas tú**. Pero **identidad, datos y dispositivos son SIEMPRE responsabilidad del cliente**, incluso en SaaS puro (Microsoft 365, por ejemplo). Esta última frase es la que más preguntas trampa genera.

2.3 Modelos de nube: público, privado, híbrido

Modelo	Definición	Caso de uso típico
Público	Infraestructura propiedad del proveedor, compartida entre clientes (multi-tenant)	Startups, cargas variables, sin CapEx inicial
Privado	Infraestructura dedicada a una sola organización (on-prem o hosted)	Banca, sanidad, gobierno con requisitos regulatorios estrictos
Híbrido	Combina público + privado con conectividad entre ambos	Empresas con datos sensibles on-prem + escalado en la nube (tu escenario típico de MSP)

También existe **community cloud** (compartida por organizaciones con requisitos comunes) — se menciona poco pero puede aparecer como distractor.

2.4 Modelo de consumo (consumption-based)

Pagas **solo por lo que usas**, sin inversión inicial en hardware. Frente al modelo tradicional:

	(Capital Expenditure)	(Operational Expenditure)
Qué es	Inversión inicial en infraestructura propia	Gasto operativo recurrente, pago por uso
Pago	Por adelantado	Según consumo, facturación periódica
Escalado	Requiere comprar más hardware (lento)	Instantáneo, bajo demanda
Modelo cloud	On-premises tradicional	Azure = OpEx
Riesgo	Sobreaprovisionar o quedarse corto	Ninguno de los dos — pagas lo justo

2.5 Modelos de precios (pricing models)

Modelo	Descripción
Pay-as-you-go	Pago por consumo real, sin compromiso
Reservas (Reserved Instances)	Compromiso de 1 o 3 años a cambio de descuento (hasta ~72%)
Spot pricing	Capacidad no utilizada de Azure a precio muy reducido, pero puede ser reclamada (evicted) en cualquier momento — ideal para cargas tolerantes a interrupciones
Hybrid Benefit	Reutiliza licencias on-prem (Windows Server, SQL Server) ya pagadas para reducir coste en Azure

2.6 Serverless

Serverless no significa “sin servidores” — significa que **tú no gestionas** los servidores. El proveedor aprovisiona, escala y factura por ejecución/consumo real, no por capacidad reservada.

- Ejemplo estrella en Azure: **Azure Functions** (compute) y **Logic Apps** (orquestación).
- Características clave de examen: escalado automático a cero, facturación por ejecución, sin gestión de infraestructura subyacente.

2.7 Beneficios del cloud ☆☆☆☆

Beneficio	Qué evalúa el examen
Alta disponibilidad (HA)	Capacidad de seguir operativo ante fallos — Azure lo logra con Availability Zones, Availability Sets, redundancia geográfica
Escalabilidad	Añadir/quitar recursos para ajustar capacidad. Vertical = más potencia a la misma máquina (scale up). Horizontal = más instancias (scale out) — Azure prioriza horizontal
Elasticidad	Escalado automático en respuesta a demanda, típicamente con Scale Sets
Fiabilidad (Reliability)	El sistema se recupera de fallos y sigue funcionando según lo diseñado
Previsibilidad (Predictability)	Rendimiento consistente (<i>performance predictability</i>) y coste consistente (<i>cost predictability</i>)
Seguridad y gobernanza	Herramientas centralizadas: Defender for Cloud, Policy, RBAC
Manejabilidad (Manageability)	Gestión vía Portal/CLI/PowerShell, autoescalado, monitorización, despliegue automatizado

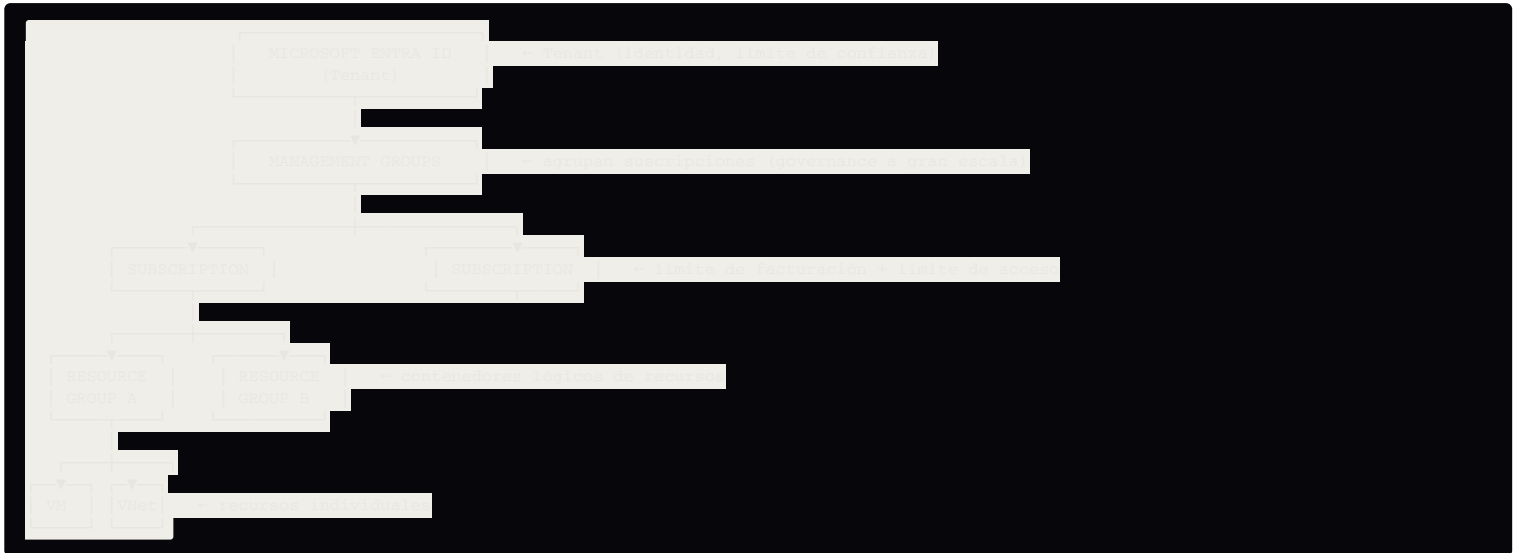
⚠ **Trampa clásica:** “Escalabilidad” y “elasticidad” no son sinónimos en el examen. Escalabilidad = *capacidad de escalar* (manual o automático). Elasticidad = escalado **automático y dinámico** según demanda en tiempo real.

