

# AZ-305: Diseño de soluciones de infraestructura de Microsoft Azure

## Requisitos previos de AZ-305 Microsoft Azure Architect Design

**La infraestructura física de Azure** comienza con los centros de datos.

Conceptualmente, los centros de datos son iguales que los grandes centros de datos corporativos. Son instalaciones con recursos organizados en bastidores, con potencia dedicada, refrigeración e infraestructura de red. Los centros de datos se agrupan en regiones de Azure o Azure Availability Zones, están diseñados para ayudarte a lograr resistencia y confiabilidad para las cargas de trabajo críticas para la empresa.

**Una región** es un área geográfica del planeta que contiene al menos un centro de datos, aunque podrían ser varios cercanos y conectados mediante una red de baja latencia. Azure asigna y controla los recursos de forma inteligente dentro de cada región para garantizar que las cargas de trabajo están bien compensadas.

**Las zonas de disponibilidad** son centros de datos separados físicamente dentro de una región de Azure. Cada zona de disponibilidad consta de uno o varios centros de datos equipados con alimentación, refrigeración y redes independientes.

**Las zonas de disponibilidad** son principalmente para las máquinas virtuales, los discos administrados, los equilibradores de carga y las bases de datos SQL. Los servicios de Azure que admiten zonas de disponibilidad se dividen en tres categorías:

- **Servicios de zona:** ancla 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.

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. Este enfoque permite la replicación de recursos en una zona geográfica que ayuda a reducir la probabilidad de que se produzcan interrupciones provocadas por eventos como desastres naturales, disturbios sociales, cortes del suministro eléctrico o interrupciones de la red física que afecten a una región completa.

**Las regiones soberanas** son instancias de Azure que están aisladas de la instancia principal de Azure. Es posible que tenga que usar una región soberana con fines legales o de cumplimiento.

Entre las regiones soberanas de Azure se incluyen las siguientes:

- **US DoD (centro), US Gov Virginia, US Gov Iowa y más:** Estas regiones son instancias físicas y lógicas con aislamiento de red de Azure para asociados y agencias de la administración pública de EE. UU. Estos centros de datos están operados por personal estadounidense sometido a evaluación e incluyen certificaciones de cumplimiento adicionales.
- **Este de China, Norte de China y más:** Estas regiones están disponibles gracias a una asociación exclusiva entre Microsoft y 21Vianet, por la cual Microsoft no mantiene directamente los centros de datos.

**La infraestructura de administración** incluye recursos de Azure y grupos de recursos, suscripciones y cuentas. Comprender la organización jerárquica le ayudará a planear los proyectos y productos dentro 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. Los grupos de recursos no se pueden anidar, lo que significa que no se puede colocar el grupo de recursos B dentro del grupo de recursos A. Los grupos de recursos proporcionan una manera cómoda de agrupar recursos. Al aplicar una acción a un grupo de recursos, se aplicará a todos los recursos que contiene. Si elimina un grupo de recursos, se eliminarán todos los recursos que contiene. Si concede o deniega el acceso a un grupo de recursos, habrá concedido o denegado acceso a todos los recursos que contiene.

**Las suscripciones** son una unidad de administración, facturación y escala. Al igual que los grupos de recursos son una manera de organizar lógicamente los recursos, las suscripciones permiten organizar lógicamente los grupos de recursos y facilitar la facturación. El uso de Azure requiere una suscripción de Azure. Una suscripción le proporciona acceso autenticado y autorizado a los servicios y productos de Azure.

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.

suscripciones adicionales para separar lo siguiente:

- **Entornos:** puedes 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:** puedes 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:** puedes crear suscripciones adicionales con fines de facturación. Dado que los costos se agregan primero en el nivel de suscripción, es posible que quieras crear suscripciones para administrar y realizar un seguimiento de los costos en función de sus necesidades. Por ejemplo, puede que quieras crear una suscripción para las cargas de trabajo de producción, y otra suscripción para las cargas de trabajo de desarrollo y pruebas.

**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. Todas las suscripciones de un grupo de administración heredan automáticamente las condiciones que tenga aplicadas, de la misma manera que los grupos de recursos heredan la configuración de las suscripciones y los recursos heredan de los grupos de recursos. 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. **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.

### 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.

**Una máquina virtual de Azure** te ofrece la flexibilidad de la virtualización sin necesidad de adquirir y mantener el hardware físico que ejecuta la máquina virtual. Pero, como oferta de IaaS, tendrá que configurar, actualizar y mantener el software que se ejecuta en la máquina virtual. Las máquinas virtuales son una opción ideal cuando necesitas lo siguiente:

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

**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, macrodatos y cargas de trabajo de contenedor.

**Los conjuntos de disponibilidad** de máquinas virtuales son otra herramienta que le ayudará a crear un entorno más resistente y de alta disponibilidad. 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.

Al aprovisionar una máquina virtual, también tendrás la oportunidad de elegir los recursos asociados a esa máquina virtual, como los siguientes:

- Tamaño (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)

**Azure Virtual Desktop** es un servicio de virtualización de escritorios y aplicaciones que se ejecuta en la nube. Te 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 puedes usar para acceder a escritorios remotos o a la mayoría de exploradores modernos. 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.

**Los contenedores** son un entorno de virtualización. Los contenedores son ligeros y se han diseñado para crearse, escalarse horizontalmente y detenerse de forma dinámica. Uno de los motores de contenedores más populares es Docker. Y Azure es compatible con Docker. 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. Por ejemplo, se puede dividir un sitio web en un contenedor que hospeda el front-end, otro que hospeda el back-end y un tercero para el almacenamiento. De esta forma, puedes separar partes de la aplicación en secciones lógicas que se pueden mantener, escalar o actualizar independientemente.

**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. Azure Container Instances es una oferta de plataforma como servicio (PaaS). Azure Container Instances te permite cargar los contenedores.

**Azure Container Apps** son similares de muchas maneras a una instancia de contenedor. Le permiten ponerse en marcha de inmediato, quitan la pieza de administración de contenedores y son una oferta de PaaS. Container Apps tienen ventajas adicionales, como la capacidad de incorporar el equilibrio de carga y el escalado.

**Azure Kubernetes Service (AKS)** es un servicio de orquestación de contenedores. Un servicio de orquestación administra el ciclo de vida de los contenedores. Al implementar una flota de contenedores, AKS puede hacer que la administración de flotas sea más sencilla y eficaz.

**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. Las funciones pueden ser **sin estado** o **con estado**. Cuando son sin estado (**valor predeterminado**), se comportan como si se reiniciaran cada vez que responden a un evento. Cuando son con estado (denominado **Durable Functions**), se pasa un contexto a través de la función para realizar el seguimiento antes de la actividad.

**Azure 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. 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. 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

**Las redes virtuales y las subredes virtuales** de Azure permiten a los recursos de Azure, como las máquinas virtuales, las aplicaciones web y las bases de datos, comunicarse entre sí, con los usuarios de Internet y con los equipos cliente en el entorno local. 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.

Le interesaría 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.

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.

**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.

**Las rutas definidas por el usuario (UDR)** permiten controlar las tablas de enrutamiento entre subredes dentro de una red virtual o entre redes virtuales. Esto permite un mayor control sobre el flujo de tráfico de red.

**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. El emparejamiento permite que los recursos de cada red virtual se comuniquen entre sí. Estas redes virtuales pueden estar en regiones distintas, lo que permite crear una red global interconectada con Azure.

**Una red privada virtual (VPN)** usa un túnel cifrado en otra red. Normalmente, las VPN se implementan para conectar entre sí dos o más redes privadas de confianza a través de una red que no es de confianza (normalmente, la red pública de Internet).

**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.

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

**Las instancias de VPN Gateway** se implementan como dos instancias en una configuración de activo-en espera, incluso si solo ve un recurso de VPN Gateway en Azure. Cuando el mantenimiento planeado o la interrupción imprevista afectan a la instancia activa, la instancia en espera asume de forma automática la responsabilidad de las conexiones sin ninguna intervención del usuario. Durante esta conmutación por error, las conexiones se interrumpen, pero por lo general se restauran en cuestión de segundos si se trata del mantenimiento planeado y en un plazo de 90 segundos en el caso de las interrupciones imprevistas.

**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. La conectividad puede ser desde una red de conectividad universal (IP VPN), una red Ethernet de punto a punto o una conexión cruzada virtual a través de un proveedor de conectividad en una instalación de ubicación compartida. **Las conexiones de ExpressRoute no pasan por la red pública de Internet.** Esto permite a las conexiones de ExpressRoute ofrecer más confiabilidad, más velocidad, latencia coherentes y mayor seguridad que las conexiones normales a través de Internet.

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

- Conectividad a 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.

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

ExpressRoute usa el BGP. BGP (Border Gateway Protocol) se usa para intercambiar rutas entre las redes locales y los recursos que se ejecutan en Azure. Este protocolo permite el enrutamiento dinámico entre la red local y los servicios que se ejecutan en la nube de Microsoft.

**ExpressRoute** admite cuatro modelos que puede usar para conectar la red local con la nube de Microsoft:

- Ubicación de CloudExchange
- Conexión Ethernet de punto a punto
- Conexión universal
- Directamente desde sitios de ExpressRoute

**La ubicación conjunta** hace referencia al centro de datos, la oficina u otras instalaciones que se encuentran físicamente en un intercambio en la nube, como un ISP. Si la instalación tiene la ubicación compartida en un intercambio en la nube, puede solicitar una conexión cruzada virtual a la nube de Microsoft.

**La conexión Ethernet de punto a punto** hace referencia al uso de una conexión punto a punto para conectar la instalación a la nube de Microsoft.

**Con la conectividad universal**, puede integrar la red de área extensa (WAN) con Azure si proporciona conexiones a las oficinas y los centros de datos. Azure se integra con la conexión WAN para proporcionarle una conexión, como la que tendría entre el centro de datos y las sucursales.

Puede conectarse **directamente a la red global de Microsoft** en una ubicación de emparejamiento distribuida estratégicamente por todo el mundo. ExpressRoute Direct proporciona conectividad dual de 100 Gbps o 10 Gbps, que es compatible con la conectividad activa/activa a escala.

**Azure DNS** es un servicio de hospedaje para dominios DNS que ofrece resolución de nombres mediante la infraestructura de Microsoft Azure. Al hospedar dominios en Azure, puede administrar los registros DNS con las mismas credenciales, API, herramientas y facturación que con los demás servicios de Azure.

Azure DNS saca provecho del ámbito y la escala de Microsoft Azure para proporcionar numerosas ventajas, incluidas las siguientes:

- Confiabilidad y rendimiento
- Seguridad
- Facilidad de uso
- Redes virtuales personalizables
- Registros de alias

Azure DNS se basa en Azure Resource Manager, que proporciona características tales como:

- Control de acceso basado en rol de Azure (Azure RBAC) para controlar quién accede a acciones específicas en la organización.

- Registros de actividad: para supervisar cómo un usuario de su organización modificó un recurso o para encontrar errores al solucionar problemas.
- Bloqueo de recursos para bloquear una suscripción, un grupo de recursos o un recurso. Los bloqueos impiden que otros usuarios de la organización eliminan o modifiquen de forma accidental recursos críticos.

