**Introducción a los aspectos básicos de Microsoft Azure**

Microsoft Azure es una plataforma de informática en la nube con un conjunto de servicios que se amplía continuamente para ayudarle a crear soluciones que satisfagan sus objetivos empresariales.

Azure tiene servicios web sencillos para hospedar su presencia empresarial en la nube.

Servicios:

* Almacenamiento remoto
* Bases de datos
* Administración centralizada de cuentas
* inteligencia artificial (IA)
* servicios centrados en el Internet de las cosas (IoT)

Conceptos como:

* responsabilidad compartida.
* modelos en la nube diferentes
* método único de precios para la nube

**Qué es la informática en la nube**

Prestación de servicios informáticos a través de Internet.

**Descripción del modelo de responsabilidad compartida.**

Proveedor:

* La seguridad física, la alimentación,
* la refrigeración
* la conectividad de red

Consumidor:

* seguridad de acceso

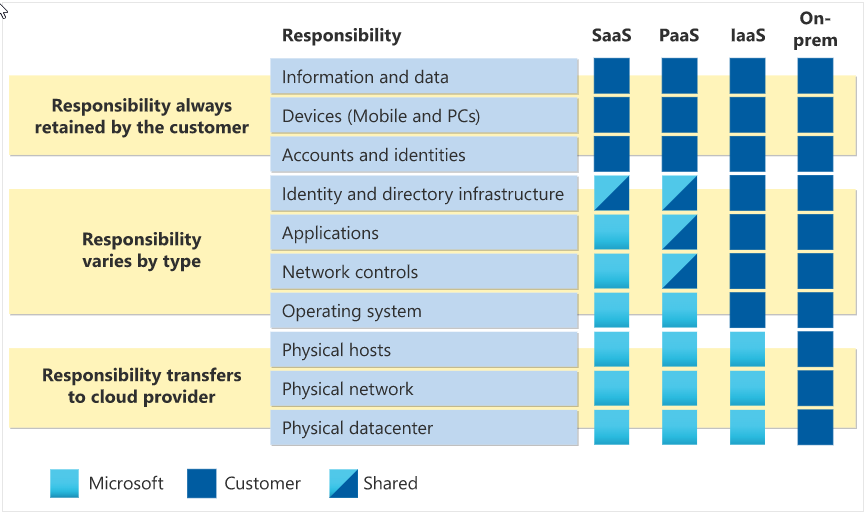
El modelo de responsabilidad compartida está muy vinculado a los tipos de servicio en la nube.

* infraestructura como servicio (IaaS),
* plataforma como servicio (PaaS)
* software como servicio (SaaS)

IaaS sitúa la mayor responsabilidad en el **consumidor** y el **proveedor** de servicios en la nube es el responsable de los conceptos básicos de seguridad física, energía y conectividad.

PaaS: siendo un punto intermedio entre IaaS y SaaS, se encuentra en algún lugar del medio y distribuye uniformemente la responsabilidad entre el proveedor de nube y el consumidor.

SaaS sitúa la mayor parte de la responsabilidad en el proveedor de servicios en la nube.



El modelo de servicio determinará la responsabilidad de cosas como lo siguiente:

* Sistemas operativos
* Controles de red
* APLICACIONES
* Identidad e infraestructura

**Definición de modelos en la nube**

Los tres principales modelos en la nube son: privados, públicos e híbridos.

**Nube privada**

Es una nube (que brinda servicios de TI a través de Internet) que utiliza una sola entidad

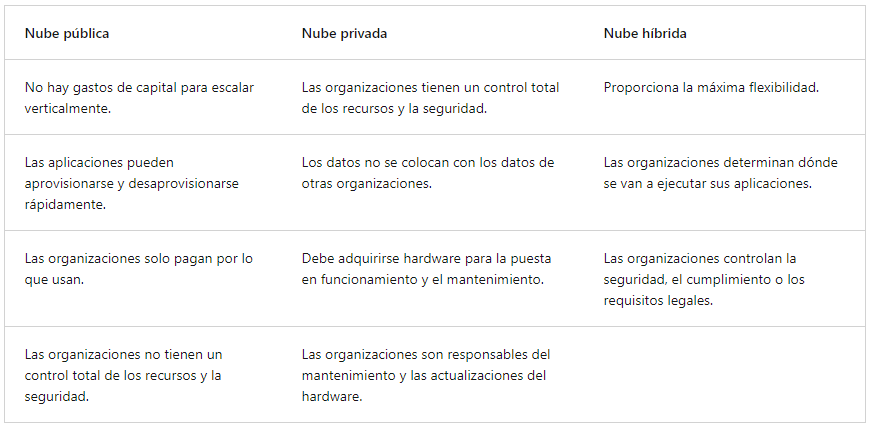
**Nube pública**

Un proveedor de nube de terceros crea, controla y mantiene una nube pública.

**Nube híbrida**

Una nube híbrida es un entorno informático que usa nubes públicas y privadas en un entorno interconectado.

En la tabla siguiente se resaltan algunos aspectos comparativos clave entre los modelos de nube.



**Nubes múltiples**

En un escenario de varias nubes, se usan varios proveedores de nube pública.

**Azure Arc**

Azure Arc es un conjunto de tecnologías que ayudan a administrar el entorno en la nube.

**Azure VMware Solution**

Azure VMware Solution le permite ejecutar las cargas de trabajo de VMware en Azure con una integración y escalabilidad perfectas.

**Descripción del modelo basado en el consumo**

Hay dos tipos de gastos que se deben tener en cuenta.

* Gastos de capital
* Gastos operativos

**La informática en la nube** se encuentra en la partida de gastos operativos porque funciona en un modelo basado en el consumo.

Este modelo basado en el consumo aporta muchas ventajas, por ejemplo:

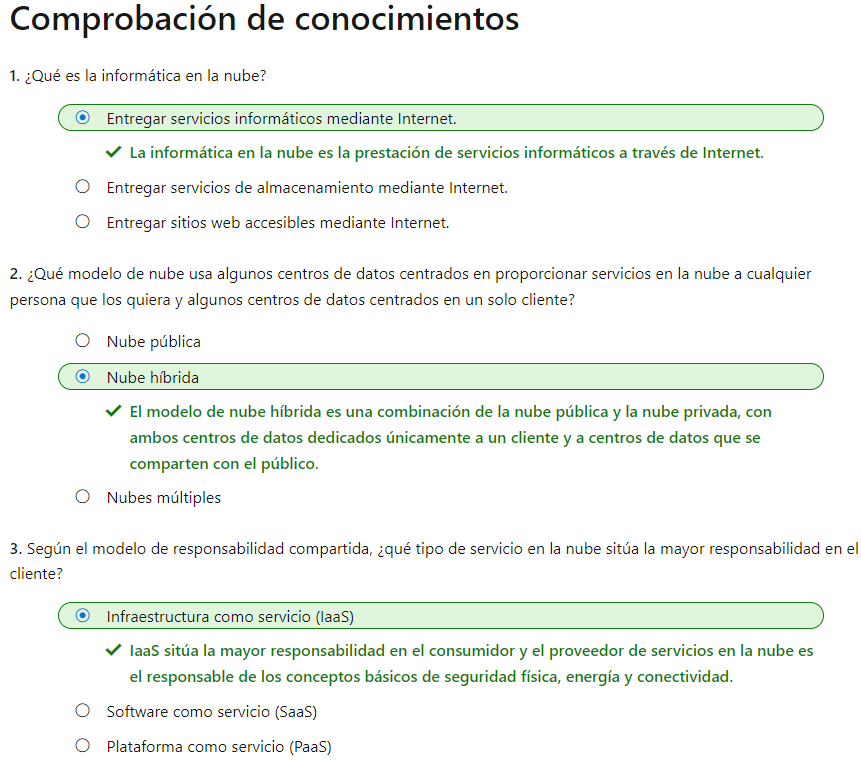
* Sin costes por adelantado.
* No es necesario comprar ni administrar infraestructuras costosas que es posible que los usuarios no aprovechen todo su potencial.
* Se puede pagar para obtener más recursos cuando se necesiten.
* Se puede dejar de pagar por los recursos que ya no se necesiten.

**Comparación de los modelos de precios en la nube**

Normalmente solo se paga por los servicios en la nube que se usan, lo que permite:

* Planifique y administre los costos operativos.
* Ejecutar la infraestructura de forma más eficaz.
* Escalar a medida que cambien las necesidades empresariales.

La informática en la nube es una forma de alquilar potencia de proceso y almacenamiento de un centro de datos de terceros.



**Descripción de las ventajas de usar servicios en la nube (ALTA DISPONIBILIDAD, ESCALABILIDAD)**

Consideraciones más importantes al compilar o implementar una app en la nube.

* tiempo de actividad (o la disponibilidad)
* la capacidad de controlar la demanda (o escala).

**Alta disponibilidad**

La alta disponibilidad se centra en garantizar la máxima disponibilidad, independientemente de las interrupciones o eventos que puedan producirse.

**AZURE** es un entorno de nube de alta disponibilidad con garantías de tiempo de actividad en función del servicio.

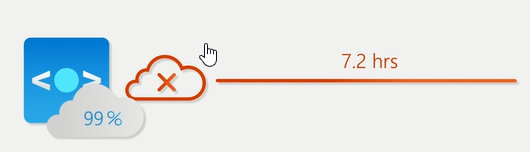
**AZURE SERVICE LEVEL AGREEMENTS (SLAs) 🡪** (acuerdo formal entre un proveedor de servicios y un cliente, el cual garantiza un nivel de servicio establecido)

Los SLAs también se utilizan dentro de las organizaciones, en un acuerdo entre el Depto. TI, y los usuarios comerciales.

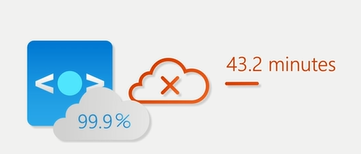
Los SLAs de AZURE se representan como porcentaje, relacionado con la disponibilidad del servicio o la app.

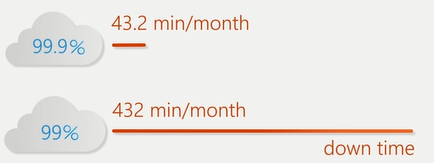
Disponibilidad 🡪 tiempo de actividad

Un SLAs disponible en 99% puede no estar disponible hasta unas 1,6 horas a la semana o 7,2 horas al mes.



Un SLAs disponible en 99.9% puede no estar disponible hasta unos 10 minutos a la semana o 43,2 minutos al mes.





Los servicios de alta disponibilidad tienen un costo adicional



**Escalabilidad**

La escalabilidad hace referencia a la capacidad de ajustar los recursos para satisfacer la demanda.

La otra ventaja de la escalabilidad es que no está pagando de más por los servicios.

El escalado suele tener dos variedades: **vertical y horizontal**.

El escalado **vertical** se centra en aumentar o disminuir las capacidades de los recursos.

El escalado **horizontal** agrega o resta el número de recursos.

**Descripción de las ventajas de la confiabilidad y la previsibilidad en la nube**

**Confiabilidad**

La confiabilidad es la capacidad de un sistema de recuperarse de los errores y seguir funcionando. También es uno de los pilares del Marco de arquitectura de Microsoft Azure.

**Predicción**

La previsibilidad se puede centrar en el **rendimiento o los costos,** están muy influidas por el Marco de arquitectura de Microsoft Azure

**Rendimiento**

La previsibilidad del rendimiento se centra en predecir los recursos necesarios para ofrecer una experiencia positiva para los clientes.

Conceptos de nube que admiten la previsibilidad del rendimiento:

* El escalado automático
* el equilibrio de carga
* la alta disponibilidad

**Coste**

La predicción de costos se centra en pronosticar el costo del gasto en la nube.

En la nube puede realizar seguimiento, supervisión del uso y manejo de los recursos y realizar la aplicación del análisis de datos.

Permite el uso de herramientas para el cálculo de los costos.

* calculadoras de costo total de propiedad (TCO)
* calculadoras de precios para obtener una estimación del posible gasto en la nube.

**Descripción de las ventajas de la seguridad y la gobernanza en la nube**

Las características en la nube admiten el cumplimiento y la gobernanza.

Las plantillas de conjunto ayudan a garantizar que todos los recursos implementados cumplan los estándares corporativos y los requisitos normativos de gobierno.

La auditoría basada en la nube ayuda a marcar cualquier recurso que no cumpla los estándares corporativos y proporciona estrategias de mitigación.

**Descripción de las ventajas de la capacidad de administración en la nube**

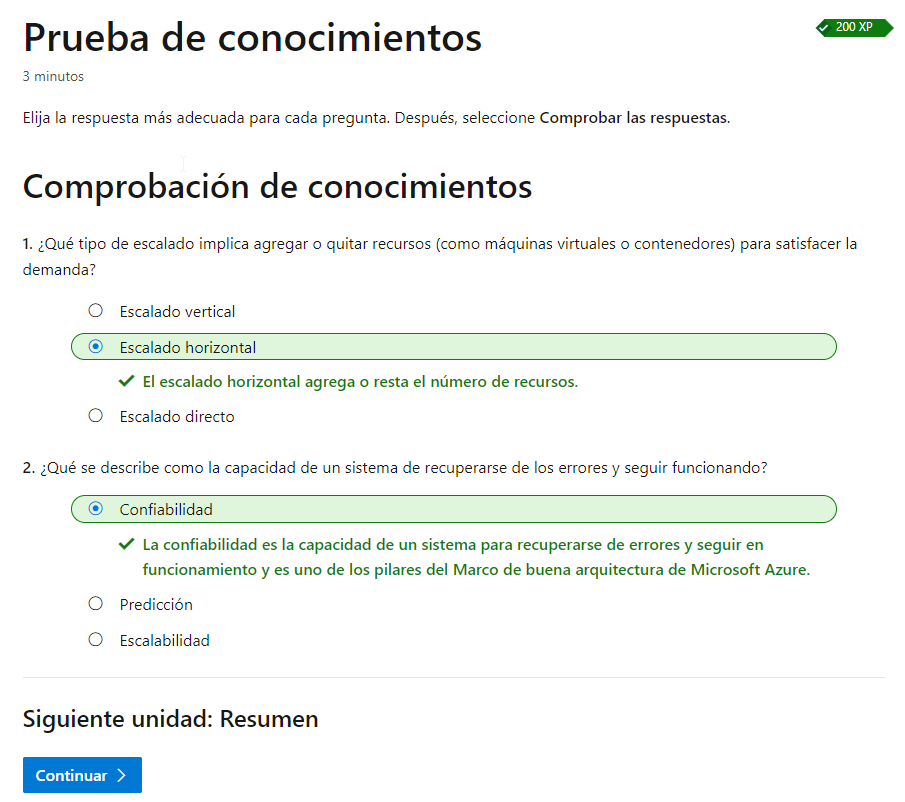
Hay dos tipos de administración para la informática en la nube.