2.8 Tipos de servicio: IaaS / PaaS / SaaS ☆☆☆☆

Qué obtienes	Infraestructura virtualizada (VMs, redes, storage)	Plataforma para desarrollar/desplegar sin gestionar el SO	Aplicación completa lista para usar
Gestionas tú	SO, runtime, middleware, apps, datos	Apps y datos	Solo datos y configuración de usuario
Ejemplo Azure	Azure Virtual Machines	Azure App Service, Azure SQL Database	Microsoft 365, Dynamics 365
Caso de uso	Migración "lift-and-shift", control total del SO	Desarrollo rápido de apps sin gestionar servidores	Uso directo sin desarrollo
Analogía	Alquilar un local vacío	Alquilar un local con cocina instalada	Restaurante con servicio completo

3. Arquitectura de Azure

3.1 Jerarquía de organización ★★★★★



Nivel	Qué es	Qué controla
Tenant	Instancia dedicada de Microsoft Entra ID, representa a la organización	Identidad, límite de seguridad más alto
Management Group	Agrupar múltiples suscripciones	Aplica Policy/RBAC a nivel masivo, herencia hacia abajo
Subscription	Unidad de facturación y de límites de servicio	Factura, cuotas, límites de recursos, aislamiento de acceso
Resource Group	Contenedor lógico (no físico) de recursos relacionados	Ciclo de vida conjunto: se despliegan/eliminan juntos
Resource	Instancia individual de un servicio (VM, VNet, storage account...)	La unidad mínima gestionable

☛ **Regla clave:** un recurso pertenece a **un único** resource group. Un resource group pertenece a **una única** subscription. Las políticas y permisos aplicados arriba en la jerarquía **se heredan hacia abajo** (management group → subscription → resource group → resource).

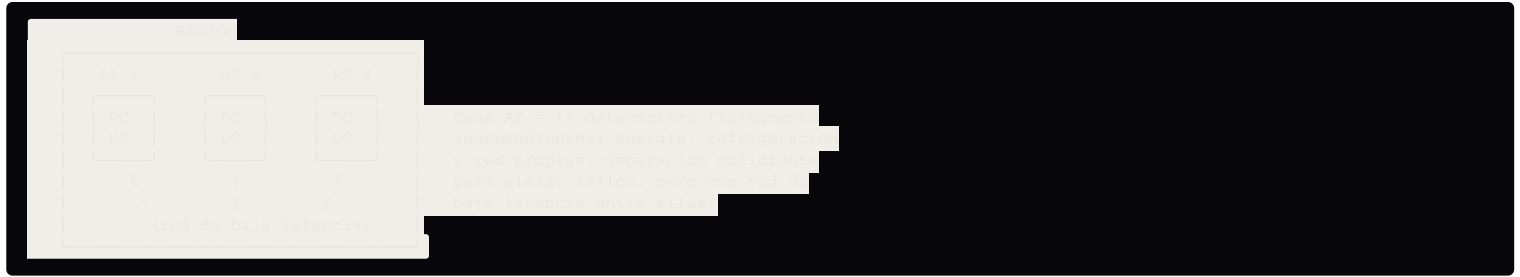
⚠ **Trampa:** los recursos dentro de un resource group **no tienen que estar en la misma región**. El resource group solo almacena metadatos y la región de éste es solo dónde se guarda esa metadata, no dónde viven los recursos.

3.2 Regiones, region pairs y sovereign regions

Concepto	Definición
Región	Conjunto de datacenters con red de baja latencia dedicada, dentro de un perímetro geográfico definido
Region pair	Cada región de Azure está emparejada con otra región dentro de la misma geografía (mínimo 300 millas de distancia) para replicación y recuperación ante desastres coordinada
Sovereign region	Regiones aisladas de la nube pública global por requisitos legales/de cumplimiento (ej. Azure Government en EE.UU., Azure China gestionada por 21Vianet)

Ventajas de los region pairs: si Microsoft aplica una actualización planificada, lo hace de forma **secuencial**, nunca a ambas regiones del par simultáneamente. En caso de desastre, la recuperación prioriza restaurar primero una de las dos regiones emparejadas.

3.3 Availability Zones vs Datacenters



Concepto	Qué protege	Nota de examen
Datacenter	Unidad física, no es unidad de resiliencia expuesta al cliente	No se selecciona directamente
Availability Zone	Fallo de todo un datacenter (energía, refrigeración, red)	No todas las regiones tienen AZs — verifica soporte por región
Availability Set	Fallo de hardware dentro de un mismo datacenter (rack, host)	Usa fault domains + update domains — ver sección 4

3.4 Suscripciones y cuentas

Una **suscripción** es el límite lógico entre facturación y acceso. Puede haber múltiples suscripciones bajo un mismo tenant (ej. una para Producción, otra para Desarrollo), cada una con sus propios límites de cuota y su propio RBAC.

4. Compute y redes

4.1 Comparativa de tipos de compute ★★★★★

Tipo	Qué es	Control	Escalado	Cuándo usarlo
Virtual Machines	Máquina virtual completa (IaaS)	Total sobre el SO	Manual o con Scale Sets	Migración lift-and-shift, apps legacy, control total del SO
Containers	Empaquetan app + dependencias, comparten kernel del host	Aislamiento de proceso, no de SO completo	Rápido, orquestable (AKS)	Microservicios, despliegues consistentes multientorno
Functions (serverless)	Ejecuta código bajo eventos, sin gestionar servidor	Ninguno sobre infraestructura	Automático, incluso a cero	Tareas cortas dirigidas por eventos, cargas esporádicas

🔑 **Mnemotecnia:** VM = “quiero todo el SO”. Container = “quiero que mi app corra igual en todos lados, sin la VM entera”. Function = “solo quiero que se ejecute mi código cuando pase algo”.

4.2 Opciones de máquina virtual

Servicio	Qué hace	Cuándo usarlo	Qué NO hace
Azure Virtual Machines	VM individual bajo demanda	Carga única, control granular	No escala automáticamente por sí sola
Virtual Machine Scale Sets (VMSS)	Grupo de VMs idénticas que escala automáticamente	Apps stateless de alto tráfico, autoescalado horizontal	No gestiona VMs con configuración distinta entre sí
Availability Sets	Agrupar VMs en fault domains (hardware/rack) y update domains (ventanas de mantenimiento) dentro de un mismo datacenter	Alta disponibilidad dentro de un único datacenter, cuando no hay AZs disponibles	No protege contra fallo de todo el datacenter (para eso: Availability Zones)
Azure Virtual Desktop (AVD)	Escritorios y apps Windows virtualizados, entregados en la nube	Trabajo remoto, BYOD, escritorios centralizados	No es una VM de propósito general

△ **Fault domain vs Update domain** (dentro de Availability Sets): - **Fault domain:** agrupación por hardware físico compartido (rack, switch, alimentación). Azure reparte tus VMs entre varios para que un fallo de hardware no tumbe todas. - **Update domain:** agrupación lógica para que Azure no reinicie todas tus VMs a la vez durante mantenimiento planificado.

