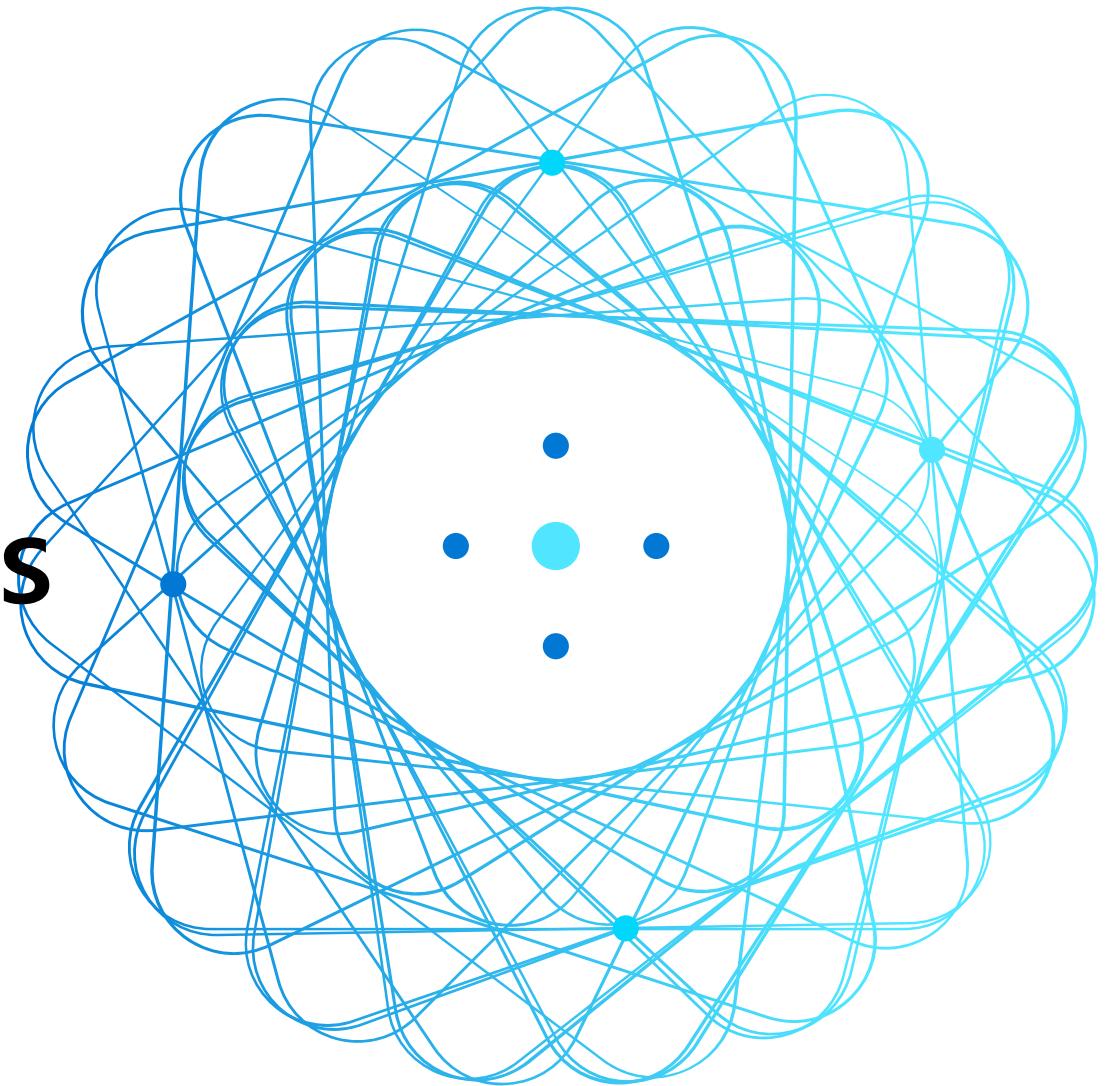
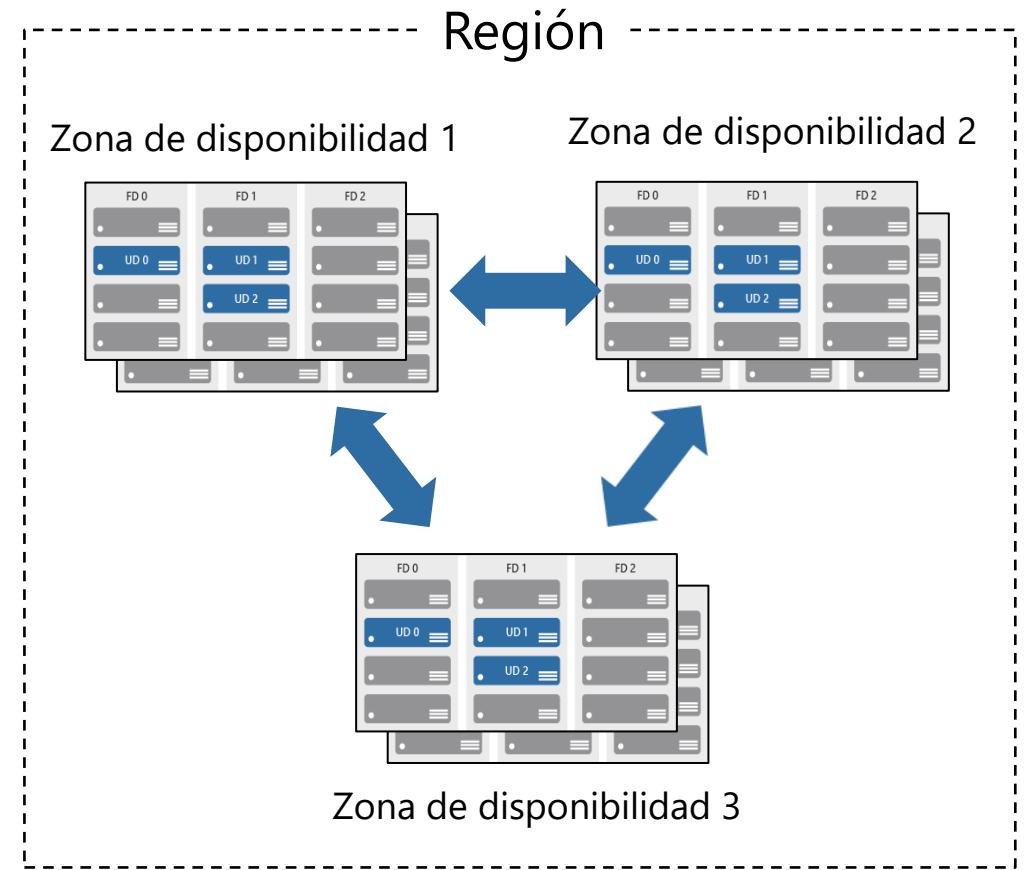


Arquitectura y servicios



Zonas de disponibilidad

- Proporcione protección contra el tiempo de inactividad debido a errores del centro de datos.
- Centros de datos separados físicamente dentro de una misma región.
- Cada centro de datos está equipado con redes, alimentación y refrigeración independientes.
- Con conexiones de red privadas de fibra óptica.