**Administración de la nube:** trata sobre administrar los recursos.

* Escalar automáticamente la implementación de recursos en función de las necesidades.
* Implementar recursos basados en una plantilla pre configurado, lo que elimina la necesidad de realizar la configuración manual.
* Supervisar el estado de los recursos y reemplazar automáticamente los recursos con errores.
* Recibir alertas automáticas basadas en métricas configuradas, de modo que esté informado del rendimiento en tiempo real.

**Administración en la nube:** trata sobre cómo puede administrar el entorno y los recursos.

* Mediante un portal web.
* Con una interfaz de línea de comandos básica.
* Mediante las API.
* Mediante PowerShell.



**Descripción de los tipos de servicio en la nube.**

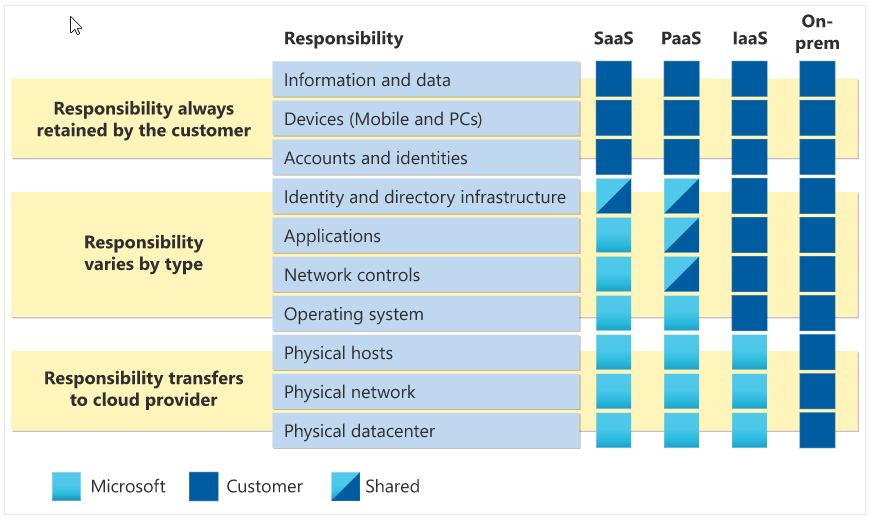
**Descripción de la infraestructura como servicio**

Es la categoría más flexible de servicios en la nube, ya que proporciona el máximo control para los recursos en la nube.

Con **IaaS**, lo que hace básicamente es alquilar el hardware en un centro de datos en la nube, pero será cosa suya lo que hace con ese hardware.

**Modelo de responsabilidad compartida**

IaaS sitúa la mayor parte de responsabilidad en usted. El proveedor de nube es el responsable de mantener la infraestructura física y su acceso a Internet.



Algunos escenarios comunes en los que IaaS puede tener sentido incluyen los siguientes:

* Migración mediante lift-and-shift
* Pruebas y desarrollo

**Descripción de la plataforma como servicio**

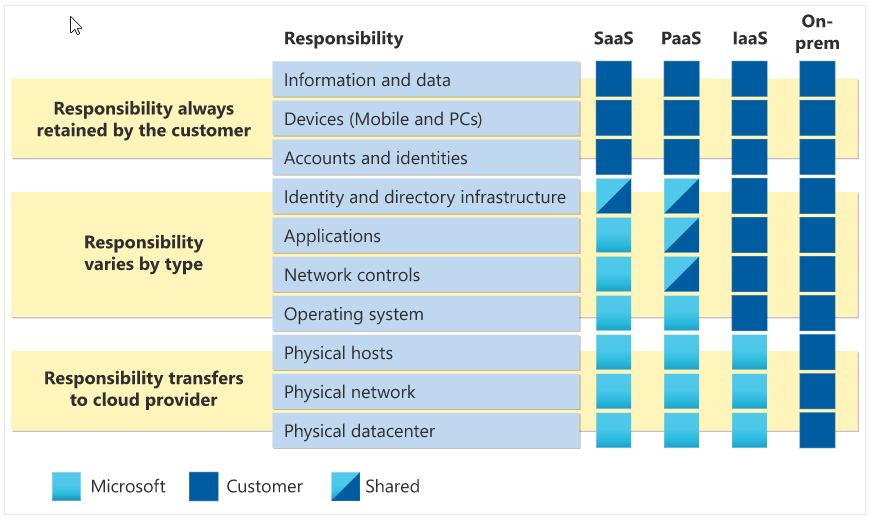
La plataforma como servicio (**PaaS**) es un punto intermedio entre alquilar espacio en un centro de datos (infraestructura como servicio) y pagar por una solución completa e implementada (software como servicio).

**PaaS** es adecuado para proporcionar un entorno de desarrollo completo sin el problema que supone mantener toda la infraestructura de desarrollo.

**Modelo de responsabilidad compartida**

PaaS divide la responsabilidad entre usted y el proveedor de nube,  el proveedor de nube también mantendrá los sistemas operativos, las bases de datos y las herramientas de desarrollo.

En función de la configuración, usted o el proveedor de nube pueden ser responsables de la configuración de red y la conectividad dentro del entorno de nube, la seguridad de red y la aplicación y la infraestructura de directorios.



Algunos escenarios comunes en los que PaaS pueden encajar incluyen:

* Marco de desarrollo
* Análisis o inteligencia empresarial

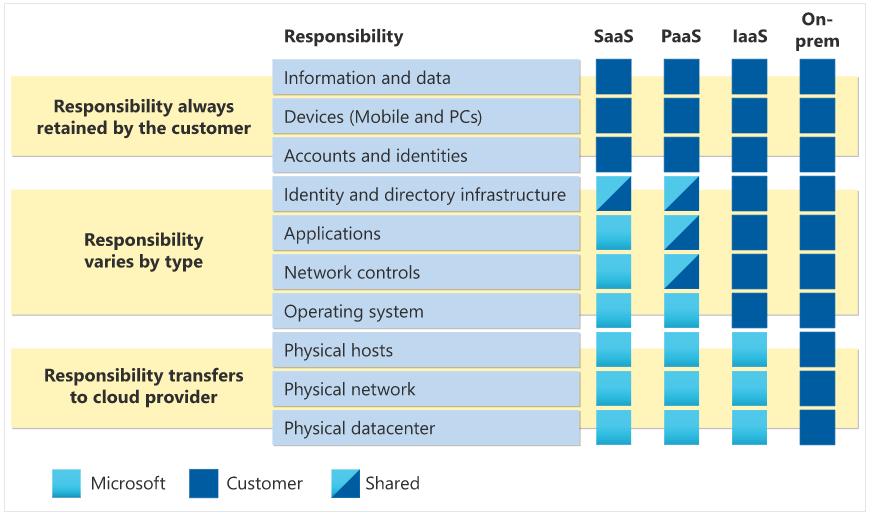
**Descripción del software como servicio**

Básicamente lo que hace es alquilar o usar una aplicación totalmente desarrollada.

Aunque el modelo de SaaS puede ser el menos flexible, también es el más sencillo de poner en marcha. Requiere la menor cantidad de conocimientos técnicos o experiencia para utilizarlo en toda su dimensión.

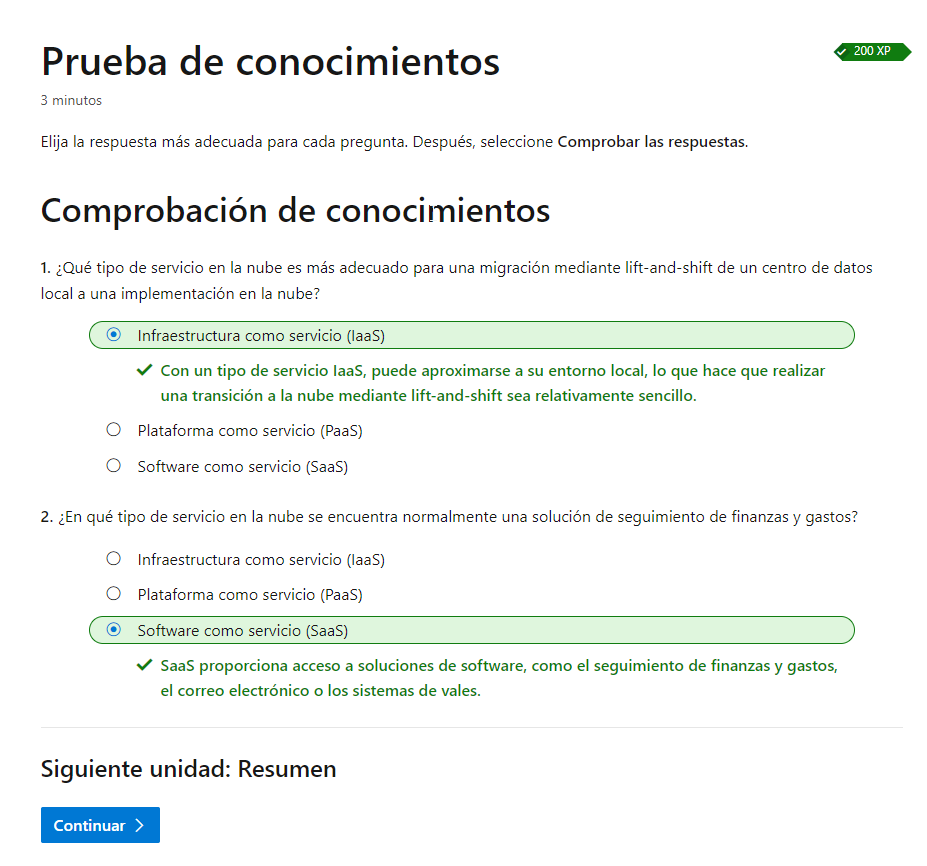
**Modelo de responsabilidad compartida**

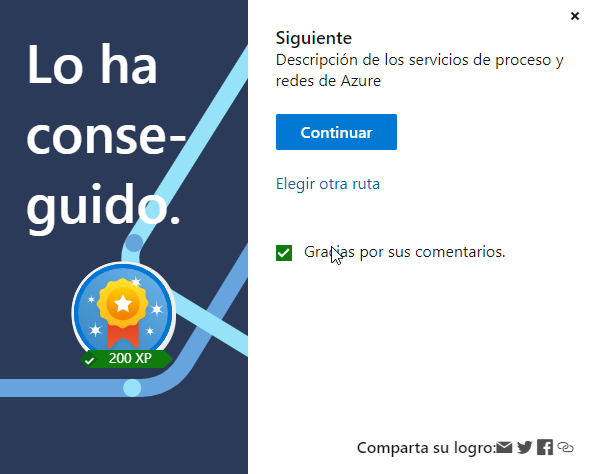
En un entorno de SaaS, serán responsabilidad suya los datos que ha puesto en el sistema, los dispositivos que le permiten conectarse al sistema y los usuarios que tienen acceso.



Algunos escenarios comunes para SaaS son los siguientes:

* Correo electrónico y mensajería
* Aplicaciones de productividad empresarial
* Seguimiento de finanzas y gastos





**Qué es Microsoft Azure**

Azure es una plataforma informática en la nube que ofrece un conjunto de servicios.

Admite los tipos de servicios IaaS, PaaS, SaaS. Los servicios que ofrece son de pago, siendo si, que solo paga por el tiempo de computación que usa.

**Tipos de plataforma**

**Azure App Servicies:**  permite implementar, operar y escalar las aplicaciones con facilidad en un entorno administrado.

**Azure Functions:**  puede crear aplicaciones sin servidor controladas por eventos sin necesidad de crear código.

**Azure Container Instances y Azure Kubernetes services:** Permite implementar aplicaciones contenedorizadas con servicios totalmente administrados.

Además, ofrece diversas bases de datos en memorias y relacionales totalmente administradas, con motores propietarios y de código abierto. También servicios de IA, y ML.

Los centros de datos regionales Azure permiten distribuir aplicaciones globalmente, de modo que pueda ubicar los datos y apps desde donde sea.

El portal Azure permite crear, configurar y controlar todos los servicios y recursos desde una interfaz web.

**¿Qué ofrece Azure?**

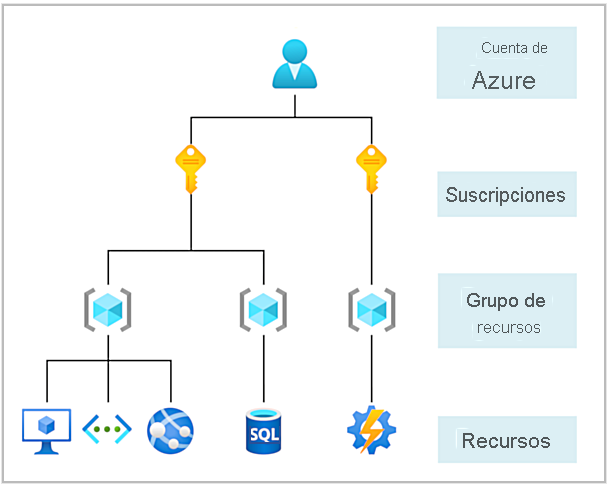
* Prepararse para el futuro
* Crear según términos propios
* Funcionamiento sin problemas en el entorno híbrido
* Confianza en la nube

**¿Qué puedo hacer con Azure?**

* ejecutar las aplicaciones existentes en máquinas virtuales
* explorar nuevos paradigmas de software
* migración de sus aplicaciones existentes

**Introducción a las cuentas de Azure**

Para crear y usar los servicios de Azure, necesita una suscripción de Azure.



**Tipos de cuentas para acceso a la plataforma AZURE**

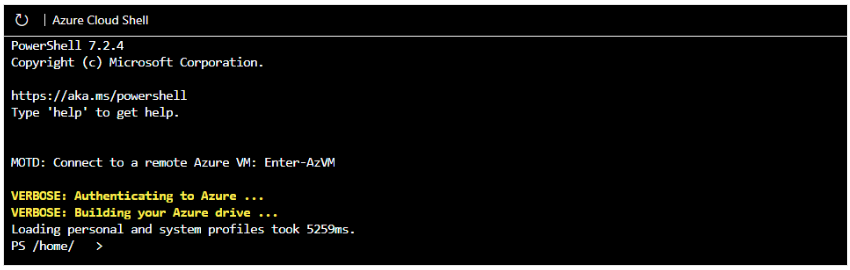
* Cuenta gratuita AZURE
* Cuenta estudiante de Azure

**¿Qué es el espacio aislado de Microsoft Learn?**

En muchos de los ejercicios de Learn se usa una tecnología denominada espacio aislado, que crea una suscripción temporal que se agrega a la cuenta de Azure. Esta suscripción temporal le permite crear recursos de Azure para la duración de un módulo de Learn. Learn limpia de forma automática los recursos temporales una vez que haya completado el módulo

El espacio aislado es el método preferido, ya que permite crear y probar recursos de Azure sin costo alguno.