Azure DNS es compatible con dominios DNS privados. Esta característica permite usar nombres de dominio personalizados propios en las redes virtuales privadas, en lugar de limitarse a los nombres proporcionados por 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.

Tipo	Servicios admitidos	Opciones de redundancia	Uso
De uso general estándar, v2	Blob Storage (incluido Data Lake Storage), Queue Storage, Table Storage y Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Tipo de cuenta de almacenamiento estándar para blobs, archivos, colas y tablas. Se recomienda para la mayoría de los escenarios con Azure Storage. Si desea compatibilidad con el sistema de archivos de red (NFS) en Azure Files, utilice el tipo de cuenta de recursos compartidos de archivos Premium.
Blobs en bloques Premium	Blob Storage (incluido Data Lake Storage)	LRS, ZRS	Tipo de cuenta de almacenamiento Prémium para blobs en bloques y blobs en anexos. Se recomiendan para escenarios con altas tasas de transacciones, que utilizan objetos más pequeños o que requieren una latencia de almacenamiento constantemente baja.
Recursos compartidos de archivos Prémium	Azure Files	LRS, ZRS	Tipo de cuenta de almacenamiento Prémium solo para recursos compartidos de archivos. Se recomienda para empresas y aplicaciones de escalado de alto rendimiento. Use este tipo de cuenta si desea una cuenta de almacenamiento que admite recursos compartidos de archivos de Bloque de mensajes del servidor (SMB) y NFS.
Blobs en páginas Premium	Solo blobs en páginas	LRS	Tipo de cuenta de almacenamiento premium solo para blobs en páginas.

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.

**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. **La redundancia** garantiza que la cuenta de almacenamiento cumple sus objetivos de disponibilidad y durabilidad, aunque se produzcan errores.

**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).

**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 (99,99999999 %) 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. LRS protege los datos frente a errores en la estantería de servidores y en la unidad.

**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. ZRS proporciona a los objetos de datos de Azure Storage una durabilidad de al menos 12 nueves (99,99999999 %) durante un año determinado. Con ZRS, los datos son accesibles para las operaciones de escritura y lectura incluso si una zona deja de estar disponible. Microsoft recomienda usar ZRS en la región primaria para escenarios que requieren de alta disponibilidad. También se recomienda ZRS para restringir la replicación de datos dentro de un país o región para cumplir los requisitos de gobernanza de datos.

**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). GRS es similar a ejecutar LRS en dos regiones, y GZRS es similar a ejecutar ZRS en la región primaria y LRS en la región secundaria.

**GRS** copia los datos de manera sincrónica tres veces dentro de una ubicación física única en la región primaria mediante LRS. Luego copia los datos de forma asincrónica en una única ubicación física en la región secundaria (el par de regiones) mediante LRS. GRS proporciona a los objetos de datos de Azure Storage una durabilidad de al menos 16 nueves (99,99999999999999 %) durante un año determinado.

**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. Microsoft recomienda el uso de GZRS en aplicaciones que requieran de coherencia, durabilidad y disponibilidad máximas, además de rendimiento excelente y resistencia para la recuperación ante desastres. **GZRS** está diseñado para proporcionar una durabilidad mínima de 16 nueves (99,99999999999999 %) de los objetos en un año determinado.

El **RPO** (Punto Objetivo de Recuperación) indica momento concreto en que se pueden recuperar los datos. Normalmente, Azure Storage tiene un RPO inferior a 15 minutos, aunque actualmente no hay ningún contrato de nivel de servicio sobre el tiempo que se tarda en replicar los datos en la región secundaria.

La plataforma de Azure Storage incluye los servicios de datos siguientes:

- **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.
- **Tablas de Azure:** Opción tabla NoSQL para datos estructurados y no relacionales.

**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. Azure Blob Storage no está estructurada, lo que significa que no hay ninguna restricción en cuanto a los tipos de datos que puede contener. Blob Storage puede administrar miles de cargas simultáneas, cantidades enormes de datos de vídeo, archivos de registro en constante crecimiento y es accesible desde cualquier lugar con conexión a Internet. Un blob podría contener gigabytes de datos binarios transmitidos desde un instrumento científico, un mensaje cifrado para otra aplicación o datos en un formato personalizado para una aplicación que se está desarrollando.

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 esporádico:** está optimizado para almacenar datos a los que se accede con poca frecuencia y al menos durante 90 días.
- **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).

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

**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. Una cola puede contener tantos mensajes como el espacio que tenga la cuenta de almacenamiento (pueden ser millones). Cada mensaje individual de la cola puede llegar a tener un tamaño máximo de 64 KB.

**El almacenamiento en Azure Disk** 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.

**Azure Table Storage** permite almacenar una gran cantidad de datos estructurados. Las tablas de Azure son un almacén de datos NoSQL que acepta llamadas autenticadas desde dentro y fuera de la nube de Azure. Las tablas de Azure son ideales para el almacenamiento de datos estructurados no relacionales.

**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.

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.
- **Azure App Service Migration Assistant.** Azure App Service Migration Assistant es una herramienta independiente utilizada 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** 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**. Data Box se transporta hacia y desde el centro de datos a través de un transportista regional. Una caja resistente asegura y protege Data Box de daños durante el trayecto. El servicio de Data Box se encarga de realizar el seguimiento de todo el proceso en Azure Portal. **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.

**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. Con AzCopy, puede copiar archivos entre cuentas de almacenamiento, cargarlos, descargarlos e incluso sincronizarlos. AzCopy incluso se puede configurar para trabajar con otros proveedores de nube para ayudar a mover archivos entre nubes.

**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** 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.

**Microsoft Entra ID** 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. Microsoft Entra ID también puede ayudarle a mantener la implementación de Active Directory local. Microsoft Entra ID es el servicio de administración de identidades y acceso basada en la nube de Microsoft.

**Microsoft Entra ID** proporciona servicios como:

- **Autenticación:** esto incluye la comprobación de la identidad para acceder a aplicaciones y recursos. También incluye funciones como el autoservicio de restablecimiento de contraseña, la autenticación multifactor, una lista personalizada de contraseñas prohibidas y servicios de bloqueo inteligente.
- **Inicio de sesión único:** gracias al inicio de sesión único (SSO), los usuarios tienen que recordar un solo nombre de usuario y una sola contraseña para acceder a varias aplicaciones. Una sola identidad está asociada a un usuario, lo que simplifica el modelo de seguridad. Cuando los usuarios cambian de rol o dejan una organización, las modificaciones de acceso se asocian a esa identidad, lo que reduce considerablemente el esfuerzo necesario para cambiar o deshabilitar cuentas.
- **Administración de aplicaciones:** Con Microsoft Entra ID, puede administrar las aplicaciones en la nube y locales. Características como Application Proxy, las aplicaciones SaaS, el portal Aplicaciones y el inicio de sesión único proporcionan una mejor experiencia de usuario.
- **Administración de dispositivos:** Además de cuentas de usuarios individuales, Microsoft Entra ID admite el registro de dispositivos. El registro permite administrar los dispositivos a través de herramientas como Microsoft Intune. También permite que las directivas de acceso condicional basadas en dispositivos limiten los intentos de acceso a solo aquellos que proceden de dispositivos conocidos, independientemente de la cuenta de usuario solicitante.

Un método para conectar Microsoft Entra ID con su AD local es usar **Microsoft Entra Connect**. **Microsoft Entra Connect** sincroniza las identidades de usuario entre Active Directory local y Microsoft Entra ID. Microsoft Entra Connect sincroniza los cambios entre ambos sistemas de identidades, para que pueda usar características como SSO, la autenticación multifactor y el autoservicio de restablecimiento de contraseña en ambos sistemas.

**Microsoft Entra 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. Al igual que Microsoft Entra ID le permite usar servicios de directorio sin tener que mantener la infraestructura que lo admite, gracias a Microsoft Entra Domain Services, obtiene la ventaja de los servicios de dominio sin necesidad de implementar, administrar y aplicar revisiones a los controladores de dominio (DC) en la nube. Cuando cree un dominio administrado de Microsoft Entra Domain Services, 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".

**Un dominio administrado** está configurado para realizar una sincronización unidireccional desde Microsoft Entra ID a Microsoft Entra Domain Services. Puede crear los recursos directamente en el dominio administrado, pero no se vuelven a sincronizar con Microsoft Entra ID. En un entorno híbrido con un entorno de AD DS local, Microsoft Entra Connect sincroniza la información de identidad con Microsoft Entra ID, que se sincroniza posteriormente con el dominio administrado.

**La autenticación** es el proceso de establecimiento de la identidad de una persona, servicio y dispositivo. Requiere que la persona, el servicio o el dispositivo proporcionen algún tipo de credencial para demostrar quiénes son. La autenticación es como presentar su documento de identidad cuando viaja. **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.

**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. Para que el inicio de sesión único funcione, las distintas aplicaciones y proveedores deben confiar en el autenticador inicial. 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.

**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 MFA ayuda a protegerse frente a las contraseñas en riesgo en situaciones en las que la contraseña se vio comprometida, pero el segundo factor no.

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.

**La autenticación multifactor de Microsoft Entra** es un servicio de Microsoft que proporciona funcionalidades de autenticación multifactor. La autenticación multifactor de Microsoft Entra permite a los usuarios elegir una forma adicional de autenticación durante el inicio de sesión, como una llamada telefónica o una notificación de aplicación móvil.

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 Microsoft Entra ID:

- Windows Hello para empresas
- Aplicación Microsoft Authenticator
- 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). Las claves de seguridad FIDO2 son un método de autenticación sin contraseña basado en estándares que no permite la suplantación de identidad y que puede venir en cualquier factor de forma. Fast Identity Online (FIDO) es un estándar abierto para la autenticación sin contraseña.

**Una identidad externa** es una persona, un dispositivo, un servicio, etc. que está fuera de la organización. Microsoft Entra External ID hace referencia a todas las formas en las que puede interactuar de forma segura con usuarios fuera de su organización. El proveedor de identidades administra la identidad del usuario externo y el usuario administra el acceso a sus aplicaciones con Microsoft Entra ID o Azure AD B2C para mantener protegidos los recursos.

Las siguientes funcionalidades componen External Identities:

- **Colaboración de empresa a empresa (B2B)**: colabore con usuarios externos y permítales usar su identidad preferida para iniciar sesión en las aplicaciones de Microsoft u otras aplicaciones empresariales (aplicaciones SaaS, aplicaciones desarrolladas de forma personalizada, etc.). Los usuarios de colaboración B2B se representan en el directorio, normalmente como usuarios invitados.
- **Conexión directa B2B**: Establezca una confianza mutua y de dos sentidos con otra organización de Microsoft Entra para una colaboración sin problemas. 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. Los usuarios de conexión directa B2B no se representan en el directorio, pero son visibles desde el canal compartido de Teams y se pueden supervisar en Teams informes del centro de administración.
- **Empresa a cliente de Microsoft Azure Active Directory (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.

**El acceso condicional** es una herramienta que usa Microsoft Entra ID para permitir (o denegar) el acceso a los recursos en función de señales de identidad. Estas señales incluyen quién es el usuario, dónde se encuentra y desde qué dispositivo solicita el acceso.

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.

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.

**El principio de privilegios mínimos** indica que solo debe conceder acceso al nivel necesario para completar una tarea. 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.