Pares de región

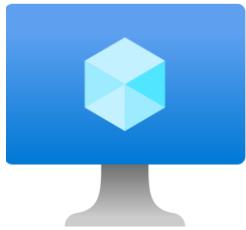
- Al menos 500 km de separación entre pares de regiones.
- Replicación automática para algunos servicios.
- Se prioriza la recuperación de una región en caso de interrupción.
- Las actualizaciones se implementan secuencialmente para minimizar el tiempo de inactividad.

Vínculo de la web: <https://aka.ms/PairedRegions-spa>

Region	Region
Centro-norte de EE. UU.	Centro-sur de EE. UU.
Este de EE. UU.	Oeste de EE. UU.
Oeste de EE. UU. 2	Centro-oeste de EE. UU.
Este de EE.UU. 2	Centro de EE. UU.
Centro de Canadá	Este de Canadá
Norte de Europa	Oeste de Europa
Oeste del Reino Unido	Sur de Reino Unido
Centro de Alemania	Nordeste de Alemania
Sudeste de Asia	Este de Asia
Este de China	Norte de China
Este de Japón	Oeste de Japón
Sudeste de Australia	Este de Australia
Sur de la India	Centro de la India
Sur de Brasil (Primario)	Centro-sur de EE. UU.

Recursos de Azure.

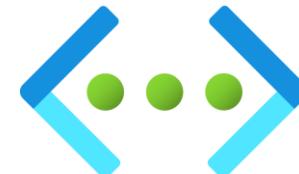
Los **recursos** de Azure son componentes como almacenamiento, máquinas virtuales y redes que están disponibles para crear soluciones en la nube.



Virtual Machines



Cuentas de
almacenamiento



Virtual Networks



Servicios de
aplicaciones



Instancias de
SQL Database



Functions

Grupos de recursos

Un **grupo de recursos** es un contenedor para administrar y agregar recursos en una sola unidad.

- Los recursos solo pueden estar presentes en un único grupo.
- Los recursos pueden estar en diferentes regiones.
- Los recursos se pueden trasladar a otros grupos de recursos.
- Las aplicaciones pueden utilizar varios grupos de recursos.