**Ejercicio: Exploración del espacio aislado de Learn**



Comandos:

az versión

bash -> me cambia a comando de CLI por bash

az interactive-> activa el modo interactivo de azure en CLI Bash

exit 🡪 me permite salir del modo az interactive

**Descripción de la infraestructura física de Azure**

Los componentes arquitectónicos principales de Azure se pueden dividir en dos grandes grupos: la infraestructura física y la infraestructura de administración.

**Infraestructura física**

La infraestructura física de Azure comienza con los centros de datos. Son instalaciones con recursos organizados en bastidores, con potencia dedicada, refrigeración e infraestructura de red.

Azure tiene centros de datos en todo el mundo. Los centros de datos se agrupan en regiones de Azure o Azure Availability Zones

**Regions**

Una región es un área geográfica del planeta que contiene al menos un centro de datos.

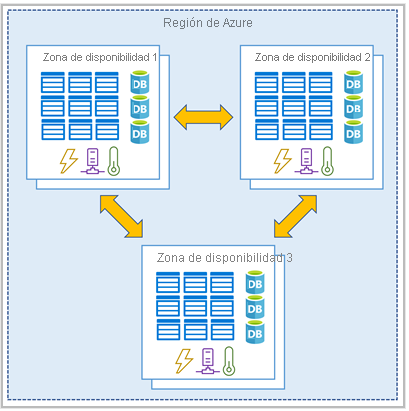
Al implementar un recurso en Azure, es habitual tener que elegir la región en la que quiere que se implemente el recurso.

Algunos servicios o características de las máquinas virtuales (VM) solo están disponibles en determinadas regiones. También hay algunos servicios globales de Azure que no requieren que seleccione una región concreta, como Azure Active Directory, Azure Traffic Manager o Azure DNS.

**Availability Zones**

Las zonas de disponibilidad son centros de datos separados físicamente dentro de una región de Azure.

Una zona de disponibilidad se configura para constituir un límite de aislamiento. Si una zona deja de funcionar, la otra continúa trabajando



Importante

Para garantizar la resistencia, se configuran un mínimo de tres zonas de disponibilidad independientes en todas las regiones habilitadas. Pero no todas las regiones de Azure admiten actualmente las zonas de disponibilidad.

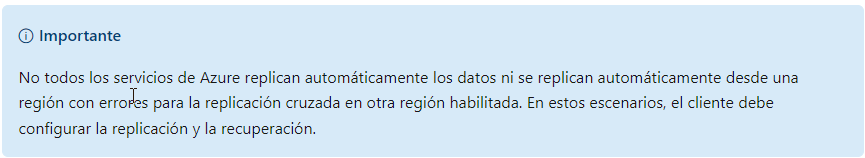
**Uso de las zonas de disponibilidad en sus aplicaciones**

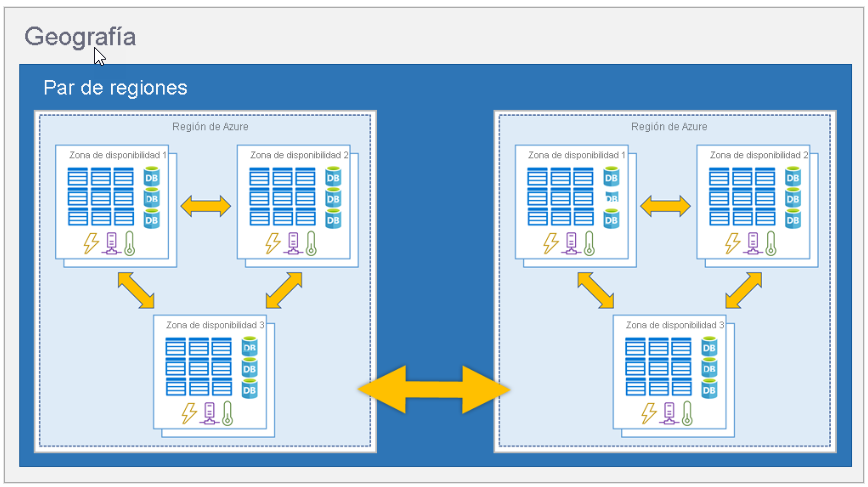
Los servicios de Azure que admiten zonas de disponibilidad se dividen en tres categorías:

* Servicios de zona: ancle el recurso a una zona específica (por ejemplo, máquinas virtuales, discos administrados, direcciones IP).
* Servicios de redundancia de zona: la plataforma se replica automáticamente entre zonas (por ejemplo, almacenamiento con redundancia de zona, SQL Database).
* Servicios no regionales: los servicios siempre están disponibles en las ubicaciones geográficas de Azure y son resistentes a las interrupciones de toda la zona, así como a las de toda la región.

**Pares de región**

La mayoría de las regiones de Azure se emparejan con otra región de la misma zona geográfica (por ejemplo, EE. UU., Europa o Asia) que se encuentre como mínimo a 500 km de distancia.





**Ventajas adicionales de los pares de región:**

* Si se produce una gran interrupción de Azure, se da prioridad a una región de cada par para asegurarse de que al menos una se restaure lo más rápido posible para las aplicaciones hospedadas en ese par de regiones.
* Las actualizaciones planeadas de Azure se implementan una a una en regiones emparejadas para minimizar el tiempo de inactividad y el riesgo de interrupción de la aplicación.
* Los datos siguen residiendo en la misma zona geográfica que su pareja (excepto Sur de Brasil) con fines de jurisdicción fiscal y de aplicación de la ley.

**Regiones soberanas**

Las regiones soberanas son instancias de Azure que están aisladas de la instancia principal de Azure.

Entre las regiones soberanas de Azure se incluyen las siguientes:

* US DoD (centro), US Gov Virginia, US Gov Iowa y más
* Este de China, Norte de China y más

**Descripción de la infraestructura de administración de Azure**

La infraestructura de administración incluye recursos de Azure y grupos de recursos, suscripciones y cuentas.

**Recursos y grupos de recursos de Azure**

Un recurso es el bloque de creación básico de Azure. Todo lo que cree, aprovisione, implemente, etc., es un recurso. Máquinas virtuales (VM), redes virtuales, bases de datos, servicios cognitivos, etc., se consideran recursos dentro de Azure.

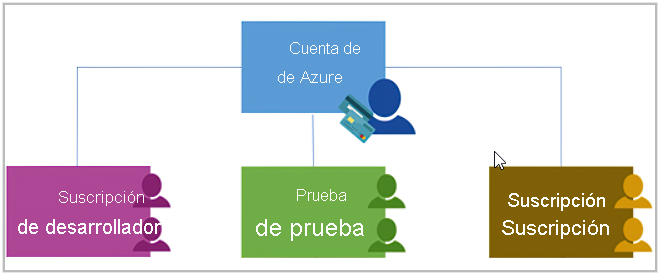


Los grupos de recursos son simplemente agrupaciones de recursos, un único recurso solo puede estar en un grupo de recursos a la vez, los grupos de recursos no se pueden anidar.

No hay reglas rígidas sobre cómo se usan los grupos de recursos, por lo que debe tener en cuenta cómo configurarlos para maximizar su utilidad.

**Suscripciones de Azure**

Las suscripciones son una unidad de administración, facturación y escala, las suscripciones permiten organizar lógicamente los grupos de recursos y facilitar la facturación.



Una cuenta puede tener varias suscripciones, pero solo es obligatorio tener una.

Hay dos tipos de límites de suscripción que puede utilizar:

* **Límite de facturación**: Este tipo de suscripción determina cómo se factura una cuenta de Azure por el uso de Azure. Puede crear varias suscripciones para diferentes tipos de requisitos de facturación. Azure genera facturas e informes de facturación independientes para cada suscripción, de modo que pueda organizar y administrar los costos.
* **Límite de control de acceso**: Azure aplica las directivas de administración de acceso en el nivel de suscripción, por lo que puede crear suscripciones independientes para reflejar distintas estructuras organizativas. Por ejemplo, dentro de una empresa hay diferentes departamentos a los que se pueden aplicar directivas de suscripción de Azure distintas. Este modelo de facturación le permite administrar y controlar el acceso a los recursos que los usuarios aprovisionan con suscripciones específicas.

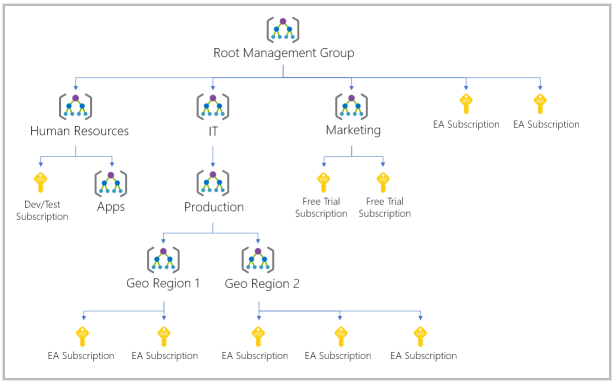
**Creación de una suscripción de Azure adicional**

* **Entornos**: puede optar por crear suscripciones con el fin de configurar entornos independientes para el desarrollo y las pruebas, para seguridad o para aislar los datos por motivos de cumplimiento. Este diseño es especialmente útil porque el control de acceso a los recursos se produce en el nivel de suscripción.
* **Estructuras organizativas**: puede crear suscripciones para reflejar las distintas estructuras organizativas. Por ejemplo, podría limitar un equipo a recursos de bajo costo, al tiempo que permite que el departamento de TI tenga un alcance completo. Este diseño permite administrar y controlar el acceso a los recursos que los usuarios aprovisionan en cada suscripción.
* **Facturación**: puede crear suscripciones adicionales con fines de facturación. Dado que los costos se agregan primero en el nivel de suscripción, es posible que quiera crear suscripciones para administrar y realizar un seguimiento de los costos en función de sus necesidades. Por ejemplo, puede que quiera crear una suscripción para las cargas de trabajo de producción, y otra suscripción para las cargas de trabajo de desarrollo y pruebas.

**Grupos de administración de Azure**

Los grupos de administración de Azure proporcionan un nivel de ámbito por encima de las suscripciones. Las suscripciones se organizan en contenedores llamados grupos de administración, a los que se aplican condiciones de gobernanza.

Los grupos de administración proporcionan capacidad de administración de nivel empresarial a gran escala con independencia del tipo de suscripciones que tenga. Los grupos de administración se pueden anidar.

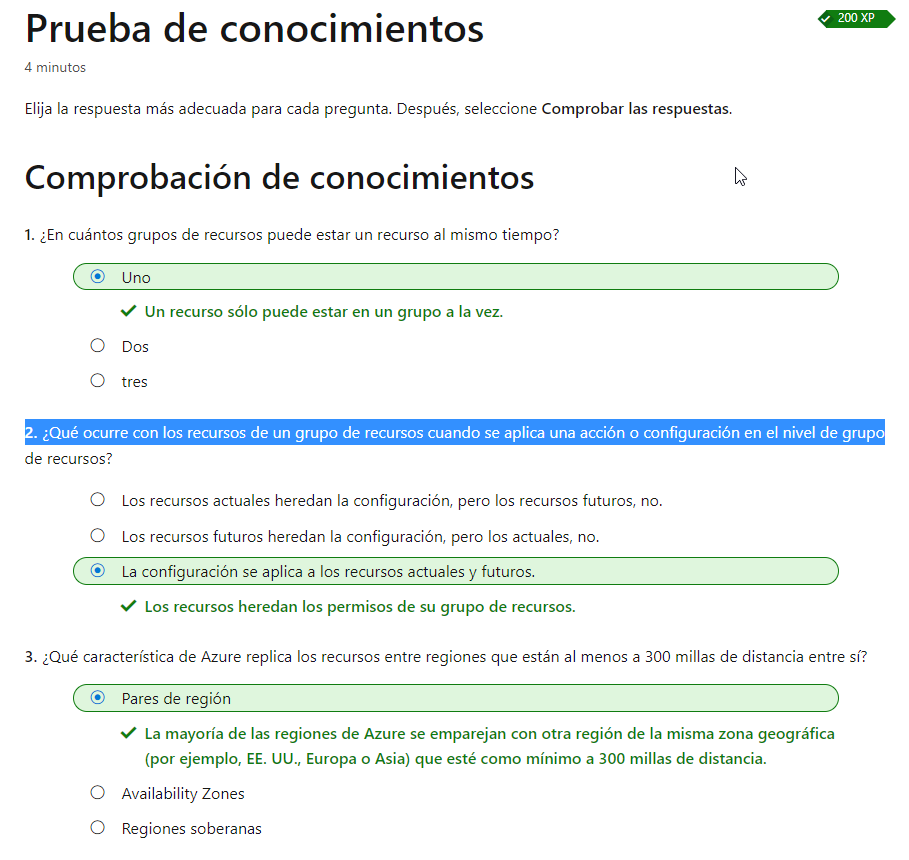


Algunos ejemplos de cómo podría usar los grupos de administración podrían ser los siguientes:

* **Crear una jerarquía que aplique una directiva**. Podría limitar las ubicaciones de las máquinas virtuales a la región Oeste de EE. UU. en un grupo denominado Producción. Esta directiva se heredará en todas las suscripciones descendientes de ese grupo de administración y se aplicará a todas las máquinas virtuales de esas suscripciones. El propietario de los recursos o las suscripciones no puede modificar esta directiva de seguridad, lo que permite una gobernanza mejorada.
* **Proporcionar acceso de usuario a varias suscripciones**. Al mover varias suscripciones bajo un grupo de administración, puede crear una asignación del control de acceso basado en roles (RBAC) en el grupo de administración. La asignación de RBAC de Azure en el nivel de grupo de administración significa que todos los grupos de administración secundaria, las suscripciones, los grupos de recursos y los recursos bajo ese grupo de administración también heredarían esos permisos. Una asignación en el grupo de administración puede permitir a los usuarios tener acceso a todo lo que necesitan, en lugar de crear scripts de Azure RBAC sobre las distintas

Datos importantes sobre los grupos 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. Este límite no incluye el nivel raíz ni el nivel de suscripción.
* Cada grupo de administración y suscripción solo puede admitir un elemento primario.