4.3 Recursos necesarios para una VM

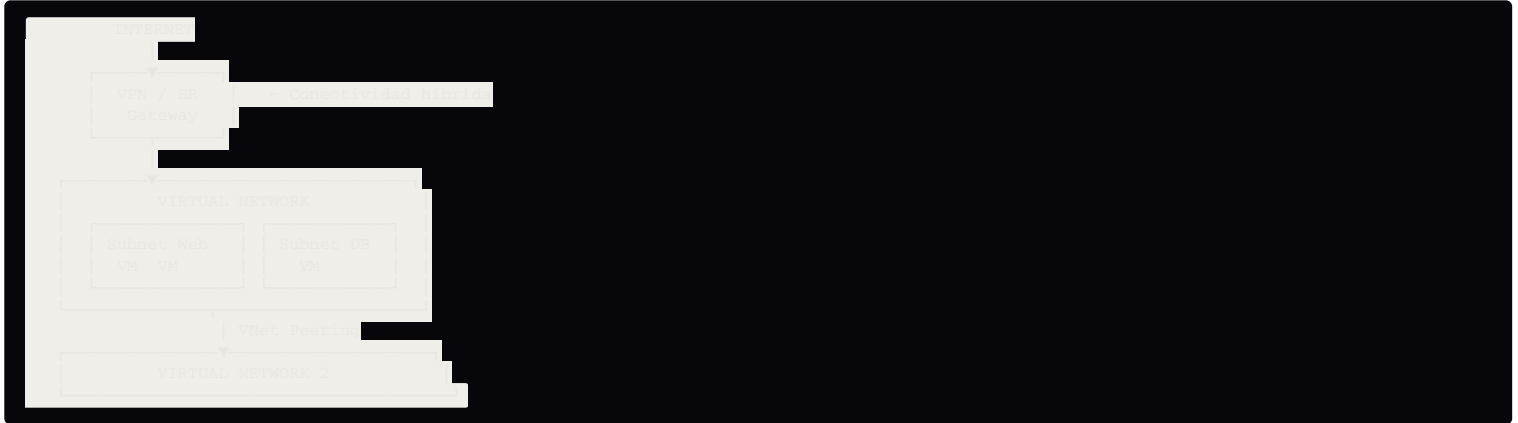
Al crear una VM, siempre necesitas como mínimo:

Recurso	Función
Resource Group	Contenedor lógico
Tamaño (Size/SKU)	Define vCPUs, RAM, almacenamiento temporal disponible
Imagen de SO	Windows, Linux (Marketplace o imagen propia)
Disco del SO (OS Disk)	Managed Disk donde vive el sistema operativo
Red virtual (VNet) + subred	Conectividad
Interfaz de red (NIC)	Conecta la VM a la subred
IP pública (opcional)	Solo si necesita ser accesible desde internet
Grupo de seguridad de red (NSG, opcional)	Filtrado de tráfico a nivel de subred/NIC

4.4 Opciones de hosting de aplicaciones

Servicio	Qué hace	Cuándo usarlo	Qué NO hace
Web Apps (App Service)	PaaS para alojar apps web/API sin gestionar SO	Apps web estándar, quieres CI/CD y autoescalado sin gestionar servidores	No da acceso al sistema operativo subyacente
Containers (ACI / AKS)	Ejecuta contenedores gestionados o un clúster completo orquestado	Microservicios, portabilidad multi-nube	ACI no orquesta a gran escala (para eso AKS)
Virtual Machines	IaaS, control total	Apps que requieren SO/configuración específica no soportada por PaaS	No ofrece autoescalado "gratis" ni parcheo automático del SO

4.5 Redes virtuales ★★★★★



Componente	Función	Nota de examen
Virtual Network (VNet)	Red privada aislada lógicamente en Azure	Límite de aislamiento de red por defecto
Subred (Subnet)	Segmentación de la VNet	Permite aplicar reglas/aislamiento por capa (web, app, datos)
VNet Peering	Conecta dos VNets con tráfico privado de baja latencia	No pasa por internet público; requiere rangos IP no solapados
Azure DNS	Resolución de nombres, hospeda dominios	No es un servicio de filtrado de tráfico
VPN Gateway	Conexión cifrada sobre internet público entre on-prem y Azure (o entre VNets)	Menor coste, mayor latencia, throughput limitado
ExpressRoute	Conexión privada dedicada a través de un proveedor, sin pasar por internet público	Mayor coste, mayor fiabilidad/latencia predecible, throughput alto

Endpoints públicos vs privados

	Público	Privado
Accesible desde	Internet	Solo desde dentro de la VNet (o VNets conectadas)
Exposición	Mayor superficie de ataque	Tráfico nunca sale a internet público
Ejemplo	IP pública en una VM	Azure Private Link / Private Endpoint hacia un servicio PaaS

🔗 Un **Private Endpoint** te permite conectar de forma privada a un servicio PaaS (como una Storage Account) usando una IP dentro de tu propia VNet, en lugar de una IP pública del servicio.

4.6 Networking avanzado — fuera del núcleo del temario ★★

Estos términos **no aparecen como objetivo explícito** en el temario AZ-900 actual (pertenecen a AZ-104), pero pueden aparecer como opciones de respuesta en preguntas de escenario. Conócelos a nivel de "para qué sirve", nada más:

Servicio	Para qué sirve en una frase
Network Security Group (NSG)	Filtra tráfico entrante/saliente a nivel de subred o NIC mediante reglas de permitir/denegar
Azure Firewall	Firewall gestionado con estado, a nivel de red virtual completa
Load Balancer	Distribuye tráfico de capa 4 (TCP/UDP) entre varias instancias
Application Gateway	Balancedor de capa 7 (HTTP/HTTPS), enrutamiento por URL, con WAF integrado
Content Delivery Network (CDN)	Sirve contenido estático desde nodos edge cercanos al usuario
Azure Private Link	Acceso privado a servicios PaaS de Azure a través de un Private Endpoint

5. Storage

5.1 Servicios de Azure Storage ★★★★★

Servicio	Tipo de dato	Caso de uso	Analogía
Blob Storage	Objetos no estructurados (binarios)	Imágenes, vídeo, backups, data lake	Carpeta gigante de archivos sueltos
Azure Files	Sistema de archivos compartido vía SMB/NFS	Reemplazo de file server on-prem, "lift and shift" de recursos compartidos	Disco de red compartido clásico
Queue Storage	Cola de mensajes simple	Desacoplar componentes de una aplicación, procesamiento asíncrono	Buzón de tareas pendientes
Table Storage	Datos NoSQL clave-valor	Datos semiestructurados a gran escala, bajo coste	Hoja de cálculo gigante sin esquema fijo
Managed Disks	Disco virtual para VMs	Disco de SO o de datos de una VM	El "disco duro" de tu VM

5.2 Tiers de Blob Storage

Tier	Coste almacenamiento	Coste acceso	Latencia	Cuándo usarlo
Hot	Alto	Bajo	Milisegundos	Datos accedidos frecuentemente
Cool	Medio	Medio	Milisegundos	Datos accedidos poco, retenidos ≥ 30 días
Cold	Bajo	Alto	Milisegundos	Accedidos raramente, retenidos ≥ 90 días
Archive	Mínimo	Máximo	Horas (requiere rehidratación)	Backups/cumplimiento legal a largo plazo, retenidos ≥ 180 días

⚠ **Trampa:** Archive **no permite lectura directa** — hay que "rehidratar" el blob primero (proceso que tarda horas). Si una pregunta menciona "acceso inmediato ocasional", la respuesta no es Archive, es Cool o Cold.