RBAC de Azure se aplica a cualquier acción que se inicie en un recurso de Azure que pasa por Azure Resource Manager. **Resource Manager** es un servicio de administración que proporciona una forma de organizar y proteger nuestros recursos en la nube.

**Confianza cero** es un modelo de seguridad que supone el peor de los escenarios posibles y protege los recursos con esa expectativa. Confianza cero presupone que hay una vulneración y comprueba todas las solicitudes como si provenieran de una red no controlada. 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.

El objetivo de **la defensa en profundidad** es proteger la información y evitar que personas no autorizadas a acceder puedan sustraerla. Una estrategia de defensa en profundidad usa una serie de mecanismos para ralentizar el avance de un ataque dirigido a adquirir acceso no autorizado a los datos.

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.

**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.

**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.

**Capa de red** en esta capa, el enfoque está en limitar la conectividad de la red en todos los recursos para permitir solo la necesaria. Al limitar esta comunicación, se reduce el riesgo de que se propaguen los ataques a otros sistemas de la red.

En esta capa, es importante que realice lo siguiente:

- 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.

**Capa de proceso,** El software malintencionado, los sistemas sin revisiones aplicadas y los sistemas protegidos inadecuadamente abren el entorno a los ataques. El enfoque en esta capa es asegurarse de que sus recursos de proceso estén seguros y de que cuenta con los controles adecuados para minimizar los problemas de seguridad.

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.

**Capa de aplicación,** La integración de la seguridad en el ciclo de vida de desarrollo de aplicaciones ayuda a reducir el número de vulnerabilidades en el código. Todos los equipos de desarrollo deberían asegurarse de que sus aplicaciones son seguras de forma predeterminada.

En esta capa, es importante que realice lo siguiente:

- 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.

**Capa de datos,** Los que almacenan y controlan el acceso a los datos son responsables de asegurarse de que están protegidos correctamente. A menudo, los requisitos legales dictan los controles y procesos que deben cumplirse para garantizar la confidencialidad, la integridad y la disponibilidad de los datos.

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.

**Microsoft Defender for Cloud** es una herramienta de supervisión para la administración de la posición de seguridad y la protección contra amenazas. Supervisa los entornos en la nube, locales, híbridos y multi nube para ofrecer instrucciones y notificaciones destinadas a reforzar la posición de seguridad. Dado que Defender for Cloud es un servicio nativo de Azure, muchos servicios de Azure se supervisan y protegen sin necesidad de ninguna implementación. Pero si también tiene un centro de datos local o también está funcionando en otro entorno en la nube, es posible que la supervisión de los servicios de Azure no le proporcione una imagen completa de su situación de seguridad.

**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.

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

**Cloud Adoption Framework** para Azure es una colección de documentación, guía técnica, procedimientos recomendados y herramientas que ayudan a alinear las estrategias empresarial, de preparación organizacional y tecnológica. Esta alineación permite un recorrido a la nube claro y procesable, que ofrece rápidamente los resultados comerciales deseados.

Cloud Adoption Framework ayuda a los clientes a atravesar un recorrido simplificado hacia la nube en tres grandes fases:

- Planear
- Ready
- Adoptar

**Cloud Adoption Framework** contiene información detallada para cubrir un recorrido de adopción de la nube de principio a fin:

- Comienza con la definición de la estrategia empresarial, que debe alinearse con los proyectos de tecnología procesables que ofrecen los resultados de negocio deseados.
- A continuación, se describe el modo en que la organización debe:
  - Preparar a su gente técnicamente.
  - Ajustar los procesos para impulsar los cambios tecnológicos y empresariales.
  - Habilitar los resultados empresariales a través de la implementación del plan de tecnología definido.
- Por último, cubre las operaciones en la nube, como gobernanza, recursos, y la administración de personas y de cambios.

Las organizaciones adoptan la nube para ayudar a impulsar la transformación empresarial, como los procesos y la mejora de productos, el crecimiento del mercado y el aumento de la rentabilidad. Las organizaciones buscan distintos desencadenadores para adoptar nuevas tecnologías, como Azure. Algunos desencadenadores impulsan a las organizaciones para migrar las aplicaciones actuales. Otros desencadenadores exigen la creación de nuevas funcionalidades, productos y experiencias.

Entre algunos desencadenadores comunes de migración e innovación se incluyen:

- Preparación para nuevas funcionalidades técnicas
- Aumento de la escala para satisfacer las demandas geográficas o de mercado
- Ahorros en costos
- Reducción de la complejidad técnica o de proveedores
- Optimización de las operaciones internas
- Mayor agilidad empresarial
- Mejoras en las experiencias o la involucración de los clientes
- Transformación de productos o servicios
- Irrupción de nuevos productos o servicios en el mercado

Al definir la **estrategia empresarial** en la nube, debe tener en cuenta el impacto empresarial, el tiempo de respuesta, el alcance global, el rendimiento, etc. Estas son las áreas clave en las que se debe centrar:

- **Establecer resultados empresariales claros:** Impulse la transparencia y el compromiso del recorrido en toda la organización.
- **Definir la justificación empresarial:** Identifique las oportunidades de valor empresarial para seleccionar la tecnología correcta.

La implementación de la primera aplicación es clave para aprender y probar con confianza, a medida que inicia su recorrido de adopción de la nube. Use un enfoque doble para seleccionarlo:

- **Criterios comerciales:** Identifique una aplicación actualmente en funcionamiento en la que el propietario tenga una motivación fuerte para moverla a la nube.
- **Criterios técnicos:** Seleccione una aplicación que tenga dependencias mínimas y que se pueda mover como un pequeño grupo de recursos.

Los recorridos de adopción de la nube más exitosos comienzan con una idea de resultado empresarial, respaldada por el razonamiento y el soporte financieros. Un resultado empresarial es conciso, perceptible y está definido, o es un cambio en el rendimiento empresarial capturado por una medida específica.

Estas son algunas herramientas que le ayudarán en la planificación financiera:

- **Calculadora del costo total de propiedad (TCO) de Azure:** use la calculadora de TCO para calcular el ahorro de costos que puede obtener al migrar las cargas de trabajo de aplicación a Azure.
- **Calculadora de precios de Azure:** calcule la factura mensual esperada con la calculadora de precios.
- **Microsoft Cost Management + Billing:** use y administre los recursos de Azure y otros recursos de la nube mediante una solución de administración de costos de varias nubes.

Desarrollar una justificación comercial clara para la adopción de la nube, con costos y rendimientos pertinentes y tangibles puede ser un proceso complejo. En primer lugar, revise algunas áreas comunes del valor empresarial de la informática en la nube para ayudar a justificar el recorrido de adopción de la nube:

- **Costo:** elimina los gastos de capital.
- **Escala:** capacidad de escalar elásticamente y ofrecer la cantidad adecuada de recursos de TI.
- **Productividad:** elimina la necesidad de muchas tareas de administración de TI.
- **Confiabilidad:** facilita la carga de la copia de seguridad de datos, la recuperación ante desastres y la continuidad empresarial.

**Entre las motivaciones para la adopción de la nube se incluyen:**

- Desencadenadores de la migración, como el ahorro de costos y la optimización de las operaciones.
- Desencadenadores de la innovación, como el escalado para satisfacer las demandas geográficas o de mercado.
- Cloud Adoption Framework para Azure permite un recorrido a la nube procesable, que ofrece rápidamente los resultados comerciales deseados.
- **Las áreas clave en las que centrarse al desarrollar la estrategia de negocio en la nube son:**
  - Definir su justificación comercial mediante la identificación de las oportunidades de valor empresarial.
  - Establecer resultados empresariales claros para impulsar la transparencia y la involucración.
- **Microsoft ofrece herramientas que le ayudarán en la planificación financiera:**
  - Calculadora del costo total de propiedad de Azure
  - Calculadora de precios de Azure
  - Microsoft Cost Management + Billing
- Su primer proyecto de adopción debe estar en línea con sus motivaciones para la adopción.

La forma en que la nube puede anticipar su estrategia de negocios depende de su situación. La nube ofrece ventajas tecnológicas fundamentales que pueden servir de ayuda en la ejecución de varias estrategias de negocios. El uso de enfoques basados en la nube puede mejorar la agilidad empresarial, reducir los costos, acelerar el tiempo de comercialización, e incluso permitir a las empresas expandirse rápidamente a nuevos mercados.

En esta fase, se centrará en dos acciones principales:

- **Racionalizar el patrimonio digital:** comprenda el patrimonio digital actual de la organización para maximizar el retorno y minimizar los riesgos mediante la ejecución de una evaluación de cargas de trabajo.
- **Crear el plan de adopción de la nube:** Desarrolle un plan en el que las cargas de trabajo priorizadas se definen y se alinean con los resultados empresariales.

**Un patrimonio digital** es la colección de recursos de TI que alimenta los procesos de negocio y las operaciones complementarias.

Hay cinco opciones para la rationalización de la nube, que a veces se denominan las **cinco R**:



## Rehospedaje

El rehospedaje, también conocido como migración lift-and-shift, cambia la ubicación de un recurso de estado actual al proveedor de nube elegido, con un cambio mínimo en la arquitectura general.

- Reducir los gastos de capital:
- Liberar espacio en el centro de datos:
- Consiga una rápida rentabilidad de la inversión en la nube.



## Refactorización

Refactorizar también hace referencia al proceso de desarrollo de aplicaciones de refactorizar el código para permitir que una aplicación satisfaga nuevas oportunidades de negocio.

- Experimentar actualizaciones más rápidas y más breves.
- Beneficiarse de la portabilidad del código.
- Lograr una mayor eficacia en la nube en las áreas de recursos, velocidad y costo.



## Rediseño arquitectónico

Cuando las aplicaciones antiguas no sean compatibles con la nube, es posible que tengan que rediseñarse para generar las eficiencias de costos y operativas en la nube.

- Aumentar la escala y la agilidad de las aplicaciones.
- Adoptar nuevas funcionalidades de nube más fácilmente.
- Usar una combinación de pilas tecnológicas.



## Recompilación/renovación

Las aplicaciones locales no compatibles, mal alineadas o desactualizadas podrían resultar demasiado caras para seguir adelante. Una nueva base de código con un diseño nativo de nube puede ser la ruta de acceso más adecuada y eficaz.

- Acelerar la innovación.
- Compilar aplicaciones con mayor rapidez.
- Reducir los costos operativos.



## Reemplazo

A veces, el mejor enfoque es reemplazar la aplicación actual por una aplicación hospedada que cumpla toda la funcionalidad requerida en la nube.

- Estandarizar en función de los procedimientos recomendados del sector.
- Acelerar la adopción de enfoques basados en procesos de negocio.
- Reasignar las inversiones en el desarrollo de aplicaciones que crean diferenciación o ventajas competitivas.

A medida que desarrolle un modelo de justificación comercial para el recorrido de su organización hacia la nube, identifique los resultados empresariales que se puedan asignar a las funcionalidades de la nube y a las estrategias de negocio específicas para alcanzar el estado deseado de transformación. Los pasos clave para crear este plan son los siguientes:

- Examine los resultados empresariales de ejemplo.
- Identifique las métricas de aprendizaje que mejor representarían el progreso hacia los resultados empresariales identificados.
- Establezca un modelo financiero que se alinea con los resultados y la métrica de aprendizaje.