**Descripción de Azure Virtual Machines**

Con Azure Virtual Machines (VM), puede crear y usar máquinas virtuales en la nube.

Las máquinas virtuales son una opción ideal cuando se necesita lo siguiente:

* Control total sobre el sistema operativo (SO).
* Capacidad de ejecutar software personalizado.
* Usar configuraciones de hospedaje personalizadas.

Una máquina virtual de Azure le ofrece la flexibilidad de la virtualización sin necesidad de adquirir y mantener el hardware físico que ejecuta la máquina virtual.

Incluso puede crear o usar una imagen ya creada para aprovisionar rápidamente máquinas virtuales.

Una imagen es una plantilla que se usa para crear una máquina virtual y puede que ya incluya un sistema operativo y otro software.

**Escalado de máquinas virtuales en Azure**

Azure también puede administrar la agrupación de máquinas virtuales con características como conjuntos de escalado y conjuntos de disponibilidad.

**Conjuntos de escalado de máquinas virtuales**

Los conjuntos de escalado de máquinas virtuales permiten crear y administrar un grupo de máquinas virtuales idénticas, de carga equilibrada.

Los conjuntos de escalado le permiten administrar, configurar y actualizar de forma centralizada un gran número de máquinas virtuales en cuestión de minutos.

Los conjuntos de escalado de máquinas virtuales también implementan automáticamente un equilibrador de carga para asegurarse de que los recursos se usan de forma eficaz. Con los conjuntos de escalado de máquinas virtuales, puede crear servicios a gran escala para áreas como proceso, macro datos y cargas de trabajo de contenedor.

**Conjuntos de disponibilidad de máquinas virtuales**

Los conjuntos de disponibilidad están diseñados para garantizar que las máquinas virtuales escalen las actualizaciones y tengan una conectividad de red y potencia variadas, lo que evita que se pierdan todas las máquinas virtuales debido a un solo fallo de energía o de la red.

Los conjuntos de disponibilidad lo hacen mediante la agrupación de las máquinas virtuales de dos maneras: dominio de actualización y dominio de error.

* **Dominio de actualización**: agrupa las máquinas virtuales que se pueden reiniciar al mismo tiempo. Esto le permite aplicar actualizaciones mientras sabe que solo una agrupación de dominios de actualización estará sin conexión a la vez. Se actualizarán todas las máquinas de un dominio de actualización. A un grupo de actualizaciones que realiza el proceso de actualización se le asigna un tiempo de 30 minutos de recuperación antes de que se inicie el mantenimiento en el siguiente dominio de actualización.
* **Dominio de error**: agrupa las máquinas virtuales por fuente de alimentación común y conmutador de red. De forma predeterminada, un conjunto de disponibilidad dividirá las máquinas virtuales en un máximo de tres dominios de error. Esto ayuda a protegerse frente a un error de alimentación física o de la red al tener las máquinas virtuales en dominios de error diferentes (por tanto, conectadas a diferentes recursos de alimentación y red).

Lo mejor de todo es que la configuración de un conjunto de disponibilidad no supone ningún costo adicional. Solo paga por las instancias de máquina virtual que cree.

**Ejemplos de cuándo usar máquinas virtuales**

* Durante las pruebas y el desarrollo.
* Al ejecutar aplicaciones en la nube.
* Al ampliar el centro de datos a la nube.
* Durante la recuperación ante desastres.

**Traslado a la nube con máquinas virtuales**

Las máquinas virtuales también son una opción excelente cuando se mueve de un servidor físico a la nube (también conocido como Lift-and-shift).

**Recursos de máquina virtual**

* amaño (propósito, número de núcleos de procesador y cantidad de RAM)
* Discos de almacenamiento (unidades de disco duro, unidades de estado sólido, etc.)
* Redes (red virtual, dirección IP pública y configuración de puertos)

**Ejercicio: Creación de una máquina virtual de Azure**

**Tarea 1: Creación de una máquina virtual Linux e instalación de Nginx**

Desde Cloud Shell, ejecute el siguiente comando az vm create para crear una máquina virtual Linux:

az vm extension set \

--resource-group learn-306a5ced-4c39-48b0-9242-f9e22e8f35f5 \

--vm-name my-vm \

--name customScript \

--publisher Microsoft.Azure.Extensions \

--version 2.1 \

--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \

--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

Ejecute el siguiente comando az vm extension set para configurar Nginx en la máquina virtual:

az vm extension set \

--resource-group learn-306a5ced-4c39-48b0-9242-f9e22e8f35f5 \

--vm-name my-vm \

--name customScript \

--publisher Microsoft.Azure.Extensions \

--version 2.1 \

--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \

--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

Este comando usa la extensión de script personalizado para ejecutar un script de Bash en la máquina virtual. El script se almacena en GitHub. Mientras se ejecuta el comando, puede optar por [examinar el script de Bash](https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh) en una pestaña independiente del explorador. Para resumir, el script:

1. Ejecuta apt-get update para descargar la información más reciente del paquete desde Internet. Este paso ayuda a garantizar que el siguiente comando pueda encontrar la versión más reciente del paquete Nginx.
2. Instala Nginx.
3. Establece la página principal, */var/www/html/index.html*, para que imprima un mensaje de bienvenida en el que se incluye el nombre de host de la máquina virtual.

**Descripción de Azure Virtual Desktop**

Azure Virtual Desktop es un servicio de virtualización de escritorios y aplicaciones que se ejecuta en la nube. Le permite usar una versión hospedada en la nube de Windows desde cualquier ubicación. Azure Virtual Desktop funciona en dispositivos y sistemas operativos, y funciona con aplicaciones que puede usar para acceder a escritorios remotos o a la mayoría de exploradores modernos.

**Aumento de la seguridad**

Azure Virtual Desktop proporciona administración centralizada de la seguridad de los escritorios de los usuarios con Azure Active Directory (Azure AD).

Con Azure Virtual Desktop, los datos y las aplicaciones se separan del hardware local y El escritorio y las aplicaciones reales se ejecutan en la nube, lo que significa que se reduce el riesgo de dejar datos confidenciales en un dispositivo personal. Además, las sesiones de usuario están aisladas en entornos de una o varias sesiones.

**Implementación de sesión múltiple de Windows 10 o Windows 11**

Azure Virtual Desktop permite usar la sesión múltiple de Windows 10 o Windows 11 Enterprise, el único sistema operativo basado en cliente de Windows que permite varios usuarios simultáneos en una sola máquina virtual.

**Descripción de contenedores de Azure**

**¿Qué son los contenedores?**

Los contenedores son un entorno de virtualización. Al igual que la ejecución de varias máquinas virtuales en un solo host físico, se pueden ejecutar varios contenedores en un solo host físico o virtual. A diferencia de las máquinas virtuales, no se administra el sistema operativo de un contenedor.

**Comparación de máquinas virtuales con contenedores**

VM- el control lo tiene el administrador, decide el SO, paquetes y herramientas. Sin embargo en una VM solo se puede ejecutar un SO a la vez, por lo tanto si se cuenta varias apps que se ejecuten en otros SO será necesario instalar los mismos.

Containers: Son una solución más ligera agrupa una sola app y sus dependencias. El host de un contenedor proporciona un entorno estandarizado. Este omite los requisitos de INFRAESTRUCTURA y SO, lo que permite que un app en un contenedor se ejecute con otras apps en otros contenedores al mismo tiempo.

Diferencias.

VM 🡪 Virtualizan el hardware

Containers🡪 virtualizan el SO

**Azure Container Instances**

Azure Container Instances ofrece la forma más rápida y sencilla de ejecutar un contenedor en Azure sin tener que administrar máquinas virtuales o adoptar servicios adicionales.

**Uso de contenedores en las soluciones**

Los contenedores se usan normalmente para crear soluciones mediante una arquitectura de microservicios. Esta arquitectura es donde se dividen las soluciones en partes más pequeñas e independientes.

**Descripción de Azure Functions**

Azure Functions es una opción de proceso sin servidor controlada por eventos que no necesita el mantenimiento de máquinas virtuales ni contenedores.

Con Azure Functions, un evento activa la función, lo que reduce la necesidad de mantener los recursos aprovisionados cuando no hay ningún evento.

SERVERLESS COMPUTING

**Ventajas de Azure Functions**

El uso de Azure Functions es idóneo si solo le interesa el código que ejecuta el servicio y no la infraestructura o la plataforma subyacente.

Functions se escala automáticamente según la demanda, por lo que es una opción correcta cuando la demanda es variable.

Azure Functions ejecuta el código cuando se desencadena y desasigna recursos automáticamente cuando la función finaliza. En este modelo, solo se le cobrará por el tiempo de CPU usado mientras se ejecuta la función.

Las funciones pueden ser sin estado o con estado.

**Descripción de las opciones de hospedaje de aplicaciones**

**Azure App Service**

App Service permite crear y hospedar aplicaciones web, trabajos en segundo plano, back-ends móviles y API RESTful en el lenguaje de programación que prefiera, sin tener que administrar la infraestructura. Ofrece escalado automático y alta disponibilidad. App Service admite Windows y Linux. Permite implementaciones automatizadas desde GitHub, Azure DevOps o cualquier repositorio Git para admitir un modelo de implementación continua.

Azure App Service es un servicio basado en HTTP para hospedar aplicaciones web, API de REST y back-ends para dispositivos móviles. Admite varios lenguajes, incluidos .NET, .NET Core, Java, Ruby, Node.js, PHP o Python. También admite entornos de Windows y Linux.

**Tipos de servicios de aplicaciones**

Con App Service, puede hospedar la mayoría de los estilos de servicio de aplicación más comunes, como los siguientes:

* Aplicaciones web
* Aplicaciones de API
* Trabajos web
* Aplicaciones móviles

**Descripción de las redes virtuales de Azure**

Una red de Azure se puede considerar una extensión de la red local con recursos que vinculan otros recursos de Azure.

Las redes virtuales de Azure proporcionan las importantes funcionalidades de red siguientes:

* Aislamiento y segmentación
* Comunicación con Internet
* Comunicación entre recursos de Azure
* Comunicación con los recursos locales
* Enrutamiento del tráfico de red
* Filtrado del tráfico de red
* Conexión de redes virtuales

Las redes virtuales de Azure admiten puntos de conexión públicos y privados para permitir la comunicación entre recursos externos o internos con otros recursos internos.

* Los puntos de conexión públicos tienen una dirección IP pública y son accesibles desde cualquier parte del mundo.
* Los puntos de conexión privados existen dentro de una red virtual y tienen una dirección IP privada en el espacio de direcciones de esa red virtual.

**Aislamiento y segmentación**

Para la resolución de nombres, puede usar el servicio de resolución de nombres integrado en Azure. También puede configurar la red virtual para que use un servidor DNS interno o externo.

**Comunicación con Internet**

Puede permitir conexiones entrantes desde Internet mediante la asignación de una dirección IP pública a un recurso de Azure o la colocación del recurso detrás de un equilibrador de carga público.

**Comunicación entre los recursos de Azure**

Le interesará habilitar los recursos de Azure para que se comuniquen entre sí de forma segura. Puede hacerlo de dos maneras:

* Las redes virtuales no solo pueden conectar máquinas virtuales, sino también otros recursos de Azure, como App Service Environment para Power Apps, Azure Kubernetes Service y conjuntos de escalado de máquinas virtuales de Azure.
* Los puntos de conexión de servicio se pueden conectar a otros tipos de recursos de Azure, como cuentas de almacenamiento y bases de datos de Azure SQL. Este enfoque permite vincular varios recursos de Azure con las redes virtuales para mejorar la seguridad y proporcionar un enrutamiento óptimo entre los recursos.

**Comunicación con recursos locales**

Las redes virtuales de Azure permiten vincular entre sí los recursos del entorno local y dentro de la suscripción de Azure. De hecho, puede crear una red que abarque tanto el entorno local como el entorno en la nube. Existen tres mecanismos para lograr esta conectividad:

* Las conexiones de red privada virtual de punto a sitio se establecen desde un equipo ajeno a la organización a la red corporativa. En este caso, el equipo cliente inicia una conexión VPN cifrada para conectarse a la red virtual de Azure.
* Las redes virtuales privadas de sitio a sitio vinculan el dispositivo o puerta de enlace de VPN local con la puerta de enlace de VPN de Azure en una red virtual. De hecho, puede parecer que los dispositivos de Azure están en la red local. La conexión se cifra y funciona a través de Internet.
* Azure ExpressRoute proporciona una conectividad privada dedicada a Azure que no se desplaza por Internet. ExpressRoute es útil para los entornos donde se necesita más ancho de banda e incluso mayores niveles de seguridad.

**Enrutamiento del tráfico de red**

De forma predeterminada, Azure enruta el tráfico entre las subredes de todas las redes virtuales conectadas, las redes locales e Internet. También puede controlar el enrutamiento e invalidar esa configuración del siguiente modo:

* Las tablas de rutas permiten definir reglas sobre cómo se debe dirigir el tráfico. Puede crear tablas de rutas personalizadas que controlen cómo se enrutan los paquetes entre las subredes.
* El Protocolo de puerta de enlace de borde (BGP) funciona con puertas de enlace de VPN de Azure, Azure Route Server o Azure ExpressRoute para propagar las rutas BGP locales a las redes virtuales de Azure.

**Filtrado del tráfico de red**

Las redes virtuales de Azure permiten filtrar el tráfico entre las subredes mediante los métodos siguientes:

* Los grupos de seguridad de red son recursos de Azure que pueden contener varias reglas de seguridad de entrada y salida. Estas reglas se pueden definir para permitir o bloquear el tráfico en función de factores como el protocolo, el puerto y las direcciones IP de destino y origen.
* Las aplicaciones virtuales de red son máquinas virtuales especializadas que se pueden comparar con un dispositivo de red protegido. Una aplicación virtual de red ejerce una función de red determinada, como ejecutar un firewall o realizar la optimización de la red de área extensa (WAN).

**Conexión de redes virtuales**

Puede vincular redes virtuales entre sí mediante el emparejamiento de red virtual. El emparejamiento permite que dos redes virtuales se conecten directamente entre sí. El tráfico de red entre redes emparejadas es privado y se desplaza por la red troncal de Microsoft, y nunca entra en la red pública de *Internet*.

**Descripción de las redes privadas virtuales de Azure**

Una red privada virtual (VPN) usa un túnel cifrado en otra red.

Las VPN pueden permitir que las redes compartan información confidencial de forma segura.