5.3 Opciones de redundancia (replicación) ★★★★★



Redundancia	Copias	Protege contra	Nivel
LRS (Locally Redundant Storage)	3 copias	Fallo de disco/nodo dentro de un datacenter	La más barata, menor resiliencia
ZRS (Zone Redundant Storage)	3 copias	Fallo de todo un datacenter (repartidas entre Availability Zones de la región)	Resiliencia intrarregional
GRS (Geo Redundant Storage)	6 copias (3+3)	Fallo de toda la región — replica asíncronamente a la región emparejada	Datos secundarios no accesibles salvo failover
GZRS (Geo Zone Redundant Storage)	6 copias (3+3)	Combina ZRS en la primaria + réplica geográfica en la pareja	Máxima resiliencia estándar
RA-GRS / RA-GZRS	Igual que GRS/GZRS	Igual, más acceso de solo lectura a la región secundaria en todo momento	Permite leer de la región secundaria sin esperar failover

☛ **RA- (Read Access)** es el matiz clave: GRS por sí solo no te deja leer la copia secundaria hasta que Microsoft (o tú) declaráis un failover. RA-GRS sí te permite lectura continua desde la secundaria.

5.4 Tipos de cuenta de almacenamiento

Tipo	Soporta	Uso típico
Standard general-purpose v2	Blob, Files, Queue, Table, Disks	Mayoría de escenarios, mejor relación coste/rendimiento
Premium (SSD)	Discos de VM de alto rendimiento, blobs de baja latencia	Cargas I/O intensivas

5.5 Herramientas de movimiento y migración de datos

Herramienta	Para qué sirve
AzCopy	CLI para copiar datos masivamente hacia/desde Blob y Files
Azure Storage Explorer	GUI para explorar y gestionar cuentas de almacenamiento
Azure File Sync	Sincroniza un file server on-prem (Windows Server) con Azure Files, con caché local
Azure Migrate	Herramienta central para evaluar y migrar servidores, VMs, BD y apps a Azure
Azure Data Box	Dispositivo físico para transferir grandes volúmenes de datos offline cuando el ancho de banda es insuficiente

6. Identidad, acceso y seguridad

6.1 Microsoft Entra ID (antes Azure AD) ★★★★★

Microsoft Entra ID es el servicio de identidad y acceso **cloud-native** de Microsoft. No es “Active Directory movido a la nube”: es un servicio distinto, basado en HTTP/HTTPS y protocolos como SAML, OAuth 2.0 y OpenID Connect (no usa LDAP/Kerberos como el AD tradicional).

	Active Directory Domain Services (on-prem)	Microsoft Entra ID
Protocolo	LDAP, Kerberos	REST/HTTPS, SAML, OAuth2, OIDC
Estructura	Unidades organizativas (OU), GPOs	Plano, basado en grupos/roles
Alcance	Dominio y bosque	Tenant cloud, multi-servicio (M365, Azure, SaaS)

Microsoft Entra Domain Services es un servicio **gestionado** que ofrece funcionalidades compatibles con AD tradicional (unir a dominio, GPOs, LDAP) sin gestionar controladores de dominio — es el puente para apps legacy que necesitan AD clásico dentro de Azure.

6.2 Métodos de autenticación

Método	Qué es
SSO (Single Sign-On)	Un único inicio de sesión da acceso a múltiples aplicaciones sin reautenticar
MFA (Multifactor Authentication)	Requiere 2+ factores: algo que sabes (contraseña) + algo que tienes (app/token) o eres (biometría)
Passwordless	Autenticación sin contraseña: Windows Hello, llave de seguridad FIDO2, Microsoft Authenticator

6.3 Identidades externas (External Identities)

Permite colaborar con usuarios **fuera** de tu organización:

- **B2B (Business to Business)**: invitas usuarios externos (partners, proveedores) a colaborar usando su propia identidad.
- **B2C (Business to Consumer)**: gestiona identidades de clientes finales para tus propias aplicaciones.

6.4 Conditional Access

Aplica reglas de acceso **“si esto, entonces aquello”** basadas en señales: ubicación, dispositivo, riesgo de la sesión, aplicación. Ejemplo: “si el usuario se conecta desde fuera de España, exigir MFA”. No es un firewall — opera a nivel de identidad, no de red.

6.5 RBAC (Role-Based Access Control) ★★★★★

Controla **quién** puede hacer **qué** sobre **qué recurso**, mediante la asignación de un **rol** a una **identidad** (usuario, grupo, service principal) en un **ámbito** (scope).

Rol integrado	Permite
Owner	Control total, incluye gestionar acceso de otros
Contributor	Crear/gestionar todo tipo de recursos, pero no puede conceder acceso a otros
Reader	Solo puede ver recursos, sin modificarlos
User Access Administrator	Solo gestiona el acceso de otros usuarios, no los recursos en sí

Los ámbitos posibles, de más amplio a más específico: **Management Group** → **Subscription** → **Resource Group** → **Resource**. Los permisos se **heredan** hacia abajo.

6.6 Zero Trust

Modelo de seguridad basado en el principio “**nunca confíes, verifica siempre**”. Tres pilares que el examen espera que reconozcas:

1. **Verificar explícitamente** — autenticar y autorizar siempre con todos los datos disponibles (identidad, ubicación, dispositivo, etc.)
2. **Usar acceso de mínimo privilegio** — Just-In-Time y Just-Enough-Access
3. **Asumir la brecha (assume breach)** — minimizar el radio de impacto, segmentar el acceso, cifrar de extremo a extremo

6.7 Defensa en profundidad (Defense in Depth)

Modelo de capas concéntricas de seguridad, para que si una capa falla, las siguientes sigan protegiendo:



6.8 Microsoft Defender for Cloud

Plataforma **CSPM** (Cloud Security Posture Management) y **CWP** (Cloud Workload Protection) que evalúa la postura de seguridad de tus recursos, da recomendaciones priorizadas y una **puntuación de seguridad (Secure Score)**, y detecta amenazas activas.

⚠ No confundir con Microsoft Sentinel (SIEM/SOAR) — Sentinel **no forma parte** del temario oficial de AZ-900 actual, aunque a veces aparece en materiales de terceros desactualizados.

7. Gestión de costes

7.1 Factores que afectan al coste en Azure

Factor	Impacto
Tipo de recurso	Cada servicio tiene su propio modelo de precio
Región	El mismo servicio puede costar distinto según la región
Consumo (compute/red/almacenamiento)	Pago por uso real
Tipo de suscripción	Pay-as-you-go, Enterprise Agreement, CSP, etc. tienen tarifas distintas
Egress de red	El tráfico saliente de Azure suele facturarse; el entrante normalmente no

7.2 Herramientas de estimación y gestión de coste

Herramienta	Para qué sirve	Cuándo se usa
Pricing Calculator	Estima el coste de una arquitectura antes de desplegarla	Fase de planificación/diseño
Total Cost of Ownership (TCO) Calculator	Compara el coste de mantener infraestructura on-premises frente a migrar a Azure	Justificar una migración ante negocio
Cost Management + Billing	Monitoriza, analiza y controla gasto ya generado; permite fijar presupuestos y alertas	Fase operativa, después del despliegue

👉 **Diferencia de examen:** Pricing Calculator = “¿cuánto va a costar si lo despliego?” (antes). Cost Management = “¿cuánto estoy gastando ya y cómo lo controlo?” (durante/después). TCO Calculator = “¿me compensa migrar frente a seguir on-prem?” (comparativa).