Grupos de recursos
(web + BD, VM, almacenamiento) en un grupo



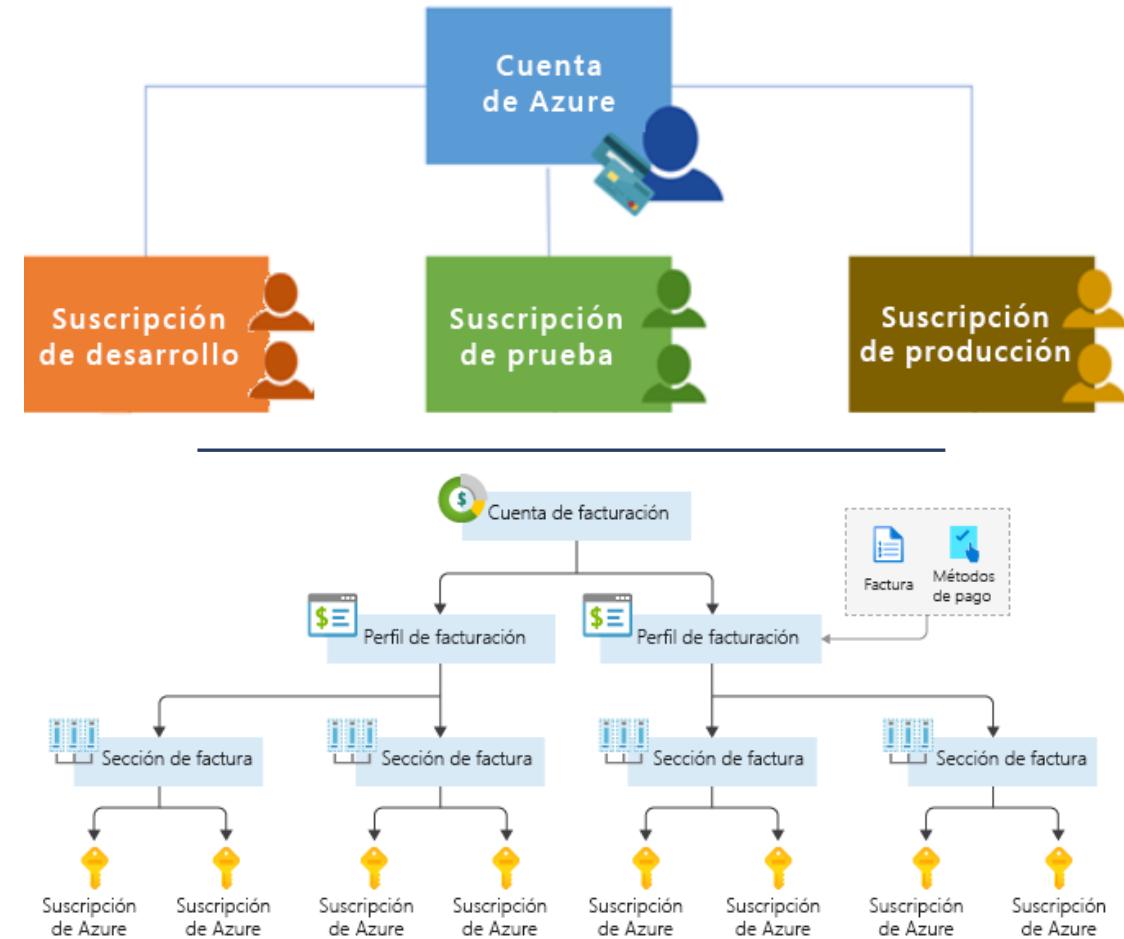
O BIEN



Suscripciones

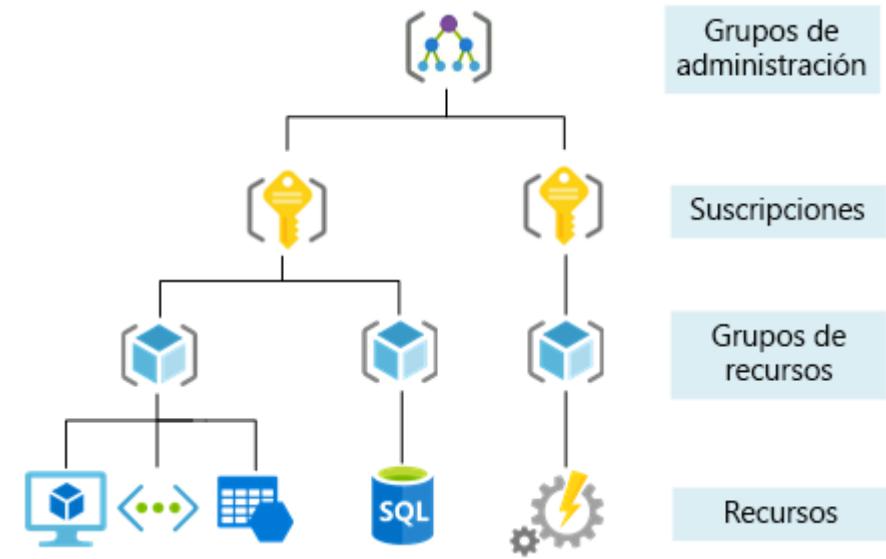
Una suscripción le proporciona acceso autenticado y autorizado a las cuentas.

- **Límite de facturación:** genere informes de facturación y facturas independientes para cada suscripción.
- **Límite de control de acceso:** administre y controle el acceso a los recursos que los usuarios pueden aprovisionar con suscripciones específicas.



Grupos de administración

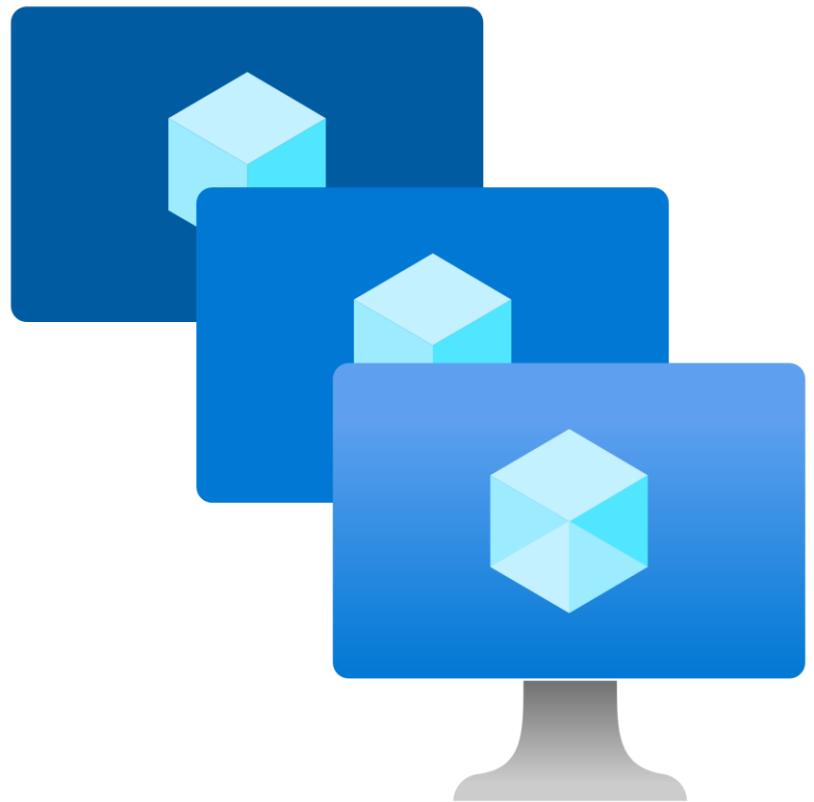
- Los grupos de administración pueden incluir varias suscripciones.
- Las suscripciones heredan las condiciones aplicadas al grupo de administración.
- Se admiten 10 000 grupos de administración en un único directorio.
- Un árbol de grupo de administración puede admitir hasta seis niveles de profundidad.