**Puertas de enlace de VPN**

Una puerta de enlace de VPN es un tipo de puerta de enlace de red virtual. Las instancias de Azure VPN Gateway se implementan en una subred dedicada de la red virtual y permiten la conectividad siguiente:

* Conectar los centros de datos locales a redes virtuales a través de una conexión de sitio a sitio.
* Conectar los dispositivos individuales a redes virtuales a través de una conexión de punto a sitio.
* Conectar las redes virtuales a otras redes virtuales a través de una conexión entre redes.

Solo se puede implementar una única instancia de puerta de enlace de VPN en cada red virtual.

Si necesita alguno de los siguientes tipos de conectividad, use una instancia de VPN Gateway basada en rutas:

* Conexiones entre redes virtuales
* Conexiones de punto a sitio
* Conexiones de varios sitios
* Coexistencia con una puerta de enlace de Azure ExpressRoute

**Escenarios de alta disponibilidad**

Si va a configurar una VPN para mantener la información segura, también querrá asegurarse de que es una configuración de VPN de alta disponibilidad y tolerante a errores.

**Configuración de activo-en espera**

**Activo/activo**

**Conmutación por error de ExpressRoute**

**Puertas de enlace con redundancia de zona**

**Describir Azure ExpressRoute**

ExpressRoute le permite ampliar las redes locales a la nube de Microsoft mediante una conexión privada con la ayuda de un proveedor de conectividad. Esta conexión se denomina circuito ExpressRoute.

**Características y ventajas de ExpressRoute**

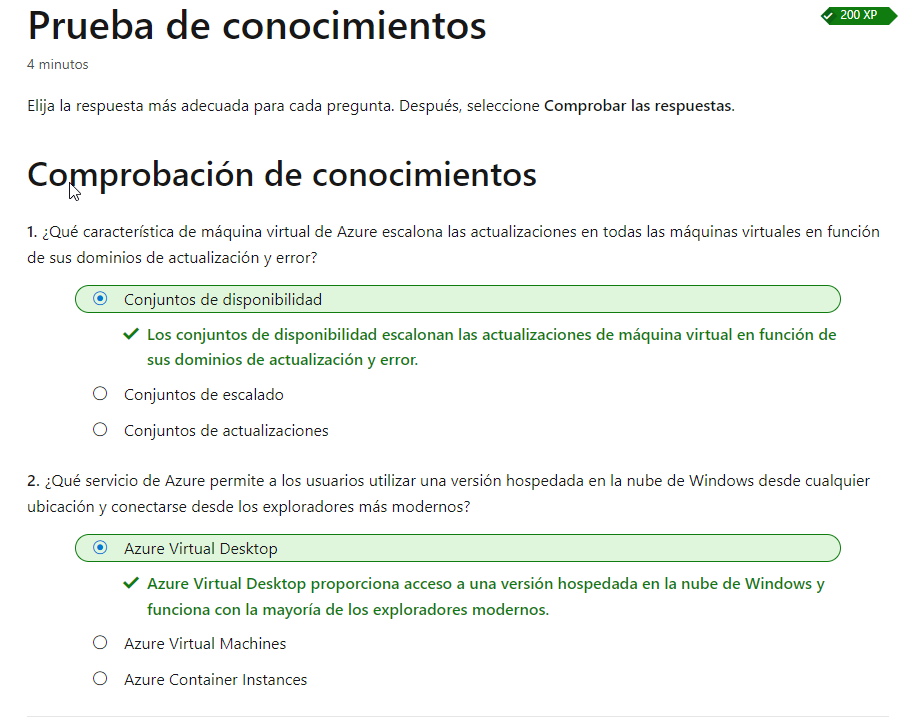
El uso de ExpressRoute como servicio de conexión entre Azure y las redes locales tiene varias ventajas.

* Conectividad de servicios en la nube de Microsoft en todas las regiones dentro de la región geopolítica.
* Conectividad global a los servicios de Microsoft en todas las regiones con Global Reach de ExpressRoute.
* Enrutamiento dinámico entre la red y Microsoft a través del Protocolo de puerta de enlace de borde (BGP).
* Redundancia integrada en todas las ubicaciones de configuración entre pares para una mayor confiabilidad.

**Conectividad con los Servicios en la nube de Microsoft**

ExpressRoute permite el acceso directo a los siguientes servicios en todas las regiones:

* Microsoft Office 365
* Microsoft Dynamics 365
* Servicios de proceso de Azure, como Azure Virtual Machines
* Servicios en la nube de Azure, como Azure Cosmos DB y Azure Storage



**Descripción de las cuentas de almacenamiento de Azure**

Una cuenta de almacenamiento proporciona un espacio de nombres único para los datos de Azure Storage al que se puede acceder desde cualquier lugar del mundo a través de HTTP o HTTPS. Los datos de esta cuenta son seguros, de alta disponibilidad, duraderos y escalables de forma masiva.

* Almacenamiento con redundancia local (LRS)
* Almacenamiento con redundancia geográfica (GRS)
* Almacenamiento con redundancia geográfica con acceso de lectura (RA-GRS).
* Almacenamiento con redundancia de zona (ZRS)
* Almacenamiento con redundancia de zona geográfica (GZRS)
* Almacenamiento con redundancia de zona geográfica con acceso de lectura (RA-GZRS)

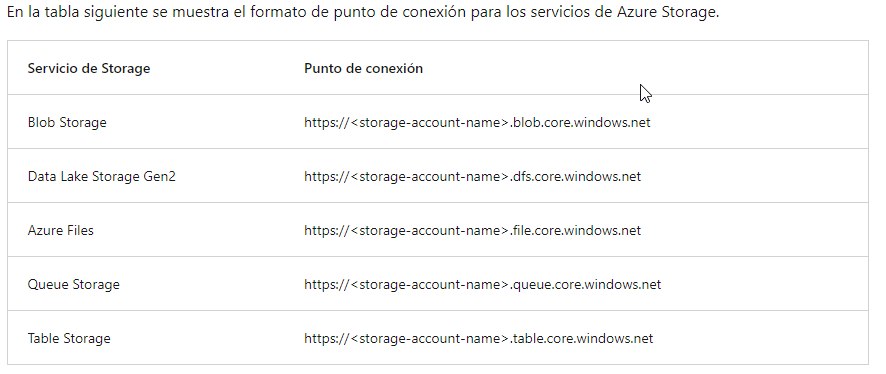


**Puntos de conexión de cuenta de almacenamiento**

Una de las ventajas de usar una cuenta de Azure Storage es tener un espacio de nombres único en Azure para los datos. Para ello, todas las cuentas de almacenamiento de Azure deben tener un nombre de cuenta único en Azure.

Cuando especifique un nombre para la cuenta de almacenamiento, tenga en cuenta estas reglas:

* Los nombres de las cuentas de almacenamiento deben tener entre 3 y 24 caracteres, y solo pueden incluir números y letras en minúscula.
* El nombre de la cuenta de almacenamiento debe ser único dentro de Azure. No puede haber dos cuentas de almacenamiento con el mismo nombre. Esto admite la capacidad de tener un espacio de nombres único y accesible en Azure.



**Descripción de la redundancia de almacenamiento de Azure**

Azure Storage siempre almacena varias copias de los datos, con el fin de protegerlos de eventos planeados y no planeados, lo que incluye errores transitorios del hardware, interrupciones del suministro eléctrico o cortes de la red, y desastres naturales.

A la hora de decidir qué opción de redundancia es la más adecuada para su escenario, intente buscar un equilibrio entre bajo costo y alta disponibilidad. Entre los factores que ayudan a determinar qué opción de redundancia debe elegir se incluye:

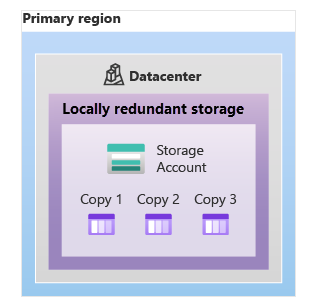
* Cómo se replican los datos en la región primaria.
* Si los datos se replican en una segunda ubicación que está alejada geográficamente de la región primaria, para protegerse frente a desastres regionales.
* Si la aplicación necesita acceso de lectura a los datos replicados en la región secundaria en caso de que la región primaria deje de estar disponible.

**Redundancia en la región primaria**

Los datos de una cuenta de Azure Storage siempre se replican tres veces en la región primaria. Azure Storage ofrece dos opciones para replicar los datos en la región primaria, el almacenamiento con redundancia local (LRS) y el almacenamiento con redundancia de zona (ZRS).

**Almacenamiento con redundancia local**

El almacenamiento con redundancia local (LRS) replica los datos tres veces dentro de un único centro de datos en la región primaria. LRS ofrece una durabilidad mínima de 11 nueves (99,999999999 %) de los objetos en un año determinado.

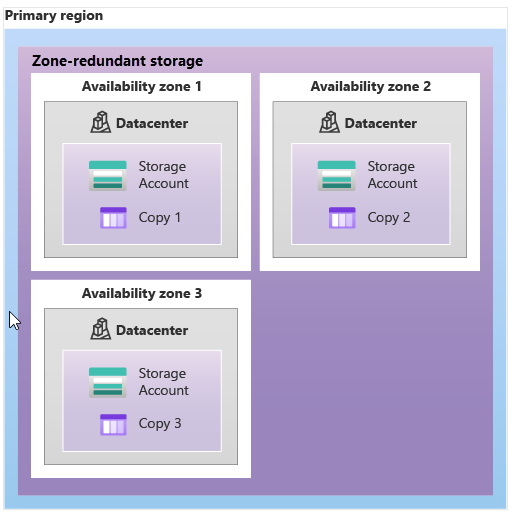


LRS es la opción de redundancia de costo más bajo y ofrece la menor durabilidad en comparación con otras opciones.

Microsoft recomienda el uso del almacenamiento con redundancia de zona (ZRS), el almacenamiento con redundancia geográfica (GRS) o el almacenamiento con redundancia de zona geográfica (GZRS).

**Almacenamiento con redundancia de zona**

Para las regiones con zona de disponibilidad habilitada, el almacenamiento con redundancia de zona (ZRS) replica los datos de Azure Storage sincrónicamente en tres zonas de disponibilidad de Azure en la región primaria.



**Redundancia en una región secundaria**

En el caso de las aplicaciones que requieren de alta durabilidad, puede optar por copiar los datos de la cuenta de almacenamiento en una región secundaria que esté a cientos de kilómetros de distancia de la región primaria.

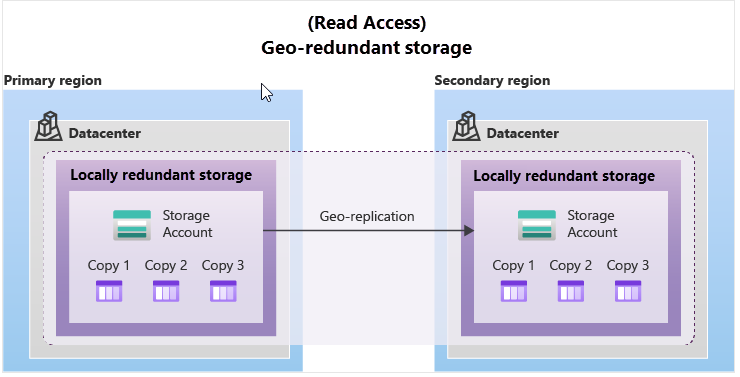
Al crear una cuenta de almacenamiento, seleccione la región principal de la cuenta. La región secundaria emparejada se determina en función de los Pares de regiones de Azure y no se puede cambiar.

Azure Storage ofrece dos opciones para copiar los datos en una región secundaria: almacenamiento con redundancia geográfica (GRS) y almacenamiento con redundancia de zona geográfica (GZRS).

El intervalo entre las escrituras más recientes en la región primaria y la última escritura en la región secundaria se conoce como objetivo de punto de recuperación (RPO)

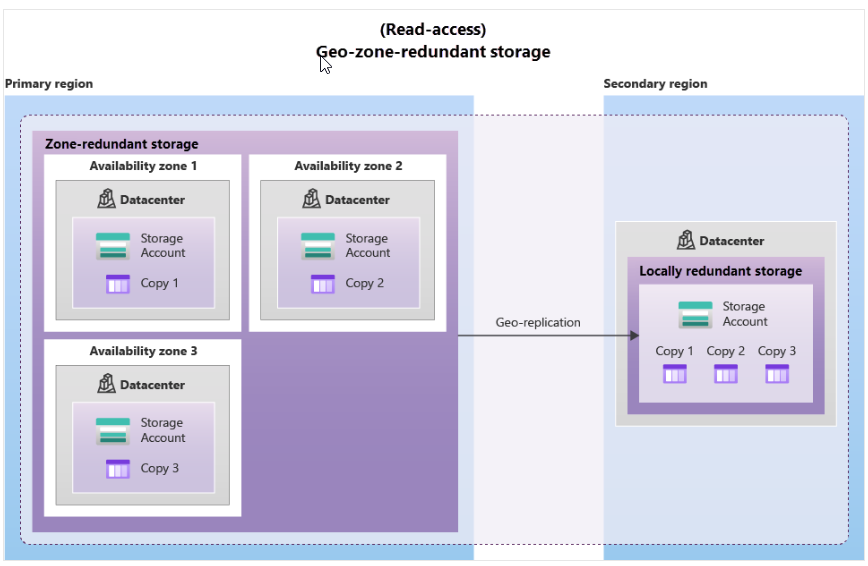
**Almacenamiento con redundancia geográfica**

GRS copia los datos de manera sincrónica tres veces dentro de una ubicación física única en la región primaria mediante LRS.



**Almacenamiento con redundancia de zona geográfica**

GZRS combina la alta disponibilidad que proporciona la redundancia entre zonas de disponibilidad con la protección frente a interrupciones regionales que proporciona la replicación geográfica. Los datos de una cuenta de almacenamiento de GZRS se almacenan en tres zonas de disponibilidad de Azure en la región primaria (de manera similar a ZRS) y también se replican en una región geográfica secundaria para protegerlos frente a desastres regionales.



**Acceso de lectura a los datos de la región secundaria**

El almacenamiento con redundancia geográfica (con GRS o GZRS) replica los datos en otra ubicación física de la región secundaria para protegerlos frente a los apagones regionales.

Recuerde que es posible que los datos de la región secundaria no estén actualizados debido al RPO.

**Descripción de los servicios de almacenamiento de Azure**

* **Blobs de Azure**: un almacén de objetos que se puede escalar de forma masiva para datos de texto y binarios. También incluye compatibilidad con el análisis de macrodatos a través de Data Lake Storage Gen2.
* **Azure Files**: recursos compartidos de archivos administrados para implementaciones locales y en la nube.
* **Colas de Azure**: un almacén de mensajería para mensajería confiable entre componentes de aplicación.
* **Azure Disks**: volúmenes de almacenamiento en el nivel de bloque para máquinas virtuales de Azure.