La adopción de la nube es un cambio estratégico que requiere la participación de los responsables de la toma de decisiones empresariales y de los usuarios finales. Ahora, se verá cómo preparar a la organización para este recorrido:

- **Definir aptitudes y apoyar la preparación:** cree e implemente un plan de preparación de aptitudes para lo siguiente:
  - Solucionar las brechas actuales.
  - Asegurar que el personal de TI y comercial esté preparado para el cambio y las nuevas tecnologías.
  - Definir las necesidades de soporte técnico.
- **Crear la zona de aterrizaje:** configure un destino de migración en la nube para controlar las aplicaciones con prioridad.

El término **zona de aterrizaje** se usa para describir un entorno aprovisionado y preparado para hospedar cargas de trabajo en un entorno de nube, como Azure. Una zona de aterrizaje plenamente funcional es el resultado final de cualquier iteración de la metodología de Cloud Adoption Framework para Azure.

**La migración a la nube** es el proceso de mover los recursos digitales existentes a una plataforma de nube. Los recursos existentes se replican en la nube con modificaciones mínimas. Después de que una aplicación o carga de trabajo se vuelvan operativas en la nube, los usuarios pasan de la solución existente a la solución de nube. La estrategia y

las herramientas que usa para migrar una aplicación en Azure dependerán considerablemente de sus motivaciones empresariales, estrategias tecnológicas y escalas de tiempo.

**Preparación para la migración:** establecer un trabajo pendiente de migración aproximado, en función del estado actual y los resultados deseados.

- **Resultados empresariales:** Los objetivos empresariales clave que impulsan esta migración. Se definen en la fase Planificación.
- **Estimación del patrimonio digital:** Una estimación aproximada del número y la condición de cargas de trabajo que se van a migrar. Se define en la fase Planificación.
- **Roles y responsabilidades:** Una definición clara de la estructura del equipo, la separación de responsabilidades y los requisitos de acceso. Se definen en la fase Preparación.
- **Requisitos de administración de cambios:** La cadencia, los procesos y la documentación necesarios para revisar y aprobar los cambios. Se definen en la fase Preparación.

**El proceso de adopción de la nube** es un recorrido, no un destino. En el camino, hay hitos claros y ventajas empresariales tangibles. El estado final de la adopción de la nube es desconocido cuando una organización comienza el recorrido. A medida que su organización mueve o implementa nuevas aplicaciones en la nube, este estado final empieza a tomar forma. Es importante tener en cuenta los siguientes aspectos de la administración y el funcionamiento de una plataforma en la nube:

- **Defina soluciones de gobernanza para el entorno de nube** que satisfagan las necesidades empresariales de la organización, proporcionen agilidad y controlen los riesgos.
- **Administre el entorno de nube en función de las soluciones de gobernanza** para que pueda evolucionar, crecer y adaptarse a las cambiantes necesidades empresariales de la organización.

**La gobernanza de la nube** crea barreras de seguridad que mantienen a la organización en una ruta segura a lo largo del recorrido. El modelo de gobernanza de Cloud Adoption Framework para Azure identifica las principales áreas de importancia. Cada área se relaciona con diferentes tipos de riesgos que la organización debe resolver al adoptar más servicios en la nube.

**La gobernanza incremental** se basa en un pequeño conjunto de directivas corporativas, procesos y herramientas para establecer una base para la adopción y la gobernanza. Esta base se denomina *producto viable mínimo (MVP)*. Un MVP permite al equipo de gobernanza incorporar con rapidez la gobernanza en las implementaciones a lo largo del ciclo de vida de la adopción.

Las **operaciones en la nube** crean un modelo de madurez que ayuda al equipo a cumplir con los compromisos de la empresa.

## **Las cinco disciplinas de gobernanza de la nube son:**

Administración de costos  
Línea de base de seguridad  
Coherencia de recursos  
Línea de base de identidad  
Aceleración de la implementación.

El papel de **un arquitecto de soluciones** no es solo ofrecer valor empresarial por medio de los requisitos funcionales de la aplicación. También consiste en garantizar que la solución se diseñe de maneras escalables, resistentes, eficientes y seguras.

**La arquitectura de un sistema** debe equilibrar y alinear los requisitos empresariales con las capacidades técnicas necesarias para ejecutar esos requisitos. **La arquitectura final** es un equilibrio de riesgo, costo y capacidad en todo el sistema y sus componentes.

**La arquitectura** es la base del diseño de la aplicación. Con el Marco de arquitectura de Azure puede estar seguro de que la aplicación es capaz de satisfacer de forma sostenible las necesidades de los clientes, tanto ahora como en el futuro.

**El Marco de arquitectura de Azure** es un conjunto de doctrinas que orientan a la hora de compilar soluciones de alta calidad en Azure. Aunque no hay un enfoque genérico para diseñar una arquitectura, hay algunos conceptos universales que se aplican con independencia de la arquitectura, la tecnología o el proveedor de nube.

El Marco de arquitectura de Azure consta de cinco pilares:

- Optimización de costos
- Excelencia operativa
- Eficiencia del rendimiento
- Confiabilidad
- Seguridad

El mayor temor de un arquitecto es que la arquitectura quede fuera de servicio y no haya forma de recuperarla. Un entorno en la nube satisfactorio está diseñado de manera que se anticipa a los errores en todos los niveles. Parte de la anticipación a los errores consiste en diseñar un sistema que se pueda recuperar tras un error en el plazo de tiempo requerido por las partes interesadas y los clientes.

Los datos son el elemento más valioso de la superficie técnica de la organización. En este pilar, la prioridad es proteger el acceso a la arquitectura mediante la autenticación y proteger la aplicación y los datos frente a vulnerabilidades de la red. La integridad de los datos también debe protegerse con herramientas como el cifrado.

Además de cada uno de estos pilares, hay algunos principios de diseño sistemáticos que se deben tener en cuenta en la arquitectura.

- **Permitir la evolución de la arquitectura:** ninguna arquitectura es estática. Permita la evolución de la arquitectura mediante el aprovechamiento de los nuevos servicios, herramientas y tecnologías a medida que estén disponibles.
- **Usar los datos para tomar decisiones:** recopile datos, analícelos y úselos para tomar decisiones sobre la arquitectura. Desde los datos de costos hasta el rendimiento, pasando por la carga de usuarios, el uso de datos puede guiarle para tomar las decisiones correctas en su entorno.
- **Formar y habilitar:** la tecnología en la nube evoluciona rápidamente. Forme a los equipos de desarrollo, operaciones y negocios para ayudarlos a tomar las decisiones adecuadas y compile soluciones para solucionar problemas empresariales. Documente y comparta la configuración, las decisiones y los procedimientos recomendados dentro de la organización.
- **Automatizar:** la automatización de actividades manuales reduce los costos operativos, minimiza los errores cometidos en los pasos manuales y proporciona coherencia entre entornos.

El paso a la nube presenta un modelo de **responsabilidad compartida**. En este modelo, el proveedor de nube administra determinados aspectos de la aplicación y deja al usuario la responsabilidad restante. En un entorno local, el usuario es responsable de todo. A medida que pasa a una infraestructura como servicio (IaaS), luego a plataforma como servicio (PaaS) y a software como servicio (SaaS), el proveedor de nube asume más parte de esta responsabilidad. Esta responsabilidad compartida juega un papel en las decisiones de arquitectura, ya que estas pueden tener implicaciones en los costos, la seguridad y las capacidades técnicas y operativas de la aplicación.

Al compilar una arquitectura de Azure, hay que tener en cuenta muchas consideraciones. Se recomienda que la arquitectura sea segura, escalable, disponible y recuperable. Para hacerlo posible, tiene que tomar decisiones basadas en el costo, las prioridades de la organización y el riesgo.

**La optimización de costos** consiste en garantizar que el dinero que invierte la organización se aprovecha al máximo. Los servicios en la nube proporcionan la informática como una utilidad. Las tecnologías en la nube se proporcionan bajo un modelo de servicio que se usa a petición. Las ofertas de servicio a petición llevan a un cambio fundamental que afecta directamente al planeamiento, la contabilidad y la organización.

Cuando una organización decide poseer infraestructura, compra equipamiento que se incluye en el balance contable como activos. Dado que se ha realizado una inversión de capital, los contables clasifican esta transacción como **gasto de capital (CapEx)**. Con el tiempo, a fin de contabilizar la duración útil limitada de los activos, estos se deprecian o se amortizan.

Los servicios en la nube, por otro lado, se clasifican como **gastos operativos (OpEx)**, debido a su modelo de consumo. Conforme a este esquema, no hay ningún activo que amortizar, sino que los gastos de explotación tienen un impacto directo en el beneficio neto, la base imponible y los gastos asociados en el balance contable.

**El aprovisionamiento de servicios** optimizado para el costo desde el principio puede reducir el trabajo en el futuro. Por ejemplo, debe asegurarse de que está seleccionando el nivel de servicio adecuado para la carga de trabajo y aprovechar los servicios que permiten ajustar el nivel de servicio. También debe usar los descuentos que haya disponibles, como las instancias reservadas y las ofertas de tipo "traiga su propia licencia".

Siempre que sea posible, se recomienda migrar de servicios IaaS a PaaS. Los servicios PaaS normalmente cuestan menos que los IaaS y reducen los costos operativos.

Con los servicios PaaS, no tiene que preocuparse de la revisión ni el mantenimiento de las máquinas virtuales, ya que normalmente el proveedor de nube se encarga de esas tareas.

**La eficacia** se centra en identificar y eliminar los gastos innecesarios dentro del entorno. La nube es un servicio de pago por uso, y los gastos que se pueden evitar normalmente son el resultado de aprovisionar más capacidad de la que exige la demanda. Los costos operativos también pueden contribuir a unos costos innecesarios o ineficaces.

El desperdicio puede manifestarse de varias maneras. Veamos algunos ejemplos:

- Una máquina virtual que siempre está inactiva un 90 por ciento.
- Pagar por una licencia incluida en una máquina virtual cuando ya se tiene una.
- Conservar datos a los que se accede pocas veces en un medio de almacenamiento optimizado para el acceso frecuente.
- Repetir manualmente la compilación de un entorno que no es de producción.

**La excelencia operativa** consiste en asegurarse de tener visibilidad completa sobre cómo se ejecuta la aplicación y de garantizar la mejor experiencia para los usuarios. La excelencia operativa incluye lograr que los procedimientos de desarrollo y lanzamiento sean más ágiles, lo que permite que el negocio se ajuste rápidamente a los cambios.

**Una arquitectura moderna** le permite automatizar las implementaciones gracias a la infraestructura como código, la automatización de las pruebas de las aplicaciones y la creación de nuevos entornos según sea necesario.

**La supervisión** le ayuda a identificar áreas de despilfarro, a solucionar problemas y a optimizar el rendimiento de la aplicación. Un enfoque multicapa es esencial. La recopilación de puntos de datos de los componentes en cada capa ayuda a alertar si hay valores fuera de los límites aceptables, así como a realizar un seguimiento del gasto a lo largo del tiempo.