7.3 Tags (etiquetas)

Pares **clave-valor** aplicados a recursos para organizarlos y **facilitar la atribución de costes**, automatización y gobernanza. Ejemplo:

Departamento: Ventas, Entorno: Producción, CentroCoste: 4521. No afectan al rendimiento — son puramente metadatos de gestión.

8. Gobernanza y cumplimiento

8.1 Microsoft Purview

Familia de servicios de **gobernanza de datos, cumplimiento y gestión de riesgos** unificada. En el contexto de AZ-900 basta con saber que Purview ayuda a **descubrir, clasificar y proteger** datos sensibles a través de todo el entorno (Azure, Microsoft 365, on-prem, multi-nube), y aporta capacidades de cumplimiento normativo centralizado.

8.2 Azure Policy ☆☆☆☆

Evalúa recursos frente a **reglas de negocio/cumplimiento** y puede **auditar, denegar o corregir automáticamente** configuraciones que no cumplen el estándar definido. No controla identidades — controla **configuración**.

Efecto de Policy	Qué hace
Deny	Bloquea la creación/modificación de un recurso no conforme
Audit	Permite la acción, pero marca el recurso como no conforme en el informe
Append	Añade campos/valores adicionales al recurso durante su creación
DeployIfNotExists	Despliega automáticamente un recurso relacionado si no existe (ej. forzar agente de monitorización)

Initiative (iniciativa): agrupación de varias políticas relacionadas, aplicadas como un conjunto único.

8.3 RBAC vs Azure Policy — la comparación más preguntada del bloque de gobernanza

Controla	Quién puede hacer una acción	Qué configuración es válida, independientemente de quién la haga
Pregunta que responde	“¿Puede este usuario crear una VM?”	“¿Puede esta VM crearse fuera de la región weu?”
Se aplica a	Identidades (usuarios, grupos, apps)	Recursos, sin importar quién los cree
Ejemplo	Dar rol Contributor a un equipo en un Resource Group	Exigir que todo storage account tenga cifrado habilitado

8.4 Resource Locks (bloqueos)

Impiden cambios accidentales, **independientemente de los permisos RBAC** que tenga el usuario.

Tipo de lock	Efecto
CanNotDelete	El recurso se puede leer y modificar, pero no eliminar
ReadOnly	El recurso solo se puede leer — ni modificar ni eliminar

△ **Trampa:** un lock aplica **incluso a un Owner**. Tener rol Owner no permite saltarse un ReadOnly lock — hay que quitar el lock primero.

✦ **Nota sobre Azure Blueprints:** aparecía en guías antiguas como herramienta de gobernanza para empaquetar plantillas ARM + políticas + asignaciones de rol. Microsoft lo ha ido reemplazando por **Template Specs** y **Deployment Stacks**. No es objetivo del temario actual — si aparece en un simulador de terceros, es señal de que ese material está desactualizado.

9. Herramientas de gestión y despliegue

9.1 Comparativa de herramientas de gestión

Herramienta	Tipo	Cuándo usarla
Azure Portal	GUI web	Exploración visual, tareas puntuales, usuarios que prefieren interfaz gráfica
Azure CLI	Línea de comandos multiplataforma (<code>az ...</code>)	Scripting, automatización, entornos Linux/macOS/Windows
Azure PowerShell	Módulo de PowerShell (<code>Get-Az...</code> , <code>New-Az...</code>)	Automatización en entornos con fuerte presencia de PowerShell/Windows
Azure Cloud Shell	Terminal basada en navegador , con CLI y PowerShell preinstalados	Gestión rápida sin instalar nada localmente, accesible desde el propio Portal

🔗 Para tu perfil (Linux + automatización), Azure CLI es probablemente tu herramienta natural — pero el examen solo pide que sepas **qué es cada una**, no su sintaxis.

9.2 Azure Arc

Extiende la gestión de Azure (Policy, RBAC, Monitor, Defender) a recursos que **viven fuera de Azure**: servidores on-premises, máquinas en otras nubes (AWS, GCP), clústeres Kubernetes externos. Azure Arc **no mueve** esos recursos a Azure — los proyecta dentro del plano de control de Azure para gestionarlos de forma unificada.

👉 Es exactamente el tipo de servicio que le interesa a un MSP con clientes híbridos: gestión centralizada sin migrar todo a la nube.

9.3 Infraestructura como código (IaC)

Define y despliega infraestructura mediante **archivos de configuración declarativos**, en lugar de pasos manuales en el Portal. Ventajas de examen: repetibilidad, control de versiones, consistencia entre entornos, reducción de errores humanos.

Herramienta	Qué es	Sintaxis
ARM Templates	Plantillas nativas de Azure Resource Manager	JSON
Bicep	Lenguaje declarativo que se transpila a ARM (JSON)	DSL más legible que JSON

△ El examen **no** exige escribir ni leer sintaxis JSON/Bicep — solo saber que ARM es el motor de despliegue subyacente de Azure y que Bicep es una capa de abstracción más cómoda sobre él.

10. Monitorización

10.1 Azure Advisor

Motor de **recomendaciones personalizadas** sobre tu entorno, organizadas en cinco categorías:



10.2 Azure Service Health vs Resource Health

Comparación de Azure Service Health vs Resource Health		
Ámbito	Problemas de la plataforma Azure (incidencias, mantenimientos, avisos) que afectan a tu suscripción	Estado de tus recursos individuales concretos
Pregunta que responde	“¿Azure tiene una incidencia en <code>westeurope</code> ahora mismo?”	“¿Por qué mi VM concreta no responde?”

10.3 Azure Monitor ★★★★★

Plataforma central de recolección y análisis de telemetría (métricas + logs) de toda tu infraestructura y aplicaciones.

Componente	Función
Log Analytics	Motor de consultas (lenguaje KQL) sobre logs recopilados por Azure Monitor
Azure Monitor Alerts	Reglas que disparan notificaciones/acciones automáticas cuando una métrica/log cumple una condición
Application Insights	Monitorización de rendimiento de aplicaciones (APM): tiempos de respuesta, tasas de fallo, dependencias externas

↔ **Diferencia de examen:** Log Analytics analiza logs de **infraestructura**; Application Insights analiza el comportamiento de **código de aplicación**. Ambos son parte de la familia Azure Monitor, no productos independientes.

11. Fuera del temario oficial: BD, IA, Analítica, IoT

Estos bloques **no aparecen como objetivo** en el skills outline vigente de AZ-900 (verificado contra la actualización oficial del 14 de enero de 2026). Pertenecen a otras certificaciones fundamentales: **DP-900** (datos/analítica), **AI-900** (inteligencia artificial). Se incluyen aquí solo como **visión general de una frase por servicio**, por si aparecen como distractor en una pregunta de arquitectura general. No dediques tiempo de estudio serio a esta sección.