**Ventajas de Azure Storage**

Los servicios de Azure Storage ofrecen las siguientes ventajas para desarrolladores de aplicaciones y profesionales de TI:

* **Duradero y altamente disponible**. La redundancia garantiza que los datos estén seguros en caso de producirse errores de hardware transitorios.
* **Seguro**. Todos los datos escritos en una cuenta de Azure Storage se cifran mediante el servicio. Azure Storage proporciona un control pormenorizado sobre quién tiene acceso a los datos.
* **Escalable**. Azure Storage está diseñado para poderse escalar de forma masiva para satisfacer las necesidades de rendimiento y almacenamiento de datos de las aplicaciones de hoy en día.
* **Administrado**. Azure controla automáticamente el mantenimiento, las actualizaciones y los problemas críticos del hardware.
* **Accesible**. Es posible acceder a los datos de Azure Storage desde cualquier parte del mundo a través de HTTP o HTTPS.

**Blob Storage**

Azure Blob Storage es una solución de almacenamiento de objetos para la nube. Puede almacenar grandes cantidades de datos, como datos de texto o binarios.

Blob Storage resulta muy conveniente para lo siguiente:

* Visualización de imágenes o documentos directamente en un explorador.
* Almacenamiento de archivos para acceso distribuido.
* Streaming de audio y vídeo.
* Almacenamiento de datos para copia de seguridad y restauración, recuperación ante desastres y archivado.
* Almacenamiento de datos para el análisis en local o en un servicio hospedado de Azure.

Azure Storage ofrece diferentes niveles de acceso para el almacenamiento de blobs, lo que le ayuda a almacenar datos de objetos de la manera más rentable. Entre los niveles de acceso disponibles se incluyen:

* **Nivel de acceso frecuente**: optimizado para almacenar datos a los que se accede con frecuencia (por ejemplo, imágenes para el sitio web).
* **Nivel de acceso esporádico**: optimizado para datos a los que se accede con poca frecuencia y que se almacenan al menos durante 30 días (por ejemplo, las facturas de los clientes).
* **Nivel de acceso de archivo**: conveniente para datos a los que raramente se accede y que se almacenan durante al menos 180 días con requisitos de latencia flexibles (por ejemplo, copias de seguridad a largo plazo).

**Las siguientes consideraciones se aplican a los distintos niveles de acceso:**

* Solo los niveles de acceso frecuente y esporádico se pueden establecer en el nivel de cuenta. El nivel de acceso de archivo no está disponible en el nivel de cuenta.
* Los niveles frecuente, esporádico y de archivo se pueden establecer en el nivel de blob durante la carga o después de esta.
* Los datos del nivel de acceso esporádico pueden tolerar una disponibilidad ligeramente inferior, pero aun así requieren una gran durabilidad, una latencia de recuperación y unas características de rendimiento similares a las de los datos de acceso frecuente. En el caso de los datos de acceso esporádico, un contrato de nivel de servicio (SLA) con una disponibilidad ligeramente inferior y unos costos de acceso mayores, en comparación con los datos de acceso frecuente, es aceptable a cambio de unos costos de almacenamiento menores.
* El almacenamiento de archivo almacena datos sin conexión y ofrece los menores costos de almacenamiento, pero los mayores costos de acceso y recuperación de datos.

**Azure Files**

Azure Files ofrece recursos compartidos de archivos totalmente administrados en la nube a los que se puede acceder mediante los protocolos SMB (Bloque de mensajes del servidor) o NFS (Network File System) estándar del sector.

**Ventajas clave de Azure Files:**

* Acceso compartido
* Totalmente administrado
* Scripts y herramientas
* Resistencia
* Capacidad de programación intuitiva

**Queue Storage**

Azure Queue Storage es un servicio para almacenar grandes cantidades de mensajes, Una vez que están almacenados, se puede acceder a los mensajes desde cualquier lugar del mundo mediante llamadas autenticadas con HTTP o HTTPS.

**Disk Storage**

El almacenamiento en disco o los discos administrados de Azure son volúmenes de almacenamiento de nivel de bloque que administra Azure para su uso con máquinas virtuales de Azure. Conceptualmente, son iguales que un disco físico, pero están virtualizados, lo que ofrece mayor resistencia y disponibilidad que un disco físico. Con los discos administrados, lo único que debe hacer es aprovisionar el disco; Azure se encargará del resto.

**Identificación de las opciones de migración de datos de Azure**

**Azure Migrate** es un servicio que le ayuda a migrar desde un entorno local a la nube. Azure Migrate funciona como centro para ayudarle a administrar la valoración y la migración del centro de datos local a Azure. Ofrece lo siguiente:

* **Plataforma de migración unificada**: un único portal para iniciar, ejecutar y realizar un seguimiento de la migración a Azure.
* **Rango de herramientas**: Rango de herramientas para la evaluación y migración Las herramientas de Azure Migrate incluyen Azure Migrate: Discovery y assessment y Azure Migrate: Server Migration. Azure Migrate también se integra con otros servicios y herramientas de Azure, así como con ofertas de proveedores de software independientes (ISV).
* **Assessment and migration** (Evaluación y migración): en el centro de Azure Migrate, puede evaluar y migrar la infraestructura local a Azure.

**Herramientas integradas**

Además de trabajar con herramientas de ISV, el centro de Azure Migrate también incluye las siguientes herramientas para ayudar con la migración:

* **Azure Migrate: Discovery and assessment** (Azure Migrate: detección y evaluación). Detecte y evalúe servidores locales que se ejecutan en VMware, Hyper-V y servidores físicos para preparar la migración a Azure.
* **Azure Migrate: Server Migration** (Azure Migrate: migración del servidor). Migre máquinas virtuales de VMware, máquinas virtuales de Hyper-V, servidores físicos, otros servidores virtualizados y máquinas virtuales de la nube pública a Azure.
* **Data Migration Assistant**. Data Migration Assistant es una herramienta independiente para evaluar servidores de SQL Server. Ayuda a identificar posibles problemas que bloquean la migración. Identifica características no admitidas, nuevas características que puede aprovechar después de la migración y la ruta de acceso correcta para la migración de la base de datos.
* **Azure Database Migration Service**. Migre bases de datos locales a máquinas virtuales de Azure en las que se ejecutan SQL Server, Azure SQL Database o instancias administradas de SQL.
* **Web app migration assistant** (Asistente de migración de aplicación web). Azure App Service Migration Assistant es una herramienta independiente para evaluar sitios web locales para la migración a Azure App Service. Use Migration Assistant para migrar aplicaciones web de .NET y PHP a Azure.
* **Azure Data Box**. Use los productos de Azure Data Box para trasladar grandes cantidades de datos sin conexión a Azure.

**Azure Data Box**

Azure Data Box es un servicio de migración física que ayuda a transferir grandes cantidades de datos de forma rápida, económica y confiable. La transferencia de datos segura se acelera mediante el envío de un dispositivo de almacenamiento propietario de Data Box que tiene una capacidad de almacenamiento utilizable máxima de 80 terabytes.

**Casos de uso**

Data Box es ideal para transferir tamaños de datos con más de 40 TB en escenarios sin conectividad de red limitada. El movimiento de datos puede ser único, periódico o una transferencia de datos masiva inicial seguida de transferencias periódicas.

Estos son los distintos escenarios donde se puede usar Data Box para importar datos en Azure.

* Migración única: cuando se mueve gran cantidad de datos locales a Azure.
* Traslade una biblioteca multimedia de cintas sin conexión a Azure para crear una biblioteca multimedia en línea.
* Migre la granja de máquinas virtuales, SQL Server y las aplicaciones a Azure.
* Traslade los datos históricos a Azure para un análisis exhaustivo y generar informes con HDInsight.
* Transferencia masiva inicial: cuando se realiza una transferencia masiva inicial con Data Box (inicialización) seguida de transferencias incrementales a través de la red.
* Cargas periódicas: cuando se genera periódicamente una gran cantidad de datos y es necesario moverlos a Azure.

Estos son los distintos escenarios donde se puede usar Data Box para exportar datos a Azure.

* Recuperación ante desastres: cuando se restaura una copia de los datos de Azure en una red local. En un escenario de recuperación ante desastres habitual, se exporta una gran cantidad de datos de Azure se exporta a Data Box. Microsoft luego los envía a Data Box y, en poco tiempo, los datos se restauran en un entorno local.
* Requisitos de seguridad: cuando necesita poder exportar datos de Azure debido a los requisitos de seguridad o de la administración pública.
* Migración de vuelta al entorno local o a otro proveedor de servicios en la nube: cuando quiera mover todos los datos de vuelta al entorno local o a otro proveedor de servicios en la nube, exporte los datos a través de Data Box para migrar las cargas de trabajo.

Una vez que los datos del pedido de importación se cargan en Azure, los discos del dispositivo se limpian, según las normas NIST 800-88r1. Si el pedido es de exportación, los discos se borran una vez que el dispositivo llega al centro de datos de Azure.

**Identificación de las opciones de movimiento de archivos de Azure**

Azure también tiene herramientas diseñadas para ayudarle a mover o interactuar con archivos individuales o grupos de archivos pequeños. Entre esas herramientas se encuentran AzCopy, Explorador de Azure Storage y Azure File Sync.

**AzCopy**

AzCopy es una utilidad de línea de comandos que puede usar para copiar blobs o archivos a una cuenta de almacenamiento o desde una cuenta de almacenamiento.

**AzCopy** incluso se puede configurar para trabajar con otros proveedores de nube para ayudar a mover archivos entre nubes.

**Explorador de Azure Storage**

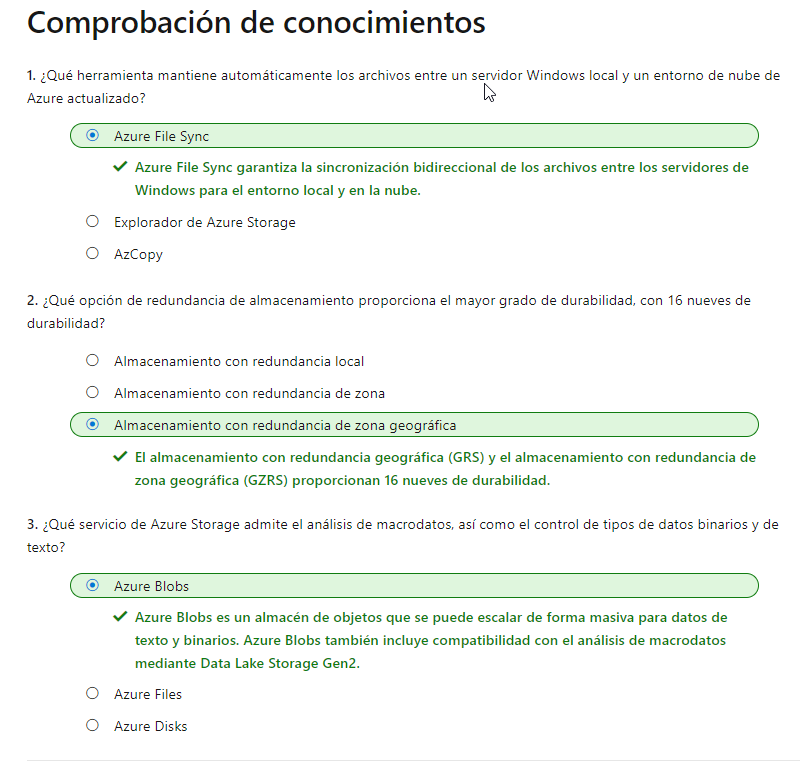
Explorador de Azure Storage es una aplicación independiente que proporciona una interfaz gráfica para administrar archivos y blobs en la cuenta de Azure Storage.

**Azure File Sync**

Azure File Sync es una herramienta que permite centralizar los archivos compartidos en Azure Files y mantener la flexibilidad, el rendimiento y la compatibilidad de un servidor de archivos de Windows.

Con Azure File Sync, puede:

* Usar cualquier protocolo disponible en Windows Server para acceder a sus datos de forma local, como SMB, NFS y FTPS.
* Tener todas las cachés que necesite en todo el mundo.
* Reemplazar un servidor local con errores instalando Azure File Sync en un nuevo servidor del mismo centro de datos.
* Configurar la nube por niveles para que los archivos a los que se accede con más frecuencia se repliquen localmente, mientras que los archivos a los que se accede con poca frecuencia se mantienen en la nube hasta que se soliciten.



**Descripción de los servicios de directorio de Azure**

Azure Active Directory (Azure AD) es un servicio de directorio que le permite iniciar sesión y acceder tanto a las aplicaciones en la nube de Microsoft como a las aplicaciones en la nube que desarrolle.

Azure AD es un servicio de administración de acceso e identidades basado en la nube de Microsoft.

Azure AD puede detectar intentos de inicio de sesión desde ubicaciones inesperadas o dispositivos desconocidos.

**¿Quién usa Azure AD?**

Azure AD es para:

* **Administradores de TI**. Los administradores pueden usar Azure AD para controlar el acceso a las aplicaciones y los recursos en función de sus requisitos empresariales.
* **Desarrolladores de aplicaciones**. Con Azure AD, los desarrolladores pueden agregar funcionalidad a las aplicaciones que compilan mediante un enfoque basado en estándares. Por ejemplo, pueden agregar funcionalidad de SSO a una aplicación o habilitar una aplicación para que funcione con las credenciales existentes de un usuario.
* **Usuarios**. Los usuarios pueden administrar sus identidades y realizar acciones de mantenimiento como el autoservicio de restablecimiento de contraseña.
* **Suscriptores de servicios en línea**. Los suscriptores de Microsoft 365, Microsoft Office 365, Azure y Microsoft Dynamics CRM Online ya usan Azure AD para autenticarse en su cuenta.

**¿Qué hace Azure AD?**

Azure AD proporciona servicios como:

* Autenticación
* Inicio de sesión único
* Administración de aplicaciones
* Administración de dispositivos

**¿Puedo conectar mi AD local con Azure AD?**

Si tuviera un entorno local que ejecuta Active Directory y una implementación en la nube mediante Azure AD, tendría que mantener dos conjuntos de identidades.

Un método de conectar Azure AD con el AD local es usar Azure AD Connect. Azure AD Connect sincroniza las identidades de usuario entre la instalación local de Active Directory y Azure AD.