**Un plan de pruebas sólido** puede destapar problemas de las implementaciones de infraestructura que pueden afectar a la experiencia del usuario; las pruebas ayudan a proporcionar una gran experiencia a los usuarios.

**La eficacia del rendimiento** consiste en ajustar los recursos disponibles para una aplicación a la demanda que recibe. La eficacia del rendimiento incluye escalar los recursos, identificar y optimizar los posibles cuellos de botella, y optimizar el código de la aplicación para el máximo rendimiento.

Los recursos de proceso pueden escalarse en dos direcciones:

- El **escalado vertical** es la incorporación de más recursos a una sola instancia. También se conoce como *escalado vertical*.



- El **escalado horizontal** es la incorporación de más instancias. También se conoce como *escalado horizontal*.



El **escalado vertical** consiste en agregar más recursos, como CPU o memoria, a una sola instancia. Esta instancia puede ser una máquina virtual o un servicio PaaS.

El **escalado horizontal** consiste en agregar más instancias a un servicio. Pueden ser máquinas virtuales o servicios PaaS. En lugar de agregar más capacidad al aumentar la eficacia de una sola instancia, se agrega capacidad mediante el aumento del número total de instancias.

El **escalado automático** es el proceso de asignación dinámica de recursos para satisfacer los requisitos de rendimiento. A medida que aumenta el volumen de trabajo, una aplicación puede necesitar más recursos para mantener los niveles de rendimiento deseados y cumplir los Acuerdos de Nivel de Servicio (SLA). El escalado automático aprovecha la elasticidad de los entornos hospedados en la nube y alivia la sobrecarga de administración.

Use el **almacenamiento en caché** en la arquitectura para ayudar a mejorar el rendimiento. El almacenamiento en caché es un mecanismo para almacenar datos o recursos que se usan con frecuencia (páginas web, imágenes) a fin de agilizar la recuperación. El almacenamiento en caché se puede usar en diferentes capas de la aplicación.

El **diseño orientado a la confiabilidad incluye** el mantenimiento del tiempo de actividad durante incidentes a pequeña escala y situaciones temporales como interrupciones de red parciales. Puede asegurarse de que la aplicación controla errores localizados mediante la integración de la alta disponibilidad en cada componente. El diseño de arquitectura orientado a la confiabilidad garantiza que la aplicación pueda cumplir los compromisos contraídos con los clientes. Quiere garantizar que los sistemas están *disponibles* para los usuarios finales y se pueden *recuperar* de cualquier posible error.

Los ejemplos de **componentes de diseño de alta disponibilidad** incluyen la agrupación en clústeres y el equilibrio de carga:

- La agrupación en clústeres reemplaza una sola máquina virtual por un conjunto de máquinas virtuales coordinadas. Si se produce un error en una máquina virtual o esta deja de ser accesible, los servicios pueden comutar por error a otra máquina virtual que pueda atender las solicitudes.
- El equilibrio de carga propaga solicitudes entre muchas instancias de un servicio, detecta las instancias con error y evita que las solicitudes se enruten hacia ellas.

En el caso de la capacidad de recuperación, debe realizar un análisis que examine las posibles pérdidas de datos y los principales escenarios de tiempos de inactividad. El análisis debe incluir un examen de las estrategias de recuperación y la relación costo-beneficio de cada una de ellas. Este ejercicio proporciona información importante sobre las prioridades de la organización y ayuda a aclarar el papel que desempeña la aplicación. Los resultados del análisis deben incluir estos valores de duración de la aplicación:

- **Objetivo de punto de recuperación (RPO):** duración máxima de pérdida de datos aceptable. El RPO se mide en unidades de tiempo, no en volumen. Por ejemplo, "30 minutos de datos", "cuatro horas de datos", etc. El RPO trata de la limitación y la recuperación de las *pérdidas* de datos, no del *robo* de datos.
- **Objetivo de tiempo de recuperación (RTO):** duración máxima del tiempo de inactividad aceptable, donde "tiempo de inactividad" se define según sus propias especificaciones. Por ejemplo, si la duración del tiempo de inactividad aceptable es de ocho horas en caso de desastre, entonces el RTO es de ocho horas.

**La seguridad** consiste en última instancia en proteger los datos que la organización usa, almacena y transmite. Los datos que la organización almacena o controla son el núcleo de los recursos que se deben proteger. Estos datos pueden consistir en información confidencial sobre los clientes, información financiera sobre la organización o datos de línea de negocio críticos relativos a la organización. Es igualmente importante proteger la infraestructura en la que residen los datos, junto con las identidades que se usan para acceder a ellos.

El uso de un enfoque multicapa para proteger el entorno aumentará su posición de seguridad. Normalmente se conoce como *defensa en profundidad* y las capas se desglosan como sigue:

- Datos
- Aplicaciones
- Máquina virtual/proceso
- Redes
- Perímetro
- Directivas y acceso
- Seguridad física

- **Capa de datos:** la exposición de una clave de cifrado o el empleo de un cifrado débil pueden hacer que los datos sean vulnerables en caso de acceso no autorizado.
- **Capa de aplicación:** La ejecución y la inserción de código malintencionado son las marcas distintivas de los ataques de capa de aplicación. Algunos ataques comunes son los de inyección de código SQL y de scripts de sitios (XSS).
- **Capa de máquina virtual o proceso:** el malware es un método habitual de ataque a un entorno e implica ejecutar código malintencionado para poner en peligro un sistema. Una vez que el malware está presente en un sistema, pueden producirse más ataques que den lugar a la exposición de credenciales y desplazamientos laterales por todo el entorno.
- **Nivel de red:** aprovechar los puertos abiertos innecesarios a Internet es un método habitual de ataque. Los puertos abiertos también pueden incluir dejar abiertos los protocolos SSH o RDP a las máquinas virtuales. Si estos protocolos están abiertos, pueden permitir ataques por fuerza bruta a los sistemas cuando los atacantes intentan acceder.
- **Capa perimetral:** en esta capa suelen producirse ataques por denegación de servicio (DoS). Estos ataques intentan sobrecargar los recursos de red y obligarlos a desconectarse o hacer que no sean capaces de responder a solicitudes legítimas.
- **Capa de directivas y acceso:** aquí es donde se produce la autenticación de la aplicación. Esta capa puede incluir protocolos de autenticación modernos, como OpenID Connect u OAuth, o autenticación basada en Kerberos, como Active Directory. La exposición de credenciales es un riesgo en esta capa y es importante limitar los permisos de las identidades. También se recomienda establecer supervisión para detectar posibles cuentas en peligro, por ejemplo, inicios de sesión procedentes de ubicaciones inusuales.
- **Capa física:** en esta capa pueden producirse accesos no autorizados a las instalaciones al colarse por puertas abiertas o robar distintivos de seguridad.

# AZ-305: Diseño de soluciones de identidad, gobernanza y supervisión

**Las suscripciones de Azure** son contenedores lógicos que sirven como unidades de administración y escala, además de límites de facturación. Se pueden aplicar límites y cuotas; además, cada organización puede usar suscripciones a fin de administrar los costos y los recursos por grupo. Una suscripción le proporciona un contenedor lógico para crear productos y servicios de Azure y pagar por ellos.

- **Trate las suscripciones como una unidad de administración democratizada.** Alinee sus suscripciones para satisfacer las necesidades y prioridades empresariales específicas de Tailwind Traders.
- **Agrupe las suscripciones en grupos de administración.** Agrupe las suscripciones que tienen el mismo conjunto de directivas y asignaciones de roles de Azure para que hereden esta configuración del mismo grupo de administración. En el caso de Tailwind Traders, las suscripciones Oeste y Este pueden heredar la configuración de directiva del grupo administración Ventas.
- **Considere la posibilidad de usar una suscripción de servicios compartidos dedicada.** Use una suscripción de servicios compartidos para garantizar que todos los recursos de red comunes se facturen juntos y se aíslen de otras cargas de trabajo. Entre los ejemplos de suscripciones de servicios compartidos se incluyen Azure ExpressRoute y Virtual WAN.
- **Tenga en cuenta los límites de escala de suscripción.** Las suscripciones sirven como unidad de escalado para cargas de trabajo de componentes. Las cargas de trabajo grandes y especializadas, como la informática de alto rendimiento, IoT y SAP, son más adecuadas para usar suscripciones independientes. Al tener suscripciones independientes para diferentes grupos o tareas de Tailwind Traders, puede evitar los [límites de recursos](#) (por ejemplo, un límite de 50 integraciones de Azure Data Factory).
- **Considere la posibilidad de utilizar la gestión administrativa.** Las suscripciones proporcionan un límite de administración que permite una separación clara de las preocupaciones. ¿Necesitará cada suscripción de Tailwind Traders un administrador independiente o puede combinar suscripciones? El grupo de administración Corporativo podría tener una sola suscripción para los departamentos de RR. HH. y Legal.
- **Tenga en cuenta cómo va a asignar las directivas de Azure.** Tanto los grupos de administración como las suscripciones funcionan como límite para la asignación de directivas de Azure. Las cargas de trabajo como las del sector de tarjetas de pago (PCI) normalmente requieren directivas adicionales para lograr el cumplimiento. En lugar de usar un grupo de administración para agrupar las cargas de trabajo que requieren el cumplimiento del PCI, puede obtener el mismo aislamiento con una suscripción. Estos tipos de decisiones garantizan que no tiene demasiados

grupos de administración de Tailwind Traders con solo unas pocas suscripciones.

- **Tenga en cuenta las topologías de red.** Las redes virtuales no se pueden compartir entre suscripciones. Los recursos se pueden conectar entre suscripciones con tecnologías distintas, como el emparejamiento de red virtual o redes privadas virtuales (VPN). Tenga en cuenta qué cargas de trabajo de Tailwind Traders deben comunicarse entre sí cuando decida si se requiere una nueva suscripción.
- **Considere la posibilidad de hacer que los propietarios de suscripciones conozcan sus roles y responsabilidades.** Realice una revisión trimestral o semestral del acceso mediante Microsoft Entra Privileged Identity Management. Las revisiones de acceso garantizan que los privilegios no proliferen a medida que los usuarios se mueven dentro de la organización del cliente Tailwind Traders.

Los **grupos de recursos** son contenedores lógicos en los que se implementan y administran los recursos de Azure. Estos recursos pueden incluir aplicaciones web, bases de datos y cuentas de almacenamiento. Puede usar grupos de recursos para:

- Colocar recursos de uso, tipo o ubicación similares en grupos lógicos.
- Organizar los recursos por ciclo de vida para que todos los recursos se puedan crear o eliminar al mismo tiempo.
- Aplicar permisos de rol a un grupo de recursos o dar acceso a un grupo para administrar un grupo de recursos.
- Usar bloqueos de recursos a fin de proteger los recursos individuales frente a eliminaciones o cambios.

#### **Características de los grupos de recursos:**

- Los grupos de recursos tienen asignada su propia ubicación (región). Esta región es donde se almacenan los metadatos.
- Si la región del grupo de recursos no está disponible temporalmente, no puede actualizar los recursos del grupo de recursos porque los metadatos no están disponibles. Los recursos de otras regiones siguen funcionando según lo previsto, pero no puede actualizarlos.
- Los recursos del grupo de recursos pueden estar en regiones diferentes.
- Un recurso puede conectarse a los recursos de otros grupos de recursos. Puede tener una aplicación web que se conecta a una base de datos de un grupo de recursos diferente.
- Los recursos se pueden mover entre grupos de recursos con algunas excepciones.
- Puede agregar un recurso a un grupo de recursos o quitarlo en cualquier momento.
- Los grupos de recursos no se pueden anidar.
- Cada recurso debe estar en un grupo de recursos único, y solo en uno.
- No se puede cambiar el nombre de los grupos de recursos.