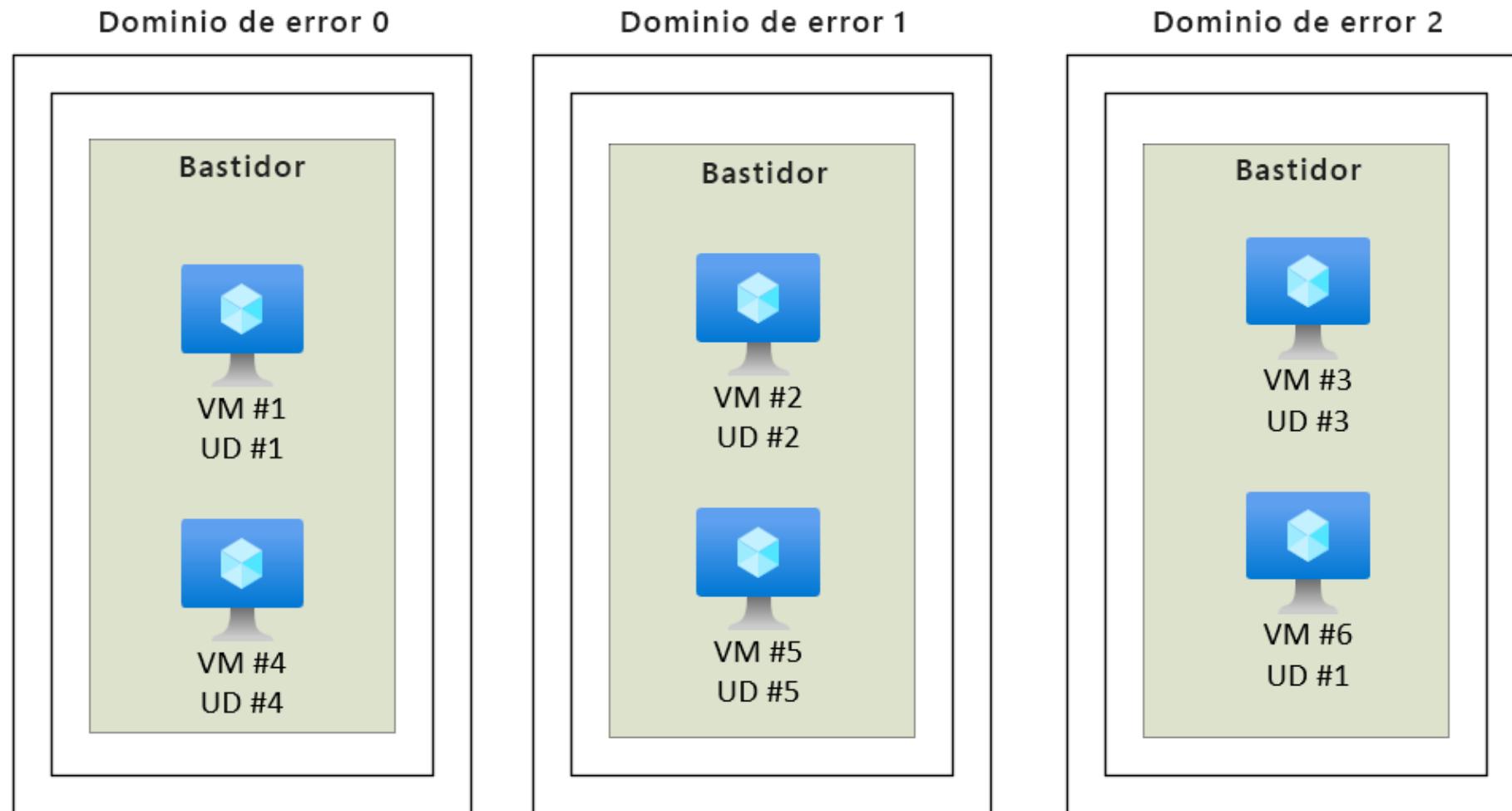
VM Scale Sets

Los conjuntos de escalado proporcionan una oportunidad de carga equilibrada para escalar automáticamente los recursos.

- Escala horizontalmente cuando aumenten las necesidades de recursos.
- Escala verticalmente cuando las necesidades de recursos sean menores.



Conjuntos de disponibilidad de máquina virtual



Azure Virtual Desktop

Azure Virtual Desktop es la virtualización de aplicaciones y escritorios que se ejecuta en la nube.

- Crear un entorno de virtualización de escritorio completo sin tener que ejecutar servidores de puerta de enlace adicionales.
- Reduzca el riesgo de que los recursos se queden atrás.
- Implementaciones de varias sesiones verdaderas.

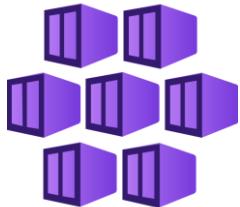


Azure Container Services

Los **contenedores** de Azure son un entorno virtualizado ligero que no requiere administración del sistema operativo y puede responder a los cambios bajo demanda.



Azure Container Instances: una oferta de PaaS que ejecuta un contenedor en Azure sin la necesidad de administrar una máquina virtual o servicios adicionales.



Azure Kubernetes Service: un servicio de organización completo para contenedores con arquitecturas distribuidas y grandes volúmenes de contenedores.

Azure Functions

Azure Functions



Código basado en eventos que ejecuta su servicio y no la infraestructura subyacente.

Comparación de opciones de proceso de Azure

Máquinas virtuales

Servidor basado en la nube que admite entornos de Windows o Linux.

Útiles para las migraciones mediante lift-and-shift a la nube.

Paquete completo del sistema operativo, incluido el sistema operativo host.

Virtual Desktop

Proporciona una experiencia de escritorio de Windows para equipo personal basada en la nube.

Aplicaciones dedicadas para conectarse y usar, o accesibles desde cualquier explorador moderno.

El inicio de sesión de varios clientes permite a varios usuarios iniciar sesión en la misma máquina al mismo tiempo.

Contenedores

Entorno ligero y en miniatura adecuado para ejecutar microservicios.

Diseñado para escalabilidad y resistencia a través de la orquestación.

Las aplicaciones y los servicios se empaquetan en un contenedor que se encuentra sobre el sistema operativo host. Varios contenedores pueden sentarse en un sistema operativo host.

Azure App Services



Azure **App Services** es una plataforma totalmente administrada para crear, implementar y escalar aplicaciones web y API rápidamente.

- Funciona con .NET, .NET Core, Node.js, Java, Python o php.
- Oferta de PaaS con requisitos de cumplimiento, seguridad y rendimiento de nivel empresarial.

Servicios de redes de Azure



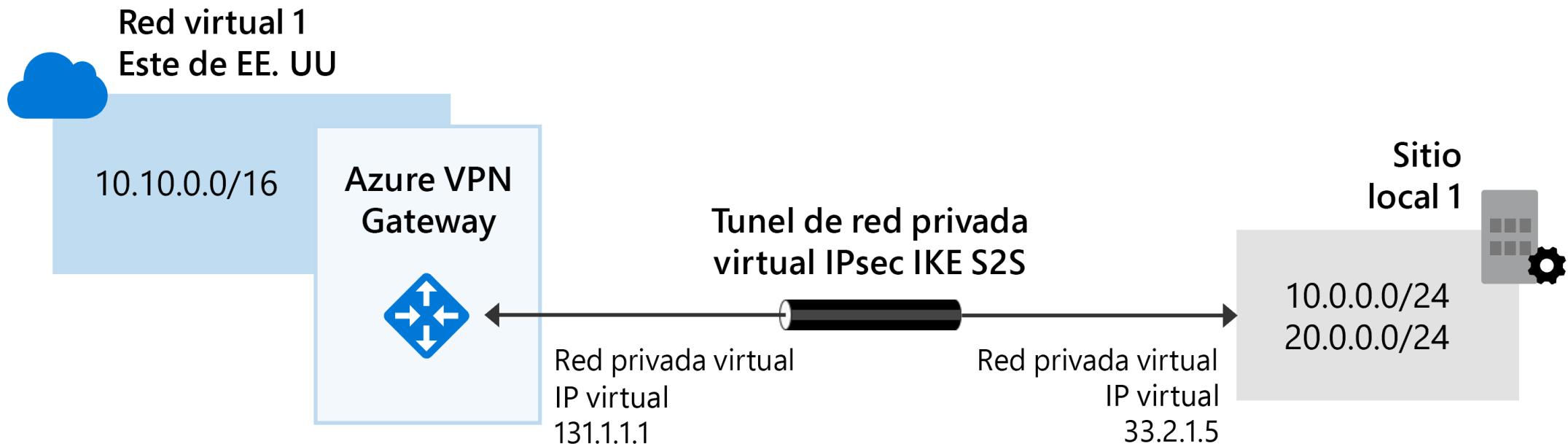
Azure Virtual Network (VNet) permite que los recursos de Azure se comuniquen entre sí, con Internet y con redes locales.