**¿Qué es Azure Active Directory Domain Services?**

Azure Active Directory Domain Services (Azure AD DS) es un servicio que proporciona servicios de dominio administrados como, por ejemplo, unión a un dominio, directivas de grupo, protocolo ligero de acceso a directorios (LDAP) y autenticación Kerberos o NTLM.

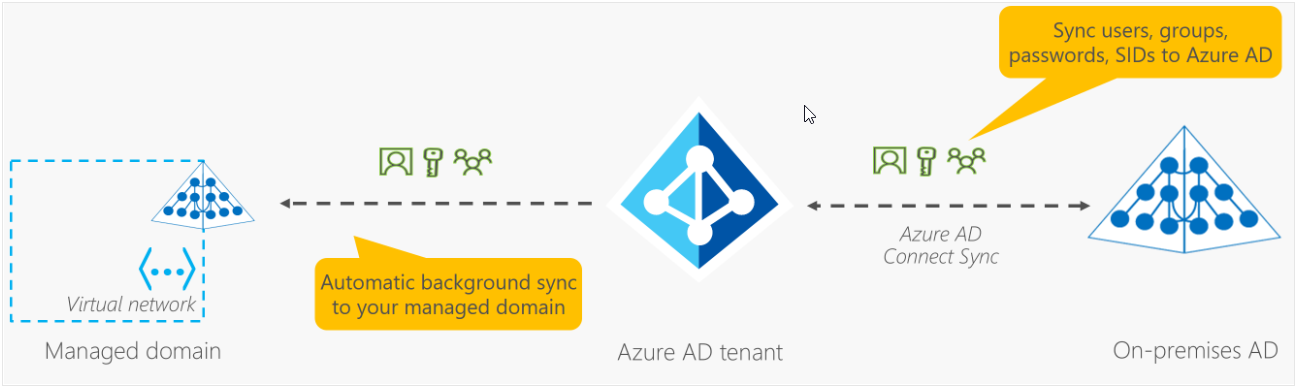
Azure AD DS se integra con el inquilino de Azure AD existente. Esta integración permite a los usuarios iniciar sesión en los servicios y las aplicaciones conectados al dominio administrado con sus credenciales existentes.

**¿Cómo funciona Azure AD DS?**

Cuando cree un dominio administrado de Azure AD DS, defina un espacio de nombres único. Este espacio de nombres es el nombre de dominio. Después, se implementan dos controladores de dominio de Windows Server en la región de Azure seleccionada. Esta implementación de controladores de dominio se conoce como "conjunto de réplicas".

**¿La información está sincronizada?**

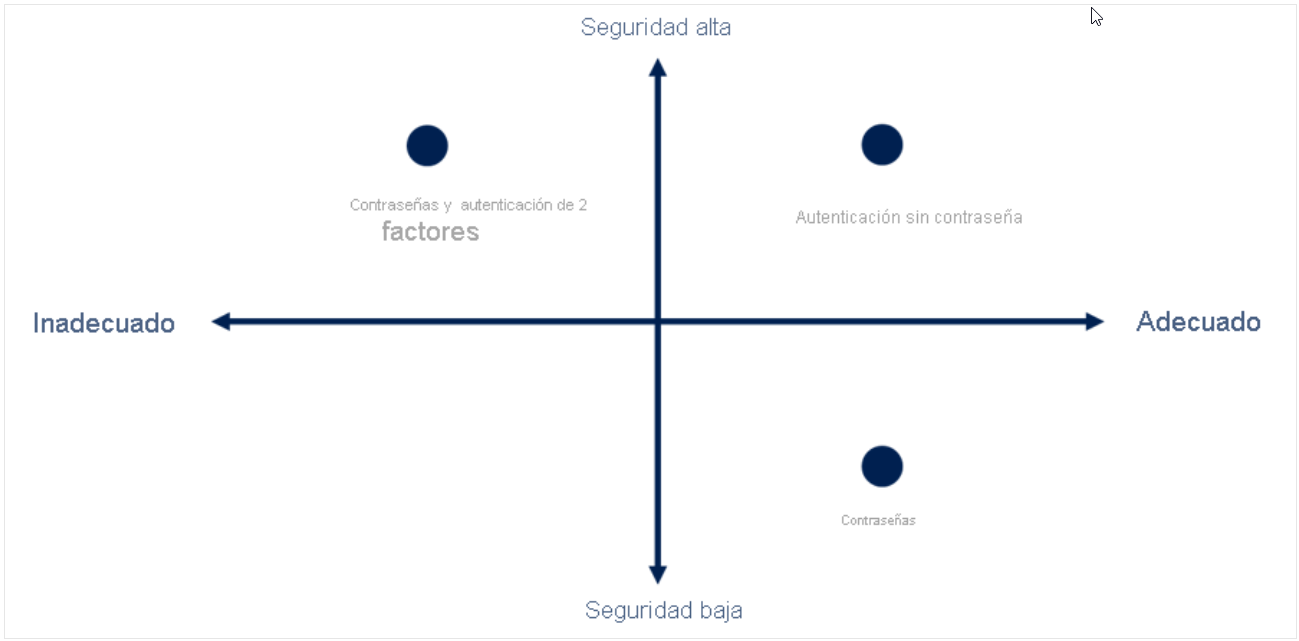
Un dominio administrado está configurado para realizar una sincronización unidireccional de Azure AD a Azure AD DS.



**Descripción de los métodos de autenticación de Azure**

Azure admite varios métodos de autenticación, incluidas las contraseñas estándar, el inicio de sesión único (SSO), la autenticación multifactor (MFA) y el acceso sin contraseña.

Observe que la autenticación sin contraseña es alta seguridad y alta comodidad, mientras que las contraseñas por sí mismas son de baja seguridad pero alta comodidad.



**¿Qué es el inicio de sesión único?**

El inicio de sesión único (SSO) permite a los usuarios iniciar sesión una vez y utilizar esa credencial para acceder a varios recursos y aplicaciones de distintos proveedores.

Con SSO, tan solo debe recordar un ID y una contraseña. El acceso a todas las aplicaciones se concede a una única identidad que está asociada a un usuario, lo que simplifica el modelo de seguridad.

**¿Qué es la autenticación multifactor?**

La autenticación multifactor es el proceso de solicitar a un usuario una forma adicional (o factor) de identificación durante el proceso de inicio de sesión.

La autenticación multifactor proporciona seguridad adicional a las identidades, ya que se requieren dos o más elementos para una autenticación completa. Estos elementos se dividen en tres categorías:

* Algo que el usuario sabe: puede ser una pregunta de seguridad.
* Algo que el usuario tiene: se puede tratar de un código que se envía al teléfono móvil del usuario.
* Algo que el usuario es: normalmente, algún tipo de propiedad biométrica, como la huella dactilar o el escaneo facial.

**¿Qué es Azure AD Multi-Factor Authentication?**

Azure AD Multi-Factor Authentication es un servicio de Microsoft que proporciona funcionalidades de autenticación multifactor. Azure AD Multi-Factor Authentication permite a los usuarios elegir una forma adicional de autenticación durante el inicio de sesión, como una llamada de teléfono o una notificación de aplicación móvil.

**¿Qué es la autenticación sin contraseña?**

El uso de características como la autenticación multifactor constituye una excelente manera de proteger una organización.

Cada organización tiene diferentes necesidades en cuanto a la autenticación. Microsoft Azure global y Azure Government ofrecen las siguientes tres opciones de autenticación sin contraseña que se integran con Azure Active Directory (Azure AD):

* Windows Hello para empresas
* Aplicación Microsoft Authenticator
* Claves de seguridad FIDO2

**Windows Hello para empresas**

Windows Hello para empresas resulta muy conveniente para los trabajadores de la información que tienen su propio equipo con Windows designado.

**Aplicación Microsoft Authenticator**

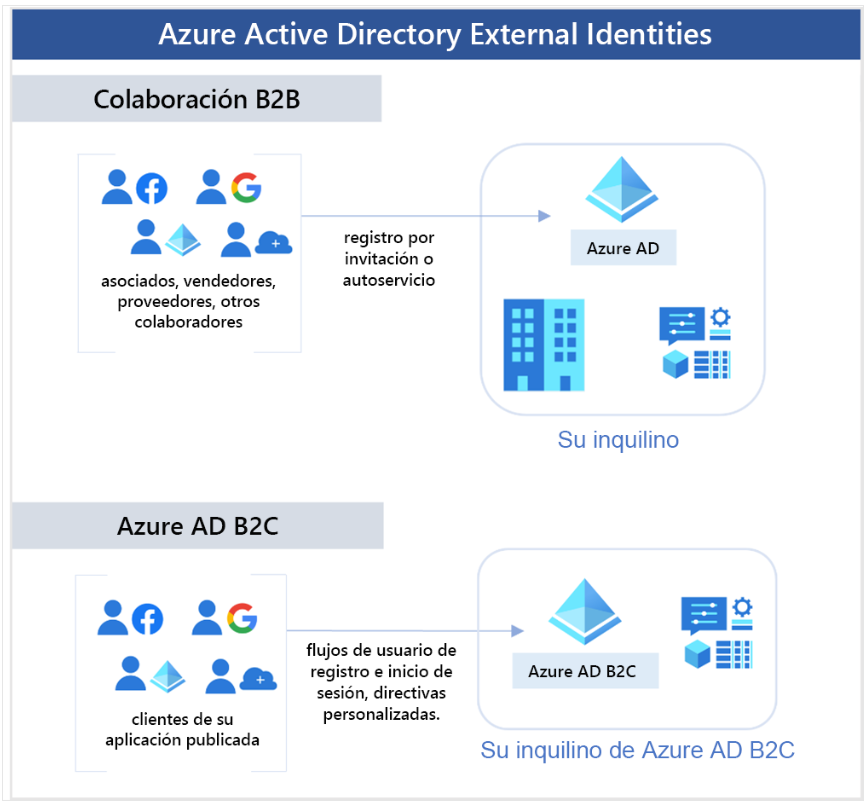
También puede permitir que el teléfono del empleado se convierta en un método de autenticación sin contraseña. Es posible que ya esté usando la aplicación Microsoft Authenticator como una opción de autenticación multifactor cómoda sumada a una contraseña.

**Claves de seguridad FIDO2**

FIDO (Fast IDentity Online) Alliance ayuda a promover los estándares de autenticación abiertos y a reducir el uso de contraseñas como forma de autenticación. FIDO2 es el estándar más reciente que incorpora el estándar de autenticación web (WebAuthn).

**Descripción de identidades externas de Azure**

Una identidad externa es una persona, un dispositivo, un servicio, etc. que está fuera de la organización. Azure AD External Identities hace referencia a todas las formas en que puede interactuar de forma segura con usuarios externos a su organización.



Las siguientes funcionalidades componen External Identities:

* **Colaboración de empresa a empresa (B2B)**: Los usuarios de colaboración B2B se representan en el directorio, normalmente como usuarios invitados.
* **Conexión directa B2B**: La conexión directa B2B actualmente es compatible con los canales compartidos de Teams, lo que permite a los usuarios externos acceder a sus recursos desde sus instancias principales de Teams.
* **Empresa a cliente de Azure AD (B2C)**: publique aplicaciones SaaS modernas o aplicaciones desarrolladas de forma personalizada (excepto aplicaciones de Microsoft) para consumidores y clientes, mientras usa Azure AD B2C para la administración de identidades y acceso.

Con Azure Active Directory (Azure AD), puede habilitar fácilmente la colaboración entre distintas organizaciones mediante la característica B2B de Azure AD.

**Descripción del acceso condicional de Azure**

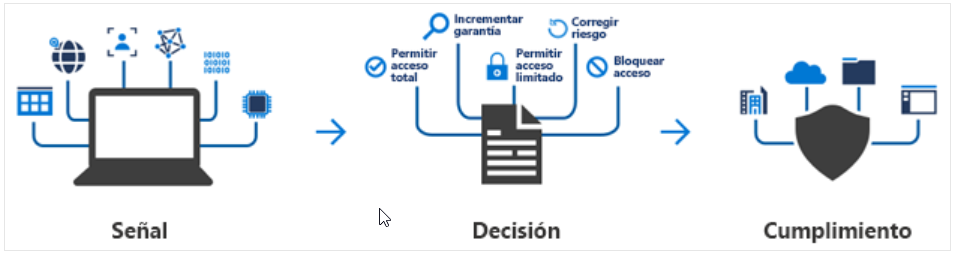
El acceso condicional es una herramienta que usa Azure Active Directory para permitir (o denegar) el acceso a los recursos en función de señales de identidad.

Con el acceso condicional, los administradores de TI pueden:

* permitir a los usuarios ser productivos en cualquier momento y lugar;
* proteger los recursos de la organización.

Durante el inicio de sesión, el acceso condicional recopila señales del usuario, toma decisiones basadas en esas señales y, después, aplica esa decisión para permitir o denegar la solicitud de acceso, o bien exigir una respuesta de autenticación multifactor.

En el diagrama siguiente se muestra este flujo:



**¿Cuándo se puede usar el acceso condicional?**

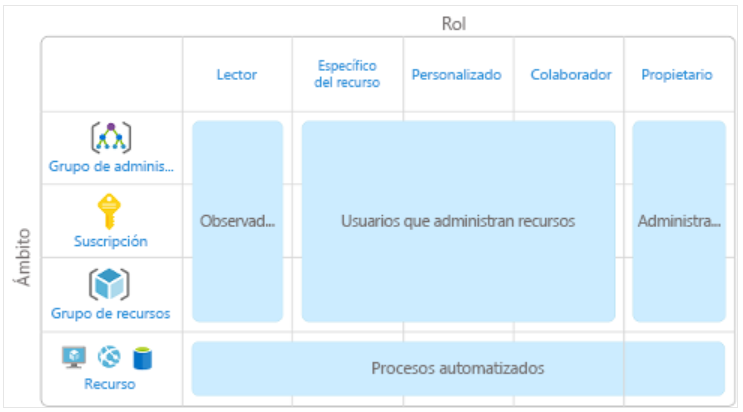
El acceso condicional resulta útil en los casos siguientes:

* Exija la autenticación multifactor (MFA) para acceder a una aplicación en función del rol, la ubicación o la red del solicitante. Por ejemplo, podría requerir MFA para administradores, pero no para usuarios normales o personas que se conectan desde fuera de la red corporativa.
* Para requerir el acceso a los servicios solo a través de aplicaciones cliente aprobadas. Por ejemplo, podría limitar qué aplicaciones de correo electrónico pueden conectarse al servicio de correo electrónico.
* Exija que los usuarios accedan a la aplicación solo desde dispositivos administrados. Un dispositivo administrado es un dispositivo que cumple los estándares de seguridad y cumplimiento.
* Para bloquear el acceso desde orígenes que no son de confianza, como ubicaciones desconocidas o inesperadas.