**Las etiquetas de recursos** son otra forma de organizar los recursos. Las etiquetas proporcionan información extra, o metadatos, sobre los recursos.

### Características de las etiquetas de recursos:

- Una etiqueta de recurso se compone de par nombre-valor. Por ejemplo, env = production O env = dev, test.
- Puede asignar una o varias etiquetas a cada recurso, grupo de recursos o suscripción de Azure.
- Las etiquetas de recursos se pueden agregar, modificar y eliminar. Estas acciones se pueden realizar con PowerShell, la CLI de Azure, Azure Resource Manager (ARM), la API de REST o Azure Portal.
- Las etiquetas se pueden aplicar a un grupo de recursos. Sin embargo, los recursos del grupo no heredan las etiquetas aplicadas al grupo de recursos.

Alignment	Descripción	Escenarios de ejemplo
Alineado con TI	La opción de etiquetado alineado con TI es útil para realizar el seguimiento de los criterios de carga de trabajo, aplicación, funcionamiento o entorno. Esta opción puede reducir la complejidad de la supervisión de los recursos. El etiquetado alineado con TI simplifica la toma de decisiones de administración en función de los requisitos operativos.	Las impresoras de Tailwind Traders están ocupadas el 80 % del tiempo. Tenemos cinco impresoras a color de alta velocidad y debemos comprar más. Use el etiquetado alineado con TI para admitir la carga de trabajo y el funcionamiento de los recursos de la impresora.
Alineado con la empresa	La opción de etiquetado alineado con la empresa ayuda a centrarse en la contabilidad, la propiedad empresarial, la responsabilidad de los costos y la importancia empresarial. Esta opción proporciona una mejor contabilidad de los costos y el valor de los recursos de TI para el negocio global. Puede usar el etiquetado alineado con la empresa para cambiar el foco del costo operativo de un recurso al valor empresarial de un recurso.	La documentación promocional del departamento de marketing de Tailwind Traders ha aumentado los ingresos de ventas en un 10 %. Debemos invertir en más funcionalidades de impresión. Use el etiquetado alineado con la empresa para admitir la propiedad, la contabilidad y el costo de los recursos de marketing.

<b>Tipo de etiqueta</b>	<b>Descripción</b>
Funcional	Las etiquetas funcionales clasifican los recursos según su propósito dentro de una carga de trabajo. Esta etiqueta muestra el entorno implementado de un recurso u otros detalles operativos y funcionalidades.
Clasificación	Las etiquetas de clasificación identifican un recurso por la forma en que se usa y las directivas que se le aplican.
Control	Las etiquetas de contabilidad permiten asociar cualquier recurso a grupos concretos de una organización para la facturación.
Asociación	Las etiquetas de asociación proporcionan información sobre las personas (salvo los miembros de TI) que están asociadas a un recurso o que se ven afectadas por el recurso.
Propósito	Las etiquetas de propósito alinean los recursos con las funciones empresariales para dar más soporte a las decisiones de inversión.

**Azure Policy** es un servicio de Azure que permite crear, asignar y administrar directivas para controlar o auditar recursos. Dichas directivas aplican distintas reglas a las configuraciones de los recursos de modo que estas configuraciones sigan cumpliendo con los estándares corporativos.

#### **Características de Azure Policy:**

- Azure Policy permite definir tanto directivas individuales como grupos de directivas relacionadas, denominadas *iniciativas*. Azure Policy incluye muchas definiciones de [iniciativas](#) y [directivas integradas](#).
- Las directivas de Azure se heredan en la jerarquía.
- Puede establecer el ámbito de las directivas de Azure y aplicarlas en varios niveles de la jerarquía de la organización.

- Azure Policy evalúa todos los recursos de Azure y los recursos habilitados para Arc (tipos de recursos específicos hospedados fuera de Azure).
- Azure Policy resalta los recursos que no cumplen con las directivas actuales.
- Use Azure Policy para evitar que se creen recursos no conformes y corregir automáticamente los recursos no conformes.
- Azure Policy se integra con Azure DevOps mediante la aplicación de directivas previas y posteriores a la implementación.

Es importante comprender que Azure Policy y RBAC de Azure son diferentes.

- Puede usar Azure Policy para asegurarse de que el estado del recurso es conforme a las reglas de negocio de la organización. El cumplimiento no depende de quién hizo el cambio ni de quién tiene permiso para realizar cambios. Azure Policy evalúa el estado de un recurso y actúa para asegurarse de que el recurso siga siendo conforme.
- RBAC de Azure se implementa para centrarse en las acciones del usuario en distintos ámbitos. RBAC de Azure administra quién puede acceder a los recursos de Azure, qué se puede hacer con esos recursos y a qué áreas se puede acceder. Si es necesario controlar las acciones, use RBAC de Azure. Si un usuario tiene acceso para realizar una acción, pero el resultado es un recurso no conforme, Azure Policy sigue bloqueando la acción.

**RBAC de Azure** le permite conceder acceso a los recursos de Azure que controla. RBAC de Azure evalúa cada solicitud de acceso y determina si el acceso debe bloquearse, no permitirse o permitirse. RBAC es un modelo de permiso. **Un modelo de permiso** significa que, cuando un usuario tiene asignado un rol específico, RBAC de Azure permite al usuario realizar las acciones asociadas a ese rol. Una asignación de roles podría conceder a un usuario permisos de lectura para un grupo de recursos. Para tener permisos de escritura, el rol tendría que permitir explícitamente el acceso de escritura.

	Azure Policy	Azure RBAC
<b>Descripción</b>	Directivas definidas para asegurarse de que los recursos son conformes a un conjunto de reglas.	Sistema de autorización que proporciona controles de acceso específicos.
<b>Foco principal</b>	Se centra en las propiedades de los recursos.	Se centra en los recursos a los que pueden acceder los usuarios.
<b>Implementación</b>	Especifique un conjunto de reglas.	Asigne roles y ámbitos.
<b>Acceso predeterminado</b>	De manera predeterminada, las reglas de directiva se establecen en <i>permitido</i> .	De manera predeterminada, todo el acceso para todos los usuarios es <i>denegado</i> .

Una **zona de aterrizaje de Azure** proporciona un entorno de infraestructura para hospedar las cargas de trabajo. Las zonas de aterrizaje garantizan la aplicación de los principios fundamentales clave antes de la implementación de los servicios.

### **Características de las zonas de aterrizaje de Azure:**

- Las zonas de aterrizaje se definen mediante grupos de administración y suscripciones diseñados para escalar según las necesidades y prioridades empresariales.
- Las directivas de Azure están asociadas a zonas de aterrizaje para garantizar el cumplimiento continuo con la plataforma de la organización.
- Las zonas de aterrizaje se aprovisionan previamente mediante código.
- Se puede definir un ámbito de zona de aterrizaje para admitir las migraciones y el desarrollo de aplicaciones para escalar a través de la cartera de TI completa de la organización.
- El acelerador de zonas de aterrizaje de Azure se puede implementar en el mismo inquilino de Microsoft Entra para una arquitectura de Azure existente. El acelerador es una implementación basada en Azure Portal.

Para implementar la autenticación y autorización, los arquitectos de Azure diseñan soluciones de **administración de identidades y accesos (IAM)**. Estas soluciones deben funcionar para todos los usuarios, las aplicaciones y los dispositivos. Una solución de IAM sólida debe tener administración unificada de identidades, acceso adaptable seguro, gobernanza de identidad simplificada y una experiencia de usuario sin problemas.

### **Características de una solución de IAM sólida:**

- **Administración unificada de identidades.** Administre todas las identidades y el acceso a todas las aplicaciones en una ubicación central, ya sea en la nube o en el entorno local, a fin de mejorar la visibilidad y el control.
- **Experiencia de usuario sin problemas.** Proporcione una experiencia de inicio de sesión sencilla y rápida para mantener la productividad de los usuarios, reducir el tiempo dedicado a la administración de contraseñas y aumentar la productividad del usuario final.
- **Acceso adaptable seguro.** Proteja el acceso a los recursos y los datos mediante una autenticación segura y directivas de acceso adaptable basadas en riesgos sin poner en peligro la experiencia del usuario.
- **Gobernanza simplificada de identidades.** Controle el acceso a aplicaciones y datos para todos los usuarios y administradores. Gobernanza automatizada de identidades que garantiza que solo los usuarios autorizados tengan acceso.

**Microsoft Entra ID** es la solución de Azure para la administración de identidades y acceso. Microsoft Entra ID es un servicio multi inquilino, basado en la nube, de administración de directorios e identidades. Combina servicios de directorio fundamentales, la administración del acceso a las aplicaciones y la protección de identidades en una única solución. Microsoft Entra ID se puede usar en entornos híbridos o en la nube.

### **Características de Microsoft Entra ID:**

- Puede implementar Microsoft Entra ID como una **solución de identidad solo en la nube** para todas las cuentas de usuario de los empleados de Tailwind Traders.
- La solución de identidad solo en la nube proporciona protección y administración de identidades para las cuentas, incluido el control de acceso basado en rol (RBAC), el acceso condicional y las revisiones de acceso. Estas características se examinarán más adelante en este módulo.
- Microsoft Entra ID también ofrece una **solución de identidad híbrida** para la administración de identidades en entornos híbridos de Tailwind Traders.
- En los entornos híbridos, Microsoft Entra ID extiende Active Directory del entorno local a la nube.
- Con Microsoft Entra Connect o la sincronización en la nube de Microsoft Entra Connect, puede incorporar identidades locales en Microsoft Entra ID. Una vez que las cuentas locales están en Microsoft Entra ID, obtienen las ventajas de una protección de identidades y administración sencilla.

**Microsoft Entra de negocio a negocio (B2B) ( Business to Business)** es una característica de Microsoft Entra ID que permite colaborar de forma segura con asociados externos. Se invita a los usuarios del partner como usuarios invitados. Sigue controlando a qué tienen acceso y durante cuánto tiempo.

**Azure AD B2C ( Business to Consumer)** es un tipo de inquilino de Microsoft Entra que se usa para administrar las identidades de los clientes y su acceso a las aplicaciones. Azure AD B2C requiere un inquilino de Microsoft Entra, pero este inquilino *no* es el mismo que el inquilino de Microsoft Entra para su organización.

- El **inquilino de Microsoft Entra** representa su organización.
- El **inquilino de Azure AD B2C** representa las identidades de las aplicaciones de cliente.

Una vez que el inquilino de Azure AD B2C esté configurado, debe registrar la aplicación. Los flujos de usuario se utilizan para administrar aspectos como inicios de sesión y registros de usuario. El inquilino de Azure AD B2C le permite crear varios tipos de flujos de usuario.