11.1 Bases de datos — probabilidad de examen: ☆ (muy baja)

Servicio	Una frase
Azure SQL Database	Base de datos relacional PaaS totalmente gestionada, compatible con SQL Server
Azure SQL Managed Instance	Instancia SQL Server gestionada con compatibilidad casi total con on-prem
Cosmos DB	Base de datos NoSQL multi-modelo, distribuida globalmente, baja latencia garantizada
Database for PostgreSQL / MySQL / MariaDB	Versiones PaaS gestionadas de motores open source

11.2 Servicios de IA — probabilidad de examen: ☆ (muy baja, temario DP-900/AI-900)

Servicio	Una frase
Azure OpenAI Service	Acceso gestionado a modelos GPT y similares dentro del perímetro de seguridad de Azure
Azure AI Document Intelligence	Extrae texto y datos estructurados de documentos (antes "Form Recognizer")
Azure AI Speech	Conversión voz-texto y texto-voz
Azure AI Vision	Análisis de imágenes: OCR, detección de objetos, moderación
Azure AI Translator	Traducción automática de texto

11.3 Analítica — probabilidad de examen: ☆ (muy baja, temario DP-900)

Servicio	Una frase
Azure Synapse Analytics	Plataforma unificada de analítica de datos a gran escala (data warehouse + big data)
Azure Databricks	Plataforma de analítica basada en Apache Spark, orientada a ingeniería/ciencia de datos
Azure Data Factory	Orquestación y ETL/ELT de flujos de datos entre orígenes
HDInsight	Servicio gestionado para frameworks big data open source (Hadoop, Spark, Kafka...)

11.4 IoT — probabilidad de examen: ☆ (prácticamente nula, temario de certificaciones de rol)

Servicio	Una frase
IoT Hub	Hub de mensajería bidireccional entre dispositivos IoT y la nube
IoT Central	Aplicación SaaS lista para usar sobre IoT Hub, sin necesidad de desarrollo
Digital Twins	Modela relaciones y estados del mundo físico en gemelos digitales

12. Comparativas clave

12.1 IaaS vs PaaS vs SaaS

	IaaS	PaaS	SaaS
Ejemplo	Virtual Machines	App Service	Microsoft 365
Gestión SO	Cliente	Proveedor	Proveedor
Flexibilidad	Máxima	Media	Mínima
Velocidad de despliegue	Lenta	Rápida	Inmediata

12.2 VM vs App Service vs Containers vs Functions

	VM	App Service	Containers (AKS/ACI)	Functions
Gestión de SO	Cliente	Proveedor	Compartida (kernel host)	Ninguna
Escalado	Manual/VMSS	Automático	Orquestado	Automático, a cero
Facturación	Por VM encendida	Por plan	Por recurso consumido	Por ejecución
Ideal para	Legacy, control total	Apps web estándar	Microservicios portables	Eventos puntuales

12.3 Blob vs Files vs Queue vs Table

	Blob	Files	Queue	Table
Estructura	No estructurada	Sistema de archivos SMB/NFS	Mensajes FIFO	NoSQL clave-valor
Acceso típico	HTTP/REST	Montaje SMB	API de cola	API de tabla
Caso de uso	Objetos, backups, media	File share compartido	Desacoplar procesos	Datos semiestructurados masivos

12.4 Opciones de redundancia

	LRS	ZRS	GRS	GZRS	RA-GRS/RA-GZRS
Copias	3	3	6	6	6
Protege datacenter	✓	✓	✓	✓	✓
Protege región completa	✗	✗	✓	✓	✓
Lectura continua en secundaria	✗	✗	✗	✗	✓

12.5 VPN Gateway vs ExpressRoute

	VPN Gateway	ExpressRoute
Conexión	Sobre internet público, cifrada	Circuito privado dedicado
Coste	Menor	Mayor
Fiabilidad/latencia	Variable	Predecible, SLA alto
Caso de uso	Conexiones pequeñas/medias, presupuesto ajustado	Cargas críticas, gran volumen, cumplimiento estricto

12.6 RBAC vs Azure Policy vs Resource Locks

	RBAC	Azure Policy	Resource Locks
Controla	Quién actúa	Qué configuración es válida	Si un recurso se puede borrar/modificar
Se salta con permisos altos	N/A	No aplica a permisos	No , ni siquiera Owner
Ejemplo	Dar acceso Contributor	Exigir etiqueta obligatoria	Impedir borrar una VNet de producción

12.7 Azure Monitor vs Advisor vs Service Health

	Azure Monitor	Advisor	Service Health
Qué observa	Métricas y logs de tus recursos	Recomendaciones de mejora sobre tu configuración	Incidencias de la plataforma Azure
Proactivo/reactivo	Reactivo (alertas ante eventos)	Proactivo (recomienda antes de que falle)	Informativo (avisa de problemas externos a ti)

12.8 CapEx vs OpEx

	CapEx	OpEx
Pago	Adelantado, gran inversión inicial	Periódico, según consumo
Propiedad del activo	Sí	No
Modelo Azure	—	✓ Azure es 100% OpEx

13. Preguntas trampa

13.1 “¿Quién es responsable de X?” (responsabilidad compartida)

Escenario típico: “Una empresa usa Microsoft 365 (SaaS). ¿Quién es responsable de proteger los datos de los usuarios?” ✓ **Correcta: el cliente.** Aunque sea SaaS y Microsoft gestione toda la pila técnica, **datos, dispositivos e identidades son siempre responsabilidad del cliente**, en los tres modelos. ✗ Por qué falla la intuición: “SaaS = Microsoft gestiona todo” es cierto para infraestructura, **falso** para datos e identidad.

13.2 Escalabilidad vs Elasticidad

Escenario típico: “Un servicio añade automáticamente instancias cuando sube el tráfico y las retira cuando baja, sin intervención humana. ¿Qué característica es?” ✓ **Correcta: Elasticidad** (automática, dinámica). ✗ Trampa: “Escalabilidad” es la opción que muchos marcan, pero escalabilidad es el concepto general (puede ser manual); elasticidad implica automatismo en tiempo real.

13.3 RBAC vs Policy

Escenario típico: “Necesitas impedir que se creen storage accounts sin cifrado, sin importar qué usuario los cree. ¿Qué usarías?” ✓ **Correcta: Azure Policy.** ✗ Trampa: RBAC controla permisos de usuarios, no reglas de configuración de recursos.

13.4 Lock vs RBAC

Escenario típico: “Un usuario con rol Owner intenta eliminar un recurso, pero no puede. ¿Por qué?” ✓ **Correcta: hay un Resource Lock** `CanNotDelete` o `ReadOnly` **aplicado.** ✗ Trampa: pensar que Owner puede saltarse cualquier restricción — los locks son independientes del RBAC.