- Puntos de conexión públicos, accesibles desde cualquier lugar de Internet
- Puntos de conexión privados, accesibles solo desde dentro de la red
- Subredes virtuales, para segmentar la red y satisfacer sus necesidades
- Emparejamiento de redes, para la conexión directa de redes privadas

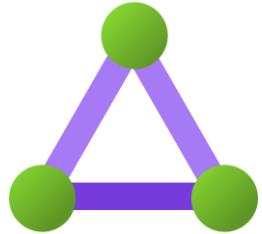
Servicios de redes de Azure



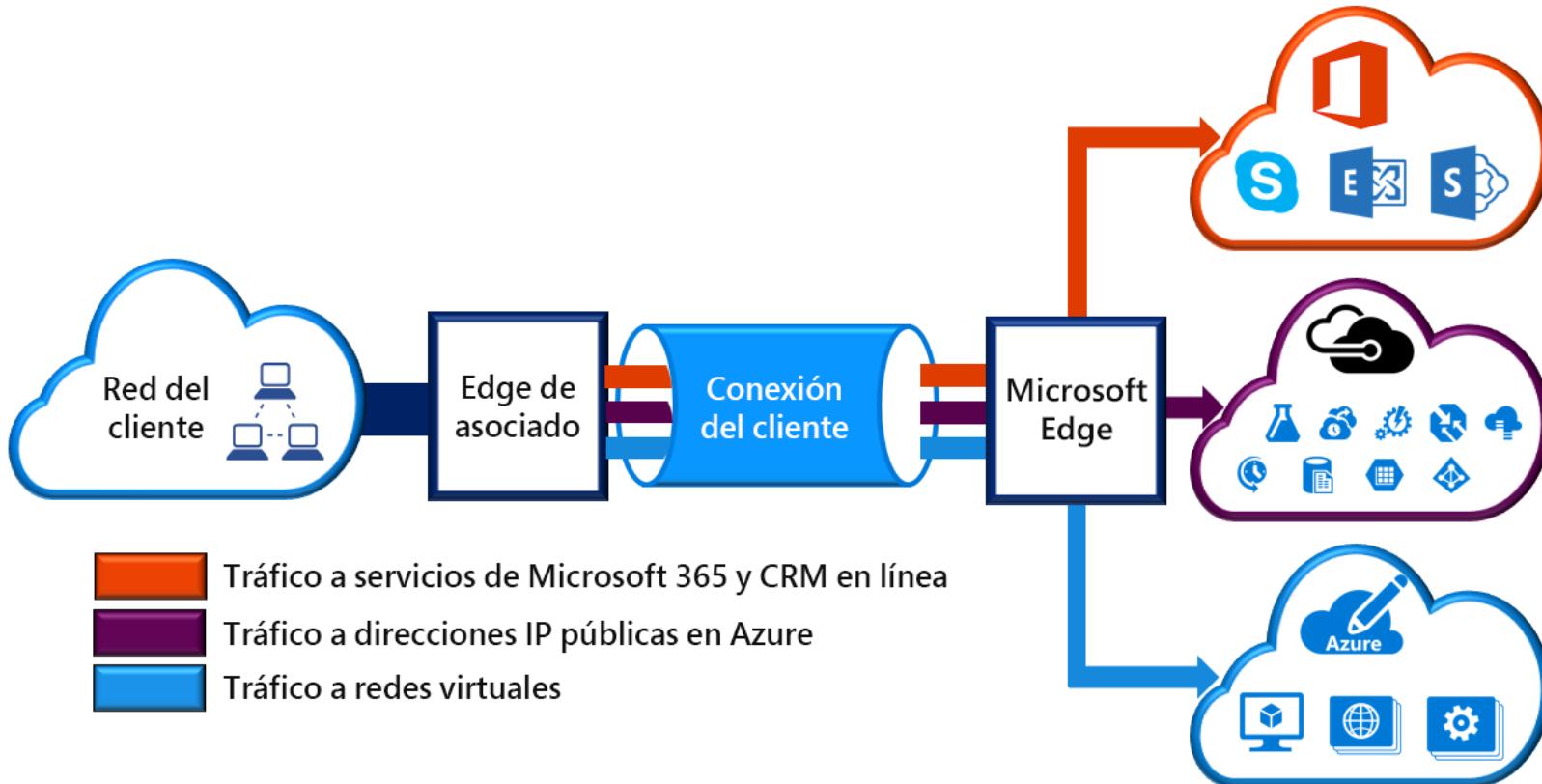
Virtual Private Network Gateway (VPN) se usa para enviar tráfico cifrado entre una red virtual de Azure y una ubicación local a través de Internet público.



Servicios de redes de Azure



Azure Express Route extiende las redes locales a Azure a través de una conexión privada que facilita un proveedor de conexión.



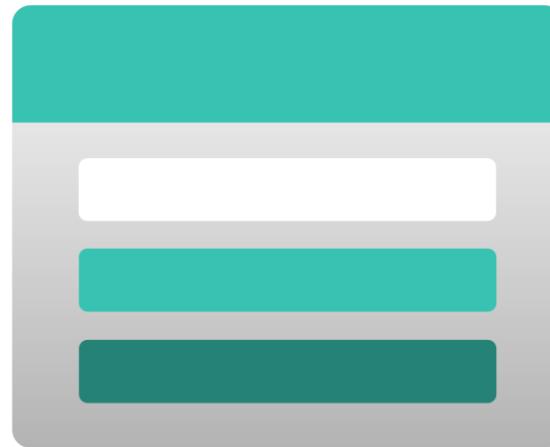


Azure DNS

- Confiabilidad y rendimiento aprovechando una red global de servidores de nombres de dominio mediante redes de Anycast.
- La seguridad de Azure DNS se basa en Azure Resource Manager, lo que permite el control de acceso basado en rol y la supervisión y el registro.
- Facilidad de uso para administrar los recursos externos y de Azure con un único servicio DNS.
- Las redes virtuales personalizables le permiten usar nombres de dominio privados y totalmente personalizados en las redes virtuales privadas.
- Los registros de alias admiten conjuntos de registros de alias para que apunten directamente a un recurso de Azure.

Cuentas de almacenamiento

- Deben tener un nombre único global.
- Suministro de acceso mediante Internet en todo el mundo.
- Determinación de los servicios de almacenamiento y las opciones de redundancia



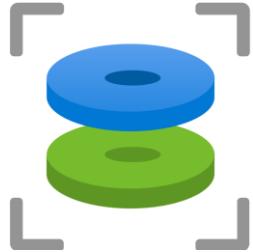
Redundancia de almacenamiento

Configuración de redundancia	Implementación	Durabilidad.
Almacenamiento con redundancia local (LRS)	Centro de datos único en la región primaria	11 nueves
Almacenamiento con redundancia de zona (ZRS)	Tres zonas de disponibilidad en la región primaria	12 nueves
Almacenamiento con redundancia geográfica (GRS)	Centro de datos único en la región primaria y secundaria	16 nueves
Almacenamiento con redundancia de zona geográfica (GZRS)	Tres zonas de disponibilidad en la región primaria y un único centro de datos en la región secundaria	16 nueves

Servicios de Azure Storage



El **almacenamiento en contenedores (Blob Storage)** está optimizado para almacenar cantidades masivas de datos no estructurados, como texto o datos binarios.



Disk Storage proporciona discos para que las máquinas virtuales, aplicaciones y otros servicios accedan y los usen.

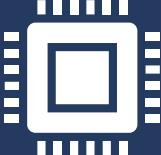


Azure Files configura recursos compartidos de archivos de red de alta disponibilidad a los que se puede acceder mediante el protocolo estándar de Bloqueo de mensajes del servidor (SMB).