### **Las características del cliente que ofrece Azure AD B2C:**

- Azure AD B2C proporciona autenticación de forma segura a los clientes a través de sus proveedores de identidades preferidos.
- Puede capturar datos de inicio de sesión, preferencias y conversión para los clientes.
- Azure AD B2C almacena atributos personalizados sobre los clientes para que pueda usar la información de las aplicaciones.
- Puede usar el registro de marca y las experiencias de inicio de sesión de la interfaz de usuario personalizadas.
- La opción B2C le permite separar la cuenta de la organización de la cuenta de cliente.

	Microsoft Entra B2B (negocio a negocio)	Azure AD de negocio a cliente (B2C)
<b>Definición del foco</b>	Tailwind Traders quiere colaborar con socios comerciales de organizaciones externas, como proveedores, asociados y proveedores. Admitirá a los usuarios como usuarios invitados en el directorio y podrían o no haber administrado TI.	Tailwind Traders quiere interactuar con los clientes de sus productos. Administrará los usuarios en un directorio o inquilino de Microsoft Entra independiente.
<b>Identificar a los usuarios</b>	Los usuarios representarán una empresa asociada de Tailwind Traders o serán empleados de Tailwind Traders.	Los usuarios serán clientes de Tailwind Traders que se representan a sí mismos.
<b>Administración de perfiles de usuario</b>	Tailwind Traders administrará perfiles de usuario asociados a través de revisiones de acceso, comprobación de correo electrónico o listas de acceso y bloqueados.	Los usuarios del cliente de Tailwind Traders administrarán sus propios perfiles.
<b>Almacenar información de usuario</b>	Administrará usuarios externos en el mismo directorio que los empleados de Tailwind Traders, pero los usuarios externos normalmente se anotarán como usuarios invitados. Los usuarios invitados pueden administrarse del mismo modo que los empleados, pueden agregarse a los mismos grupos, etc.	Administrará usuarios externos en el directorio de Azure AD B2C. Se administran de manera independiente del directorio de asociados y de empleados de Tailwind Traders (si existe).
<b>Habilitación de la detección de usuarios y compatibilidad con la privacidad</b>	Los usuarios asociados de Tailwind Traders serán reconocibles y pueden encontrar a otros usuarios de su organización.	Los usuarios del cliente de Tailwind Traders serán invisibles para otros usuarios. Se aplicará la privacidad y el contenido.
<b>Uso de proveedores de identidades</b>	Los usuarios externos colaborarán mediante cuentas profesionales, cuentas educativas, cualquier dirección de correo electrónico, proveedores de identidades basados en SAML y WS-Fed, Gmail y Facebook.	Usuarios consumidores con cuentas de aplicaciones locales (cualquier dirección de correo electrónico o nombre de usuario), diversas identidades admitidas de redes sociales y usuarios con identidades corporativas o emitidas por una entidad gubernamental mediante la federación del proveedor de identidades basada en SAML o WS-Fed accederán a las aplicaciones.
<b>Personalización de la interfaz de usuario y compatibilidad con la personalización de marca</b>	Espera usar la personalización de marca de interfaz de usuario para el host o la organización que invita (Tailwind Traders).	Quiere que la personalización de marca sea totalmente personalizable por aplicación u organización y no sea específica de Tailwind Traders.

El **Acceso condicional** es una herramienta que usa Microsoft Entra ID para permitir (o denegar) el acceso a los recursos. Cuando un usuario inicia sesión, el acceso condicional examina quién es el usuario, dónde está y desde qué dispositivo solicita acceso. En función de estas señales, el acceso condicional puede permitir el acceso, aplicar la autenticación multifactor (MFA) o denegar el acceso.

## Características del acceso condicional:

- MFA admite un control granular. Puede usar MFA de forma selectiva y requerirlo solo para determinados usuarios.
- Microsoft Entra ID permite usar ubicaciones con nombre con directivas de aplicación para controlar el acceso.
- El acceso al servicio solo se puede restringir a través de aplicaciones cliente aprobadas.
- El acceso a las aplicaciones se puede limitar a los dispositivos administrados que cumplen los estándares de seguridad y cumplimiento.
- Los orígenes que no son de confianza se pueden bloquear, como los orígenes de una ubicación desconocida o inesperada.
- El **modo de solo informe** ayuda a los administradores a evaluar el impacto de las directivas de acceso condicional antes de habilitarlas en su entorno.
- La herramienta **What If** lo ayuda a planear las directivas de acceso condicional y a solucionar problemas relacionados con ellas.

Resultado	Descripción
Solo informe: Correcto	Se cumplieron todas las condiciones de directiva configuradas, los controles de concesión no interactivos requeridos y los controles de sesión. Por ejemplo, una notificación de MFA ya presente en el token cumple un requisito de autenticación multifactor o una directiva de dispositivo compatible se cumple realizando una comprobación de dispositivo en un dispositivo compatible.
Solo informe: Error	Se cumplieron todas las condiciones de directiva configuradas, pero no se cumplieron todos los controles de concesión no interactivos requeridos ni los controles de sesión. Por ejemplo, una directiva se aplica a un usuario donde se configura un control de bloqueo, o un dispositivo produce un error en una directiva de dispositivo compatible.
Solo informe: Se requiere una acción del usuario	Se cumplieron todas las condiciones de directiva configuradas, pero se requiere la acción del usuario para cumplir los controles de concesión requeridos o los controles de sesión. Con el modo de solo informe, no se solicita al usuario que cumpla los controles requeridos. Por ejemplo, no se solicita a los usuarios los desafíos de autenticación multifactor ni las condiciones de uso.
Solo informe: No aplicado	No se cumplieron todas las condiciones de directiva configuradas. Por ejemplo, el usuario se excluye de la directiva o la directiva solo se aplica a determinadas ubicaciones con nombre de confianza.

**Identity Protection** es una herramienta que le permite a las organizaciones realizar tres tareas clave:

- Automatizar la detección y corrección de riesgos basados en la identidad.
- Investigue los riesgos mediante el uso de los datos de Azure Portal.
- Exporte datos de detección de riesgo a otras herramientas.

## Características de Identity Protection:

- Identity Protection proporciona **detecciones de directivas riesgo** que incluyen todas las acciones sospechosas identificadas relacionadas con las cuentas de usuario en el directorio.

- Se evalúan dos directivas de riesgo: **riesgo de usuario** e **riesgo de inicio de sesión**:
- Un **riesgo de usuario** representa la probabilidad de que una identidad o cuenta determinada esté en peligro. Un ejemplo es cuando se filtran las credenciales válidas de un usuario. Los riesgos de usuario se calculan sin conexión, usando orígenes de inteligencia sobre amenazas internos y externos de Microsoft. Estos son algunos riesgos de usuario que se pueden identificar:
  - **Credenciales filtradas:** Microsoft busca credenciales filtradas en la Dark Web, sitios de pegado u otros orígenes. Estas credenciales filtradas se comparan con las credenciales actuales válidas de los usuarios de Microsoft Entra para ver si coinciden.
  - **Inteligencia sobre amenazas de Microsoft Entra:** Este tipo de detección de riesgo indica una actividad de usuario inusual para el usuario en cuestión o que es coherente con patrones de ataque conocidos.
- **Un riesgo de inicio de sesión** representa la probabilidad de que el propietario de la identidad no haya autorizado un inicio de sesión (solicitud de autenticación) determinado. El riesgo de inicio de sesión se puede calcular en tiempo real o sin conexión. Estos son algunos riesgos de inicio de sesión que se pueden identificar:
  - **Dirección IP anónima:** intento de inicio de sesión desde una dirección IP anónima, como un explorador Tor o una VPN anonimizada.
  - **Viaje inusual:** dos inicios de sesión del mismo usuario que se originan en una ubicación geográficamente lejana. Dado el comportamiento anterior, al menos una de las ubicaciones también puede ser atípica para el usuario.
  - **Dirección IP vinculada a malware:** un inicio de sesión desde una dirección IP que está infectada con malware y se sabe que el malware se comunica activamente con un servidor de bots.
  - **Difusión de contraseña:** ataque de difusión de contraseña en el que un actor incorrecto intenta derrotar el bloqueo y la detección al intentar iniciar sesión con nombres de usuario diferentes y la misma contraseña.

**Una revisión de acceso de Microsoft Entra** es una revisión planeada de las necesidades de acceso, los derechos y el historial de acceso de los usuarios.

#### **Características de una revisión de acceso:**

- Las revisiones de acceso mitigan el riesgo mediante la protección, supervisión y auditoría del acceso a los recursos críticos.
- Las revisiones de acceso se usan para garantizar que los usuarios adecuados tengan el acceso correcto a los recursos apropiados.

- Confirme el acceso correcto de los usuarios a las aplicaciones integradas con Microsoft Entra ID para el inicio de sesión único, incluidas las aplicaciones SaaS y las aplicaciones de línea de negocio.
- Comprueba la pertenencia a un grupo que esté sincronizado con Microsoft Entra ID o creado en Microsoft Entra ID o Microsoft 365, incluido Microsoft Teams.
- Compruebe los paquetes de acceso que agrupan recursos (grupos, aplicaciones y sitios) en un único paquete para administrar el acceso.
- Las revisiones de acceso también pueden usarse para roles de Microsoft Entra y de recursos de Azure definidos en Privileged Identity Management (PIM).

Existen tres tipos de revisores:

- **Propietarios de recursos:** los propietarios empresariales de un recurso.
- **Delegados:** un grupo de personas seleccionadas por el administrador de revisiones de acceso.
- **Usuario final:** un usuario que auto atesta su necesidad de acceso continuado.

Componente de revisión de acceso	Implementación
¿Cuáles son los recursos que se van a revisar?	Recursos de Microsoft Dynamics
¿Con qué frecuencia se debe realizar la revisión de acceso?	Una vez al mes
¿Quiénes son los revisores?	Administradores de programas del grupo de negocios de Dynamics
¿Cómo se notificará a los revisores?	24 horas antes del inicio de la revisión, envíe un correo electrónico al alias <a href="mailto:Dynamics-PMs@tailwind-traders.org">Dynamics-PMs@tailwind-traders.org</a> . Incluya un mensaje personalizado animado para proteger la cooperación de los revisores.
¿Cuánto tiempo tarda la revisión en completarse?	Como máximo, 24 horas, que es 48 horas después de que se notifique a los revisores por primera vez.
¿Hay acciones automáticas para estos recursos?	Sí. Las acciones automáticas incluyen: - Quitar el acceso de cualquier cuenta de usuario que no haya tenido ningún inicio de sesión interactivo en un plazo de 90 días. - Quitar usuarios del grupo de seguridad <a href="#">dynamics-access</a> . - Realizar acciones de revisión de acceso para las cuentas de usuario que no se revisen dentro del tiempo especificado para completarse.
¿Hay acciones manuales disponibles para los revisores?	Sí. Los revisores pueden aprobar eliminaciones de cuentas de usuario antes de que se complete la acción automatizada, según sea necesario.
¿Cómo se notificará a los usuarios afectados?	Se enviará un correo electrónico a usuarios internos (miembros) que se quitan, se explicará su eliminación y cómo pueden recuperar el acceso.

**La entidad de seguridad** define la directiva de acceso y los permisos para el usuario (**entidad de seguridad de usuario**) o la aplicación (**entidad de servicio**) en el inquilino de Microsoft Entra. La entidad de seguridad admite características principales como la autenticación de un usuario y una aplicación durante el inicio de sesión o la autorización durante el acceso a los recursos.