13.5 GRS vs RA-GRS

Escenario típico: “Necesitas poder leer tus datos desde la región secundaria en todo momento, no solo tras un desastre. ¿Qué redundancia eliges?” ✓ **Correcta: RA-GRS** (o RA-GZRS si además necesitas resiliencia zonal en la primaria). ✗ Trampa: elegir GRS a secas — GRS replica pero **no permite lectura** de la secundaria salvo failover.

13.6 VPN Gateway vs ExpressRoute

Escenario típico: “Una empresa necesita la máxima fiabilidad y baja latencia predecible para tráfico crítico entre su datacenter y Azure, y el presupuesto no es la principal restricción.” ✓ **Correcta: ExpressRoute.** ✗ Trampa: elegir VPN Gateway “porque es más barato” cuando el enunciado prioriza fiabilidad/latencia, no coste.

13.7 Region Pair vs Availability Zone

Escenario típico: “¿Qué protege a una aplicación si se cae por completo una región entera de Azure?” ✓ **Correcta: replicación a la región emparejada (region pair)**, no Availability Zones. ✗ Trampa: las Availability Zones protegen contra fallo de **un datacenter**, no de la región completa.

13.8 Azure Arc

Escenario típico: “Una empresa quiere aplicar Azure Policy y monitorización de Azure Monitor sobre servidores físicos on-premises, sin migrarlos a la nube.” ✓ **Correcta: Azure Arc.** ✗ Trampa: pensar que hay que migrar los servidores a VMs de Azure primero — Arc los gestiona **in situ**.

13.9 Availability Set vs Availability Zone (segunda vuelta)

Escenario típico: “Necesitas que tu aplicación siga funcionando si se incendia el datacenter completo donde corre, no solo si falla un servidor.” ✓ **Correcta: Availability Zones** (datacenters físicamente separados dentro de la región). ✗ Trampa: elegir Availability Set — solo protege de fallos de hardware **dentro** del mismo datacenter, no de la pérdida total del edificio.

13.10 Hot/Cool/Cold vs Archive

Escenario típico: “Necesitas guardar backups legales durante 7 años, con acceso extremadamente infrecuente y el menor coste posible; ocasionalmente auditoría pide un fichero con margen de horas.” ✓ **Correcta: Archive tier.** ✗ Trampa: elegir Cool o Cold “por si acaso necesito acceso rápido” — el enunciado ya admite horas de espera, así que Archive es la opción de coste mínimo correcta.

13.11 Conditional Access vs MFA

Escenario típico: “Quieres exigir un segundo factor de autenticación solo cuando el inicio de sesión provenga de un país no habitual, no siempre.” ✓ **Correcta: Conditional Access** (con MFA como resultado de la política condicional). ✗ Trampa: responder solo “MFA” — MFA es el mecanismo, Conditional Access es el motor de reglas que decide **cuándo** exigirlo.

13.12 Serverless vs PaaS

Escenario típico: “Un desarrollador quiere ejecutar una pequeña pieza de código solo cuando llega un archivo nuevo a un contenedor de Blob Storage, sin pagar nada mientras no ocurre nada.” ✓ **Correcta: Azure Functions.** ✗ Trampa: responder App Service — App Service (PaaS) sigue facturando por el plan aunque la app esté inactiva; Functions en plan de consumo puede escalar a cero coste.

14bis. Glosario rápido A-Z

Término	Definición en una línea
ARM (Azure Resource Manager)	Motor de despliegue y gestión que procesa todas las peticiones a recursos de Azure
AzCopy	Herramienta CLI para copiar datos masivamente hacia/desde Storage
Azure Arc	Extiende gestión de Azure a recursos fuera de Azure
Azure Advisor	Recomendador proactivo de coste/seguridad/fiabilidad/rendimiento/excelencia operacional
Bicep	DSL declarativo que se transpila a plantillas ARM
Conditional Access	Motor de reglas de acceso condicional basadas en señales de contexto
Defender for Cloud	Plataforma CSPM/CWP de postura de seguridad y protección de cargas
ExpressRoute	Conexión privada dedicada entre on-prem y Azure
Fault domain	Agrupación lógica por hardware físico compartido dentro de un Availability Set
Management Group	Agrupación de suscripciones para aplicar gobernanza a gran escala
Microsoft Entra ID	Servicio de identidad cloud-native de Microsoft (antes Azure AD)
Microsoft Purview	Familia de servicios de gobernanza y cumplimiento de datos
RBAC	Control de acceso basado en roles: identidad + rol + ámbito
Region pair	Región emparejada con otra de la misma geografía para DR coordinado
Resource Group	Contenedor lógico de recursos con ciclo de vida conjunto
Resource Lock	Bloqueo que impide borrar/modificar un recurso, independiente del RBAC
Scale Set (VMSS)	Grupo de VMs idénticas con autoescalado
Tenant	Instancia dedicada de Microsoft Entra ID que representa a la organización
Update domain	Agrupación lógica para escalar reinicios de mantenimiento planificado
Zero Trust	Modelo de seguridad: verificar siempre, mínimo privilegio, asumir brecha

14ter. Simulacro rápido — 15 preguntas

Formato similar al examen real. Tápate las respuestas y respóndelas en menos de 60 segundos cada una.

1. Una empresa necesita reutilizar licencias de Windows Server ya compradas para reducir el coste de sus VMs en Azure. ¿Qué modelo de precio usa?

Respuesta: Azure Hybrid Benefit.

2. ¿Qué componente de Azure Monitor se usa específicamente para analizar el rendimiento de una aplicación web (tiempos de respuesta, errores)?

Respuesta: Application Insights.

3. Una organización quiere que cierta configuración de red se aplique automáticamente a todas las suscripciones bajo un mismo departamento. ¿Qué nivel de la jerarquía usarías para aplicar la política?

Respuesta: Management Group.

4. ¿Qué tipo de redundancia de Storage ofrece la protección más alta **sin** salir de la región primaria?

Respuesta: ZRS (Zone Redundant Storage).

5. Un equipo de desarrollo necesita ejecutar contenedores sin gestionar un clúster completo, solo cargas puntuales y simples. ¿Qué servicio encaja mejor?

Respuesta: Azure Container Instances (ACI).

6. ¿Verdadero o falso? Un Resource Lock de tipo ReadOnly impide incluso que Azure Monitor recoja métricas del recurso.

Respuesta: Falso — ReadOnly impide cambios de configuración, no la lectura de telemetría.

7. ¿Qué modelo de responsabilidad compartida deja más tareas en manos del proveedor: IaaS o PaaS?

Respuesta: PaaS.

8. Una empresa quiere decidir si migrar su datacenter a Azure le compensa económicamente a 3 años vista. ¿Qué herramienta usa?

Respuesta: TCO Calculator.

9. ¿Qué servicio de Azure permite a un usuario externo (partner) colaborar usando su propia identidad corporativa?

Respuesta: Microsoft Entra External Identities (B2B).

10. ¿Qué diferencia principal hay entre Azure Policy en modo "Audit" y en modo "Deny"?

Respuesta: Audit permite la acción pero la marca como no conforme; Deny la bloquea directamente.