Puntos de conexión públicos del servicio de Storage

Servicio de Storage	Punto de conexión público
Blob Storage	<code>https://<storage-account-name>.blob.core.windows.net</code>
Data Lake Storage Gen2	<code>https://<storage-account-name>.dfs.core.windows.net</code>
Azure Files	<code>https://<storage-account-name>.file.core.windows.net</code>
Queue Storage	<code>https://<storage-account-name>.queue.core.windows.net</code>
Table Storage	<code>https://<storage-account-name>.table.core.windows.net</code>

Niveles de acceso al almacenamiento de Azure

 Acceso frecuente	 Acceso esporádico	 Archivo
Optimizado para almacenar datos a los que se accede con frecuencia.	Optimizado para almacenar datos a los que se accede con poca frecuencia y se almacenan durante al menos 30 días.	Optimizado para almacenar datos a los que rara vez se accede y se almacenan durante al menos 180 días con requisitos de latencia flexibles.

Puede cambiar entre estos niveles de acceso en cualquier momento.

Azure Migrate

- Plataforma de migración unificada
- Gama de herramientas integradas e independientes
- Evaluación y migración



Azure Data Box

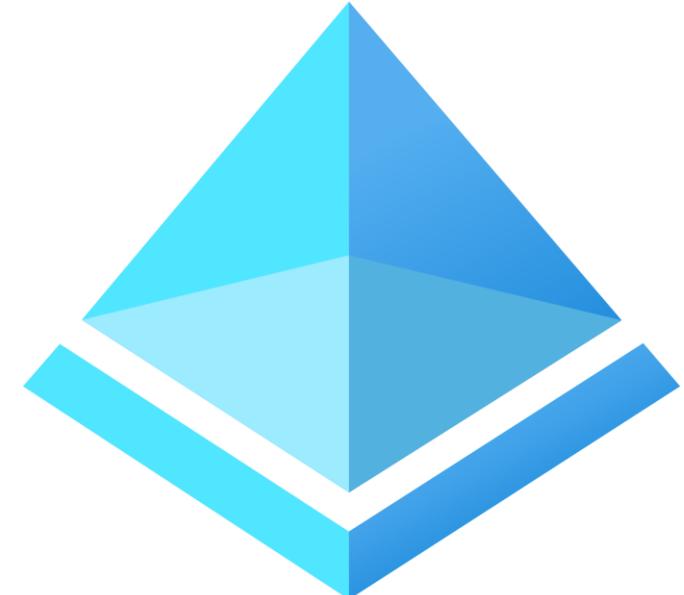
- Almacene hasta 80 terabytes de datos.
- Traslade sus copias de seguridad de recuperación ante desastres a Azure.
- Proteja sus datos en una funda resistente durante el tránsito.
- Mueva datos fuera de Azure para satisfacer los requisitos de cumplimiento normativo.
- Mueva datos a Azure desde ubicaciones remotas con conectividad limitada o sin conectividad.



Azure Active Directory (AAD)

Azure Active Directory (AAD) es el servicio de administración de identidad y acceso basado en la nube de Microsoft Azure.

- Autenticación (los empleados inician sesión para acceder a los recursos).
- Inicio de sesión único (SSO).
- Administración de aplicaciones.
- Negocio a negocio (B2B).
- Servicios de identidad de negocio a cliente (B2C).
- Administración de dispositivos.



Azure Active Directory Domain Services (Azure AD DS)



- Todas las ventajas de los servicios de dominio basados en la nube sin administrar controladores de dominio
- Ejecución de aplicaciones heredadas (que no pueden usar estándares de autenticación modernos) en la nube
- Sincronización automática desde Azure AD

Diferencias entre autenticación y autorización

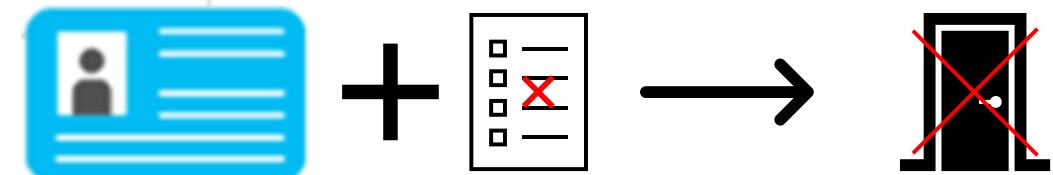
Authentication

- Identifica a la persona o el servicio que intenta acceder a un recurso.
- Solicita credenciales de acceso legítimas.
- Bases para crear principios seguros de identidad y control de acceso.



Authorization

- Determina el nivel de acceso de una persona o servicio autenticados.
- Define a qué datos pueden acceder y qué pueden hacer con ellos.



Azure Multi-Factor Authentication

Proporciona seguridad adicional para sus identidades al requerir dos o más elementos para la autenticación completa.