**Descripción del control de acceso basado en roles de Azure**

**¿Cómo se aplica el control de acceso basado en roles a los recursos?**

El control de acceso basado en roles se aplica a un ámbito, que es un recurso o un conjunto de recursos en los que este acceso se permite.



Los ámbitos pueden ser lo siguiente:

* Un grupo de administración (una colección de varias suscripciones)
* Una sola suscripción
* Un grupo de recursos.
* Un solo recurso

RBAC de Azure es jerárquico, ya que, al conceder acceso en un ámbito primario, todos los ámbitos secundarios heredan esos permisos. Por ejemplo:

* Cuando asignamos el rol Propietario a un usuario en el ámbito del grupo de administración, dicho usuario podrá administrar todo el contenido de todas las suscripciones dentro de ese grupo de administración.
* Cuando asignamos el rol Lector a un grupo en el ámbito de suscripción, los miembros de dicho grupo podrán ver todos los grupos de recursos y recursos dentro de esa suscripción.

**¿Cómo se aplica RBAC de Azure?**

RBAC de Azure emplea un modelo de permisos. Cuando se le asigna un rol, RBAC de Azure le permite realizar acciones dentro del ámbito de ese rol. Si una asignación de roles nos concede permisos de lectura a un grupo de recursos y otra asignación de roles nos concede permisos de escritura al mismo grupo de recursos, tendremos permisos tanto de lectura como de escritura en ese grupo de recursos.

**Descripción del modelo de Confianza cero**

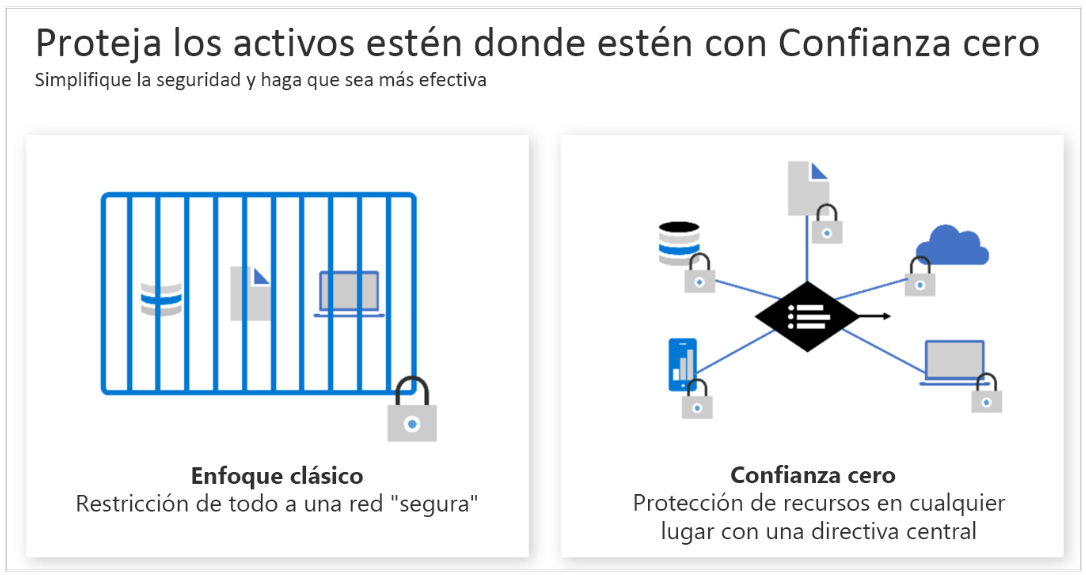
Confianza cero es un modelo de seguridad que supone el peor de los escenarios posibles y protege los recursos con esa expectativa.

Para abordar este nuevo mundo informático, Microsoft recomienda encarecidamente el modelo de seguridad de Confianza cero, que se basa en estos principios rectores:

* **Comprobar explícitamente**: realice siempre las operaciones de autorización y autenticación en función de todos los puntos de datos disponibles.
* **Usar el acceso de privilegios mínimos**: limite el acceso de los usuarios con Just-in-Time y Just-Enough-Access (JIT/JEA), directivas que se adaptan al nivel de riesgo y protección de datos.
* **Asumir que hay brechas**: minimice el radio de expansión y el acceso a los segmentos. Comprobación del cifrado de un extremo a otro. Utilice el análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

**Ajuste a Confianza cero**

El modelo de Confianza cero revoluciona ese escenario. En lugar de suponer que un dispositivo es seguro porque está dentro de la red corporativa, exige que todos los usuarios se autentiquen. Después, concede acceso basado en la autenticación, no de la ubicación.



**Descripción de defensa en profundidad**

El objetivo de la defensa en profundidad es proteger la información y evitar que personas no autorizadas a acceder puedan sustraerla.

**Capas de defensa en profundidad**

Puede visualizar la defensa en profundidad como un conjunto de capas, con los datos que se van a proteger en el centro y todas las demás capas en funcionamiento para proteger esa capa de datos central.



Aquí tiene una breve descripción del rol de cada capa:

* La capa de seguridad física es la primera línea de defensa para proteger el hardware informático del centro de datos.
* La capa de identidad y acceso controla el acceso a la infraestructura y al control de cambios.
* La capa perimetral usa protección frente a ataques de denegación de servicio distribuido (DDoS) para filtrar los ataques a gran escala antes de que puedan causar una denegación de servicio para los usuarios.
* La capa de red limita la comunicación entre los recursos a través de controles de acceso y segmentación.
* La capa de proceso protege el acceso a las máquinas virtuales.
* La capa de aplicación ayuda a garantizar que las aplicaciones sean seguras y estén libres de vulnerabilidades de seguridad.
* La capa de datos controla el acceso a los datos empresariales y de clientes que es necesario proteger.

Azure proporciona herramientas y características de seguridad en todas las capas del concepto de defensa en profundidad. Veamos cada capa con más detalle:

**Seguridad física**

La protección física del acceso a los edificios y el control del acceso al hardware de proceso del centro de datos son la primera línea de defensa.

**Identidad y acceso**

La capa de identidad y acceso consiste en garantizar que las identidades están protegidas, que solo se otorga el acceso necesario y que se registran los cambios y los eventos de inicio de sesión.

En esta capa, es importante que realice lo siguiente:

* Controle el acceso a la infraestructura y al control de cambios.
* Use el inicio de sesión único (SSO)y la autenticación multifactor.
* Audite los eventos y los cambios.

**Perímetro**

El perímetro de la red protege frente a ataques basados en red contra los recursos. Identificar estos ataques, eliminar sus repercusiones y recibir alertas sobre ellos cuando suceden son formas importantes de proteger la red.

En esta capa, es importante que realice lo siguiente:

* Use protección contra DDoS para filtrar los ataques a gran escala antes de que puedan afectar a la disponibilidad de un sistema para los usuarios.
* Use firewalls perimetrales para identificar los ataques malintencionados contra la red y alertar sobre ellos.

**Red**

En esta capa, el enfoque está en limitar la conectividad de la red en todos los recursos para permitir solo la necesaria.

* Limite la comunicación entre los recursos.
* Deniegue de forma predeterminada.
* Restrinja el acceso entrante de Internet y limite el saliente cuando sea apropiado.
* Implemente conectividad segura a las redes locales.

**Compute**

El software malintencionado, los sistemas sin revisiones aplicadas y los sistemas protegidos inadecuadamente abren el entorno a los ataques.

En esta capa, es importante que realice lo siguiente:

* Proteja el acceso a las máquinas virtuales.
* Implemente la protección del punto de conexión de los dispositivos y mantenga los sistemas revisados y actualizados.

**Application**

La integración de la seguridad en el ciclo de vida de desarrollo de aplicaciones ayuda a reducir el número de vulnerabilidades en el código.

* Garantice que las aplicaciones son seguras y están libres de vulnerabilidades.
* Almacene los secretos de aplicación confidenciales en un medio de almacenamiento seguro.
* Convierta la seguridad en un requisito de diseño en todo el desarrollo de aplicaciones.

**data**

Los que almacenan y controlan el acceso a los datos son responsables de asegurarse de que están protegidos correctamente.

En casi todos los casos, los atacantes intentan conseguir datos:

* Almacenados en una base de datos.
* Almacenados en discos en máquinas virtuales.
* Almacenados en aplicaciones de software como servicio (SaaS), como Office 365.
* Administrados mediante el almacenamiento en la nube.

**Descripción de Microsoft Defender for Cloud**

Microsoft Defender for Cloud es una herramienta de supervisión para la administración de la posición de seguridad y la protección contra amenazas.

Defender for Cloud proporciona las herramientas necesarias para proteger los recursos, realizar un seguimiento de su posición de seguridad, protegerse frente a ciberataques y simplificar la administración de la seguridad. La implementación de Defender for Cloud es fácil, ya está integrada de forma nativa en Azure.

**Protección allá donde se implemente**

Dado que Defender for Cloud es un servicio nativo de Azure, muchos servicios de Azure se supervisan y protegen sin necesidad de ninguna implementación.

Cuando sea necesario, Defender for Cloud puede implementar automáticamente un agente de Log Analytics para recopilar datos relacionados con la seguridad.

Para entornos híbridos y de varias nubes, los planes de Microsoft Defender se amplían a máquinas que no son de Azure con la ayuda de Azure Arc.

**Protecciones nativas de Azure**

Defender for Cloud le permite detectar amenazas en:

* Servicios de PaaS de Azure: puede detectar amenazas dirigidas a servicios de Azure como Azure App Service, Azure SQL, la cuenta de Azure Storage y otros servicios de datos. También puede realizar la detección de anomalías en los registros de actividad de Azure mediante la integración nativa con Microsoft Defender para aplicaciones en la nube (anteriormente conocido como Microsoft Cloud App Security).
* Servicios de datos de Azure: Defender for Cloud incluye capacidades que le ayudarán a clasificar automáticamente los datos en Azure SQL. También puede obtener evaluaciones de las posibles vulnerabilidades en los servicios de Azure SQL y Azure Storage, además de recomendaciones sobre cómo mitigarlas.
* Redes: Defender for Cloud le permite limitar la exposición a los ataques por fuerza bruta. Si reduce el acceso a los puertos de las máquinas virtuales mediante el acceso de máquina virtual Just-In-Time, puede proteger la red al prevenir el acceso innecesario. Puede establecer directivas de acceso seguro en los puertos seleccionados, solo para usuarios autorizados, direcciones IP o intervalos de direcciones IP de origen permitidos y durante un período limitado.

**Defensa de los recursos híbridos**

Defender for Cloud también puede proteger los recursos de otras nubes (como AWS y GCP).

Por ejemplo, si ha conectado una cuenta de Amazon Web Services (AWS) a una suscripción de Azure, puede habilitar cualquiera de estas protecciones:

* Las características de CSPM de Defender for Cloud se extienden a los recursos de AWS. Este plan sin agente evalúa los recursos de AWS según las recomendaciones de seguridad específicas de AWS e incluye los resultados en la puntuación de seguridad. También se evaluará el cumplimiento de los recursos de los estándares integrados específicos de AWS (AWS CIS, AWS PCI DSS y Procedimientos recomendados de seguridad fundamentales de AWS). La página de inventario de recursos de Defender for Cloud es una característica habilitada para varias nubes que permite administrar los recursos de AWS junto con los de Azure.
* Microsoft Defender para Kubernetes amplía la detección de amenazas de contenedores y defensas avanzadas a los clústeres Linux de Amazon EKS.
* Microsoft Defender para servidores proporciona la detección de amenazas y defensas avanzadas a las instancias de EC2 con Windows y Linux.

**Evaluación, protección y defensa**

Defender for Cloud cubre tres necesidades vitales a medida que administra la seguridad de los recursos y las cargas de trabajo en la nube y en el entorno local:

* Evaluación continua: conozca la posición de seguridad. Identifique y realice un seguimiento de las vulnerabilidades.
* Protección: proteja los recursos y los servicios con Azure Security Benchmark.
* Defensa: detecte y resuelva las amenazas a recursos, cargas de trabajo y servicios.



**Evaluación continua**

Microsoft Defender para servidores incluye integración nativa automática con Microsoft Defender para puntos de conexión. Si ha habilitado esta integración, tendrá acceso a los hallazgos relacionados con vulnerabilidades de la administración de amenazas y vulnerabilidades de Microsoft.

Entre estas herramientas de evaluación tendrá exámenes de vulnerabilidades regulares y detallados que cubren el proceso, los datos y la infraestructura. Puede revisar los resultados de estos exámenes desde Defender for Cloud y responder a ellos.

**Seguridad**

Desde los métodos de autenticación hasta el control de acceso y el concepto de Confianza cero, la seguridad en la nube es un aspecto esencial que debe realizarse correctamente.

Defender for Cloud evalúa si los nuevos recursos están configurados según los procedimientos recomendados de seguridad. Si no es así, se marcan y se obtiene una lista prioritaria de recomendaciones para lo que necesita corregir. Las recomendaciones le permitirán disminuir la superficie expuesta a ataques en cada uno de los recursos.

**Defensa**

Las dos primeras áreas se centraban en evaluar, supervisar y mantener su entorno. Defender for Cloud también le permite defender su entorno proporcionando alertas de seguridad y características avanzadas de protección contra amenazas.

**Alertas de seguridad**

Cuando Defender para la nube detecta una amenaza en cualquier área del entorno, genera una alerta de seguridad. Alertas de seguridad:

* Descripción de los detalles de los recursos afectados
* Sugerencia de pasos para la corrección
* Suministro, en algunos casos, de una opción para desencadenar una aplicación lógica en la respuesta

Tanto si Defender para la nube genera una alerta como si la recibe desde un producto de seguridad integrado, puede exportarla. La protección contra amenazas de Defender para la nube incluye el análisis de la cadena de eliminación de fusión, que correlaciona de manera automática las alertas del entorno en función del análisis Cyber Kill Chain, para ayudarle a comprender mejor todo el proceso de un ataque, dónde empezó y qué tipo de impacto tuvo en los recursos.

**Protección contra amenazas avanzada**

Defender for Cloud proporciona características avanzadas de protección contra amenazas para muchos de los recursos implementados, incluidas las máquinas virtuales, las bases de datos SQL, los contenedores, las aplicaciones web y la red. Entre las protecciones se incluyen la protección de los puertos de administración de las VM con acceso Just-in-Time y controles de aplicaciones adaptables para crear listas de permitidos con las aplicaciones que deben o no ejecutarse en las máquinas.