11. Una aplicación necesita escalar automáticamente el número de instancias según la carga en tiempo real, sin intervención manual. ¿Qué recurso de compute usarías como base?

Respuesta: Virtual Machine Scale Set (VMSS).

12. ¿Qué tipo de cuenta de Storage recomienda Microsoft por defecto para la mayoría de escenarios modernos?

Respuesta: Standard general-purpose v2.

13. ¿Cuál es la diferencia entre un endpoint público y un Private Endpoint en Azure?

Respuesta: El público es accesible desde internet; el Private Endpoint asigna una IP privada dentro de tu VNet y el tráfico nunca sale a internet.

14. Una empresa detecta que un recurso crítico fue borrado accidentalmente por un usuario con rol Contributor. ¿Qué medida lo habría evitado sin cambiar sus permisos RBAC?

Respuesta: Aplicar un Resource Lock CanNotDelete.

15. ¿Qué principio de Zero Trust se aplica cuando se limita el acceso de un usuario solo a los recursos estrictamente necesarios para su tarea, y solo durante el tiempo necesario?

Respuesta: Uso de acceso de mínimo privilegio (Just-In-Time / Just-Enough-Access).

14. Chuleta final — repaso de última hora

Léela la noche antes o en el transporte de camino al examen. Es el 20% del contenido que genera el 80% de las preguntas.

Responsabilidad compartida

Datos, dispositivos e identidad → siempre del cliente. El resto se desplaza al proveedor a medida que subes de IaaS → PaaS → SaaS.

Jerarquía

Tenant → Management Group → Subscription → Resource Group → Resource — herencia hacia abajo.

Resiliencia

- **Availability Set** → protege de fallo de hardware **dentro** de un datacenter (fault domain / update domain).
- **Availability Zone** → protege de fallo de **todo un datacenter**.
- **Region Pair** → protege de fallo de **toda una región**.

IaaS / PaaS / SaaS

IaaS = VMs (gestionas SO). PaaS = App Service, SQL DB (gestionas app y datos). SaaS = M365 (gestionas solo datos/usuarios).

Storage — redundancia

LRS (1 datacenter) < ZRS (varias AZ, misma región) < GRS (región emparejada, sin lectura) < RA-GRS (región emparejada, **con** lectura) < GZRS/RA-GZRS (ZRS + geo).

Storage — tiers

Hot (frecuente) → Cool (30+ días) → Cold (90+ días) → Archive (180+ días, requiere rehidratación, sin lectura inmediata).

Networking

VNet Peering = privado entre VNets. VPN Gateway = cifrado sobre internet público, barato. ExpressRoute = circuito privado dedicado, caro y predecible.

Identidad

Entra ID = identidad cloud-native (no es AD replicado). RBAC = quién puede actuar. Conditional Access = reglas “si-entonces” de acceso. Zero Trust = verificar siempre, mínimo privilegio, asumir brecha.

Gobernanza

RBAC = permisos de usuario. Policy = reglas de configuración de recursos. Locks = impiden borrar/modificar, **ni Owner los salta**.

Coste

Pricing Calculator = estimar **antes**. Cost Management = controlar **durante/después**. TCO Calculator = comparar on-prem vs Azure.

Herramientas de gestión

Portal (GUI) · CLI/PowerShell (scripting) · Cloud Shell (terminal en navegador) · Azure Arc (gestiona recursos **fuera** de Azure) · ARM/Bicep (IaC).

Monitorización

Advisor = recomienda (proactivo). Service Health = incidencias de la plataforma. Resource Health = estado de tus recursos. Azure Monitor = métricas/logs (Log Analytics + Alerts + Application Insights).

Términos que NO son objetivo oficial de AZ-900

BD (SQL/Cosmos), IA (OpenAI/Vision/Speech), Analítica (Synapse/Databricks), IoT, NSG/Firewall/Load Balancer/App Gateway/CDN en detalle, Blueprints (deprecado). Repásalos solo por encima.

15. Checklist final

Marca cada casilla solo cuando puedas explicarla **en voz alta, sin mirar el documento**, en una frase.

Conceptos Cloud

- Sé definir cloud computing y sus 5 características
- Sé dibujar de memoria la tabla de responsabilidad compartida (on-prem/IaaS/PaaS/SaaS)
- Sé diferenciar público, privado e híbrido, con un caso de uso cada uno
- Sé explicar CapEx vs OpEx y por qué Azure es OpEx
- Sé diferenciar escalabilidad de elasticidad
- Sé qué significa serverless (y qué NO significa)
- Sé diferenciar IaaS, PaaS y SaaS con un ejemplo de Azure cada uno

Arquitectura

- Sé recitar la jerarquía Tenant → Management Group → Subscription → Resource Group → Resource
- Sé qué es un region pair y para qué sirve
- Sé diferenciar Availability Zone de Availability Set
- Sé que un resource group no obliga a que sus recursos estén en la misma región

Compute y redes

- Sé comparar VMs, containers y Functions
- Sé qué son fault domains y update domains
- Sé listar los recursos mínimos que necesita una VM
- Sé diferenciar VPN Gateway de ExpressRoute
- Sé qué es VNet Peering
- Sé diferenciar endpoint público de privado

Storage

- Sé cuándo usar Blob, Files, Queue y Table
- Sé ordenar los tiers de Blob (Hot/Cool/Cold/Archive) y sus restricciones
- Sé explicar LRS, ZRS, GRS, GZRS y la diferencia de las variantes RA-
- Sé para qué sirven AzCopy, Storage Explorer, File Sync, Azure Migrate y Data Box

Identidad y seguridad

- Sé qué es Microsoft Entra ID y en qué se diferencia de AD Domain Services clásico
- Sé qué son SSO, MFA y passwordless
- Sé qué es Conditional Access
- Sé qué hace RBAC y cómo se compone (identidad + rol + ámbito)
- Sé explicar Zero Trust con sus 3 principios
- Sé qué es defensa en profundidad
- Sé qué hace Microsoft Defender for Cloud

Gestión de costes

- Sé diferenciar Pricing Calculator, TCO Calculator y Cost Management
- Sé para qué sirven las tags

Gobernanza

- Sé qué hace Microsoft Purview a alto nivel
- Sé qué hace Azure Policy y diferenciarlo de RBAC
- Sé qué son los Resource Locks y que ni Owner los salta

Herramientas

- Sé diferenciar Portal, CLI, PowerShell y Cloud Shell
- Sé qué hace Azure Arc
- Sé qué es IaC y diferenciar ARM de Bicep a alto nivel

Monitorización

- Sé diferenciar Advisor, Service Health y Resource Health
- Sé qué son Log Analytics, Alerts y Application Insights dentro de Azure Monitor

Preguntas trampa

Repasé las 8 preguntas trampa de la sección 13 y entiendo por qué falla la opción intuitiva en cada una

AZ-900 Study Guide — Versión 2026 · Basado en el skills outline oficial de Microsoft Learn actualizado el 14 de enero de 2026 (última verificación: 23 de noviembre de 2025)
· Documento de repaso intensivo, no sustituye la práctica hands-on en el portal de Azure.