- Algo que sabe ↔ Algo que posee ↔ Algo que es



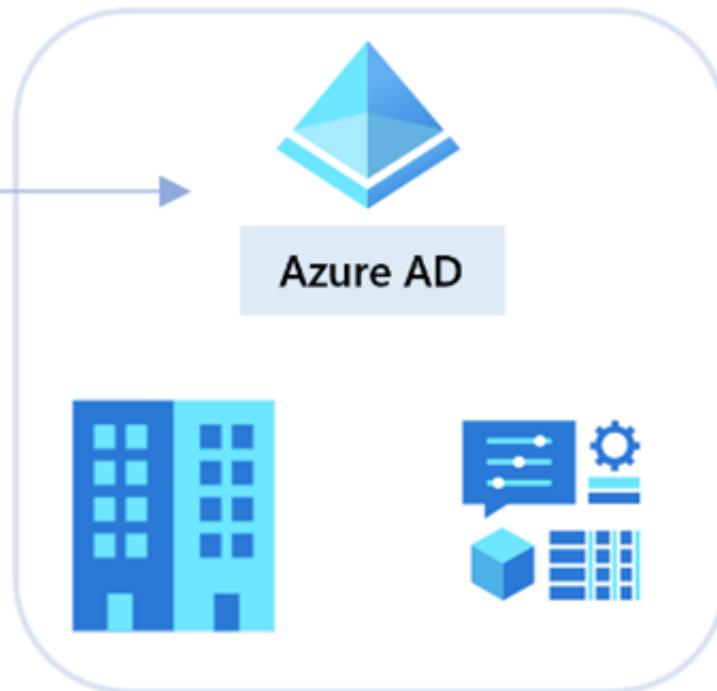
External Identities B2B

Colaboración B2B



socios, proveedores,
otros colaboradores

invitación o registro
de autoservicio



Su inquilino

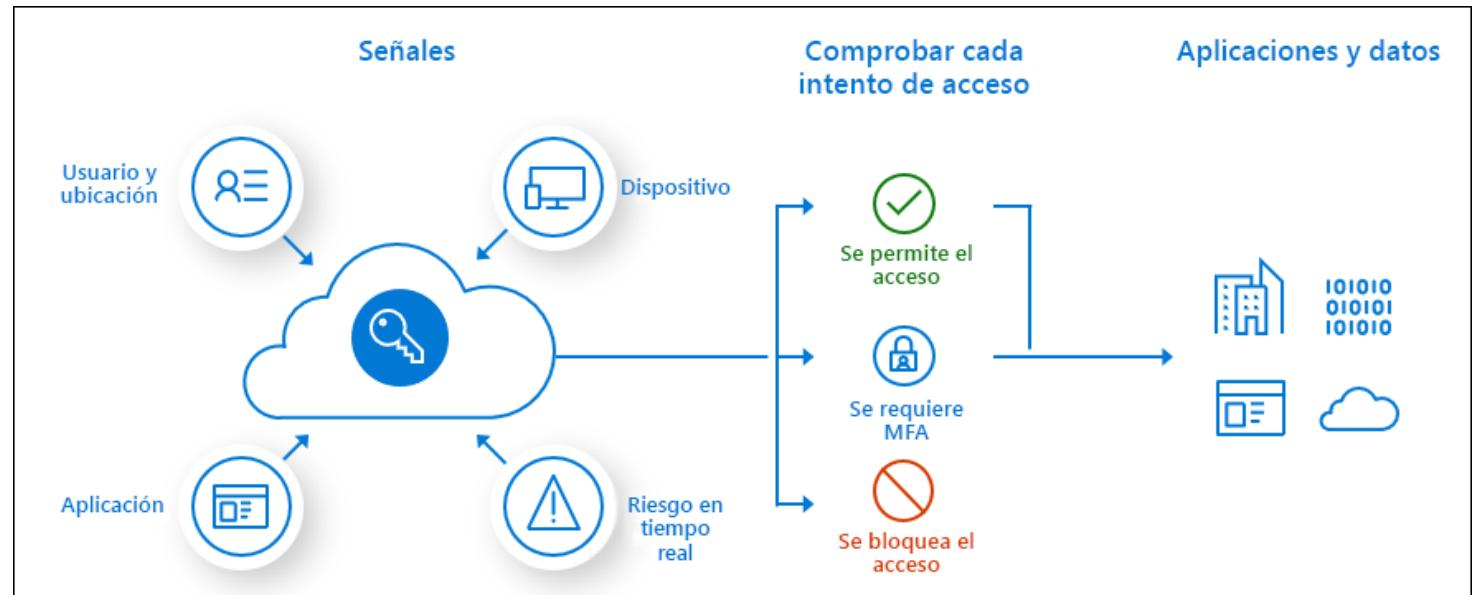
External Identities B2C



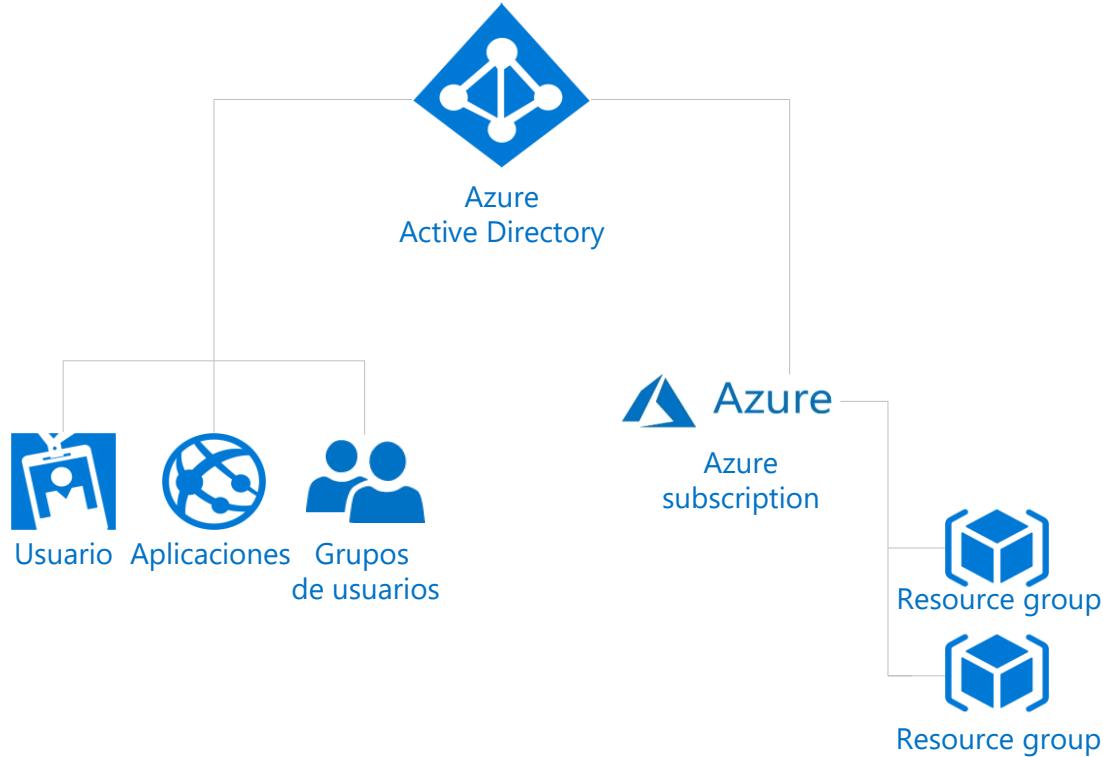
Acceso condicional

El acceso condicional es lo que usa Azure Active Directory para reunir señales, tomar decisiones y aplicar las directivas de la organización.

- Usuario o pertenencia a un grupo
- Ubicación de la IP
- Dispositivo
- Application
- Detección de riesgos



Control de acceso basado en roles de Azure (RBAC de Azure)

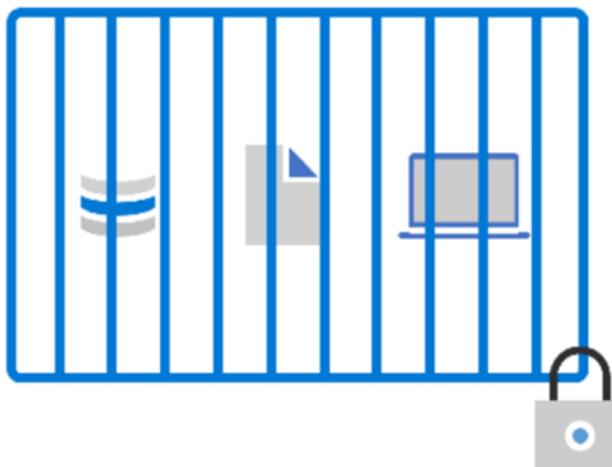


- Administración de acceso específico.
- Separe las tareas dentro del equipo y conceda a los usuarios solo el acceso que necesitan para realizar sus trabajos.
- Permite el acceso a Azure Portal y controlar el acceso a los recursos.

Confianza cero

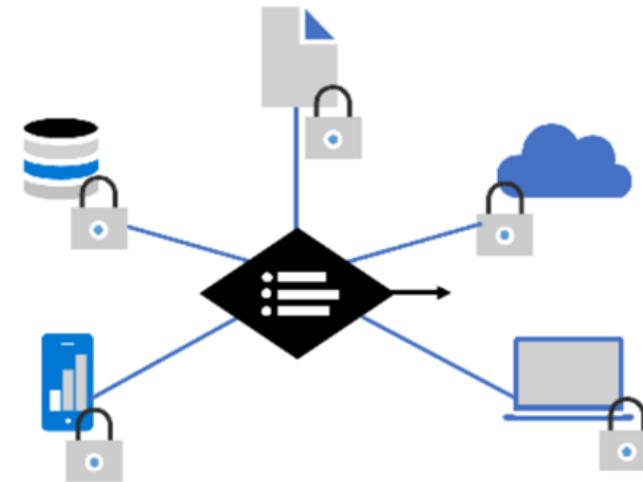
Proteja los recursos estén donde estén con Zero Trust

Simplifique la seguridad y mejore su efectividad



Enfoque clásico

Restringir todo a una red 'segura'

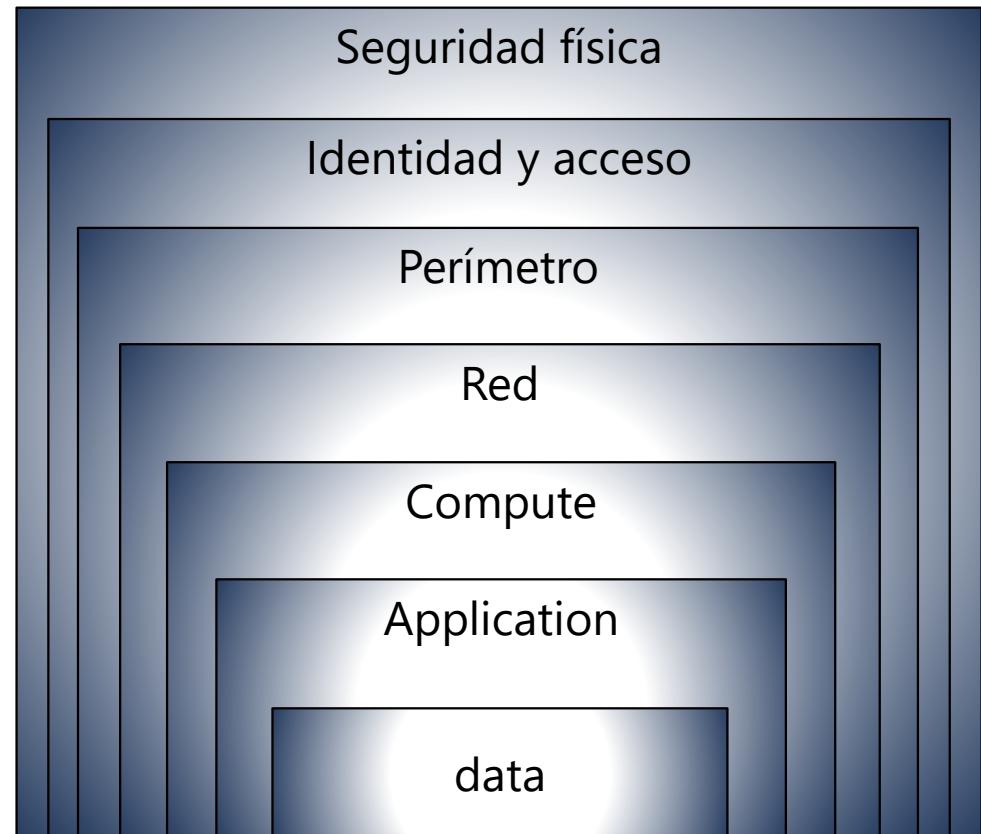


Zero Trust

Proteja los recursos allí donde estén con una directiva central

Defensa en profundidad

- Un enfoque por capas para asegurar los sistemas informáticos.
- Proporciona múltiples niveles de protección.
- Los ataques contra una capa están aislados de las capas subsiguientes.



Microsoft Defender for Cloud

Microsoft Defender for Cloud es un servicio de supervisión que proporciona protección contra amenazas, tanto en Azure como en los centros de datos locales.

- Proporciona recomendaciones de seguridad.
- Detecta y bloquea malware.
- Analiza e identifica posibles ataques.
- Control de acceso para los puertos cuando es necesario.

The screenshot shows the Microsoft Defender for Cloud Information General dashboard. At the top, it displays four key metrics: 4 Suscripciones de Azure, 9 Recursos evaluados, 4 Recomendaciones activas, and 67 Alertas de seguridad. Below these are several cards providing detailed information:

- Posición de seguridad:** Shows a 96% security score across Azure, AWS, and GCP. It includes a button to "Explore su posición de seguridad".
- Protecciones de cargas de trabajo:** Shows 100% coverage of resources for total protection, with 2 plans of resources. It includes a chart of alerts by severity (0 High, 46 Medium, 21 Low) and a link to "Mejorar las funcionalidades de protección contra amenazas".
- Cumplimiento normativo:** Shows an Azure Security Benchmark score of 34 de 43 controls superados. It includes a link to "Mejorar su cumplimiento".
- Firewall Manager:** Shows 5 Firewalls, 3 Firewall rules, and 4 Regions with firewalls. It includes a link to "Mejorar la seguridad de la red".
- Inventario:** Shows 0 virtual machines without supervision and 9 total resources. It includes a link to "Explorar los recursos".
- Information Protection:** Shows 0 sensitive data discovered with Purview integration. It includes a link to "Descubrir ahora".

On the right side, there are two sections:

- Actualizar al nuevo plan de contenedores:** Describes the "Nuevo plan" which combines existing Defender features with new ones like native Kubernetes security, vulnerability evaluation, and threat protection.
- Libro de estimación de costos para el plan del contenedor:** Provides an estimation of costs for the container plan, mentioning AKS V Azure Arc, and the number of images per container included for digitalization.

At the bottom, there are sections for "Recomendaciones más habituales (por recursos)" and "Ver en el repositorio de GitHub > Implementación de plantillas de ARM >".