Las dos formas en que una aplicación se puede representar en Microsoft Entra ID: como un objeto de aplicación o por una entidad de servicio.

- **Objetos de aplicación:** aunque hay excepciones, un objeto de aplicación se puede considerar *la definición de una aplicación*. Un objeto de aplicación permite al servicio saber cómo emitir tokens a la aplicación en función de la configuración del objeto. El objeto de aplicación solo existirá en su directorio principal, incluso si se trata de una aplicación multi inquilino que admite entidades de servicio en otros directorios.
- **Entidades de servicio:** la entidad de servicio de una aplicación se puede considerar *una instancia de una aplicación*. Las entidades de servicio suelen hacer referencia a un objeto de aplicación. Varias entidades de servicio pueden hacer referencia a un objeto de aplicación entre directorios.

Hay tres tipos de entidades de servicio que puede usar para su organización: **aplicación, identidad administrada y heredada**.

**Aplicación:** una entidad de servicio de aplicación es una representación local o la instancia de aplicación de un objeto de aplicación global en un único inquilino o directorio. Se trata de una instancia concreta creada a partir del objeto de aplicación, que hereda ciertas propiedades del objeto. La entidad se crea en cada inquilino donde se usa la aplicación y hace referencia al objeto único global. El objeto de entidad de servicio define lo que la aplicación puede hacer en el inquilino específico, quién puede acceder a la aplicación y a qué recursos puede acceder la aplicación.

**Identidad administrada:** este tipo de entidad de servicio representa una identidad administrada, lo que elimina la necesidad de administrar las credenciales. Las identidades administradas proporcionan una identidad que usan las aplicaciones al conectarse a los recursos que admiten la autenticación de Microsoft Entra.

- Términos comunes para identidades administradas y entidades de servicio:
  - **Client ID:** el identificador único vinculado a la aplicación y a la entidad de servicio creada al aprovisionar la identidad.
  - **Id. de objeto:** el objeto de entidad de servicio de la identidad administrada.
  - **Azure Instance Metadata Service:** la API de REST que se habilita cuando Azure Resource Manager crea una máquina

virtual. Solo se puede acceder al punto de conexión desde dentro de la máquina virtual.

- **Heredado:** una entidad de servicio heredada representa una aplicación heredada que se creó antes de que se introdujeran los registros de aplicaciones o una aplicación creada a través de una experiencia de configuración heredada. Una entidad de servicio heredada puede tener credenciales, nombres de entidad de servicio, direcciones URL de respuesta y otras propiedades que un usuario autorizado puede editar. Una entidad de servicio heredada no tiene un registro de aplicación asociado.

### **Características de los objetos de aplicación y las entidades de servicio:**

- Una aplicación puede tener como máximo un objeto de aplicación, que se registra en un directorio "home".
- Una aplicación puede tener uno o varios objetos de entidad de servicio que representen instancias de la aplicación en todos los directorios en los que actúa.
- Un objeto de aplicación tiene una relación 1:1 con la aplicación de software y una relación 1:many con sus objetos de entidad de servicio.
- Debe crearse una entidad de servicio en cada inquilino donde se usa la aplicación para establecer una identidad para el inicio de sesión o el acceso a los recursos que va a proteger el inquilino.
- Una aplicación de inquilino único tendrá solo una entidad de servicio (en su inquilino principal), que normalmente se crea y se consiente para su uso durante el registro de la aplicación. Una aplicación multiinquilino también tiene una entidad de servicio creada en cada inquilino donde un usuario de ese inquilino ha dado su consentimiento para su uso.
- Se pueden conceder acceso y permisos a las entidades de servicio de identidad administrada, pero no se pueden actualizar ni modificar directamente.
- Las entidades de servicio heredadas solo se puede usar en el inquilino donde se crearon.

**Un objeto de entidad de servicio** para una aplicación se puede crear de maneras diferentes:

- Cuando una aplicación tiene permiso para acceder a los recursos de un inquilino (tras el registro o consentimiento), se crea un objeto de entidad de seguridad de servicio.
- Al registrar una aplicación desde Azure Portal, se crea automáticamente una entidad de servicio.
- Puede crear objetos de entidad de servicio en un inquilino mediante Azure PowerShell, la CLI de Azure, Microsoft Graph y otras herramientas.

**La identidad administrada** de Azure es una característica de Microsoft Entra ID que puede usar de forma gratuita. Esta característica crea de forma automática identidades para permitir que las aplicaciones se autentiquen con recursos y servicios de Azure. Las identidades administradas están disponibles en todas las ediciones de Microsoft Entra ID, incluida la edición gratuita que viene con una suscripción de Azure. Puede usar identidades administradas en App Service sin costo adicional y sin ninguna configuración necesaria. Las identidades administradas proporcionan una identidad para que las aplicaciones se usen al conectarse a recursos que admiten la autenticación de Microsoft Entra.

### **Características de las identidades administradas:**

- Una identidad administrada combina la autenticación de Microsoft Entra y el control de acceso basado en roles (RBAC) de Azure.
- Cuando se usan identidades administradas, no es necesario rotar las credenciales ni preocuparse por que las certificaciones expiren. Azure se encarga de la rotación de credenciales y la expiración en segundo plano. A fin de configurar una aplicación para que use una identidad administrada, se utiliza el token proporcionado para llamar al servicio.
- Los recursos que admiten identidades administradas asignadas por el sistema le permiten:
  - Habilitar o deshabilitar las identidades administradas en el nivel de recurso.
  - Usar roles de RBAC para conceder permisos.
  - Revise las operaciones de creación, lectura, actualización y eliminación (CRUD) en los registros de actividad de Azure.
  - Revise la actividad de inicio de sesión en los registros de inicio de sesión de Microsoft Entra.
- Las identidades administradas se pueden habilitar o deshabilitar en una aplicación en cualquier momento.

Hay dos tipos de identidades administradas:

- **Asignada por el sistema:** algunos servicios de Azure permiten habilitar identidades administradas directamente en una instancia de servicio. Cuando se habilita una identidad administrada asignada por el sistema, se crea una identidad en Microsoft Entra que está vinculada al ciclo de vida de esa instancia de servicio. Cuando se elimina el recurso, Azure elimina automáticamente la identidad. Por diseño, solo ese recurso de Azure puede usar esa identidad para solicitar tokens de Microsoft Entra ID.
- **Asignada por el usuario:** también puede crear una identidad administrada como un recurso independiente de Azure. Cree una identidad administrada asignada por el usuario y asígnela a una o varias instancias de un servicio de Azure. Una identidad asignada por el usuario se administra independientemente de los recursos que la utilicen.

**Azure Key Vault** proporciona un área de almacenamiento segura de forma que puede administrar todos los secretos de la aplicación y cifrar correctamente los datos en tránsito o mientras se almacenan.

Azure Key Vault puede ayudarle a resolver problemas de seguridad para Tailwind Traders:

- **Administre secretos.** Puede almacenar de forma segura y controlar estrechamente el acceso a tokens, contraseñas, certificados, claves de API y otros secretos.
- **Administrar claves.** Key Vault es una solución de administración de claves que permite crear y controlar fácilmente claves de cifrado para cifrar los datos corporativos.
- **Administre certificados.** Key Vault es un servicio que facilita la inscripción, administración e implementación de certificados públicos y privados de la Capa de sockets seguros y de Seguridad de la capa de transporte (SSL/TLS) para su uso con Azure y sus recursos internos conectados.

#### **Características de Key Vault:**

- Key Vault está disponible en dos niveles de servicio:
  - **El nivel Estándar** permite cifrar los datos con una clave de software.
  - **El nivel Premium** ofrece claves protegidas por módulo de seguridad de hardware (HSM).
- Puede establecer directivas con acceso restringido a los secretos que estén adaptadas a las aplicaciones y los individuos que las necesitan.
- La información confidencial de la aplicación se puede separar de otra configuración y código, lo que reduce el riesgo de pérdidas accidentales.
- El almacenamiento de secretos centralizado permite que los cambios necesarios se produzcan en un solo lugar.
- El registro y supervisión en Key Vault ayuda a saber cómo y cuándo se accede a los secretos.
- Key Vault proporciona acceso seguro a la información confidencial desde dentro de las aplicaciones:
  - Las claves, los secretos y los certificados están protegidos sin escribir código adicional y puede usar estos recursos de las aplicaciones.
  - Los clientes pueden poseer y administrar sus propias claves, secretos y certificados. Las aplicaciones no poseen la responsabilidad ni la responsabilidad potencial de los recursos de los clientes.
  - La aplicación puede usar claves para firmar y cifrar mientras mantiene la administración de claves externa de la aplicación.

- Puede administrar credenciales, como contraseñas, claves de acceso y tokens de firma de acceso compartido almacenándolos en Key Vault como secretos.
- La **eliminación temporal** está diseñada para evitar la eliminación accidental del almacén de claves y las claves, los secretos y los certificados almacenados en el mismo. Puede considerar la eliminación temporal como una papelera de reciclaje.
- **Protección de purga** La protección de purga está diseñada para evitar la eliminación de su almacén de claves, las claves, los secretos y los certificados de un agente interno malintencionado. Considere esto como una papelera de reciclaje con un bloqueo basado en el tiempo. Puede recuperar los elementos en cualquier momento durante el período de retención que haya configurado.

**Azure Monitor** se basa en una plataforma de datos de supervisión común que permite ver, analizar y trabajar con datos recopilados de los recursos. La plataforma ofrece muchas características que admiten dos componentes principales: **Registros** y **Métricas**.

**Los registros de Azure Monitor** le permiten recopilar y organizar datos de los recursos que supervisa. Configure qué datos se recopilan y cómo se organizan en la plataforma. Otras características de Azure Monitor almacenan automáticamente sus datos en Registros. Puede usar los datos almacenados con los datos recopilados para ayudar a supervisar el rendimiento de su entorno.

**Métricas de Azure Monitor** captura datos numéricos de los recursos supervisados y almacena los resultados en una base de datos organizada a tiempo. Las métricas se recopilan a intervalos especificados. Puede usar métricas para comprobar cómo funciona el sistema en un momento determinado o en determinadas circunstancias.

## **Características de Azure Monitor:**

- Se pueden recopilar datos de diferentes recursos en Azure Monitor y analizarlos en conjunto usando un conjunto común de herramientas.
- Los registros permiten realizar un análisis completo mediante consultas de registro.
- Las métricas admiten escenarios casi en tiempo real, como alertas de prioridad y respuesta a problemas críticos.
- Los datos de supervisión se pueden enviar a otras ubicaciones para admitir determinados escenarios, como el seguimiento y los informes.
- Los orígenes de datos de supervisión de las aplicaciones de Azure se pueden organizar en niveles y se puede acceder a cada nivel de diferentes maneras.
  - Los niveles más altos son para la propia aplicación.
  - Los niveles inferiores son componentes de la plataforma Azure.

Azure Monitor almacena los datos de registro en un área de trabajo de registros de Azure Monitor (Log Analytics). **Un área de trabajo** es un recurso de Azure que actúa como límite administrativo o ubicación geográfica para el almacenamiento de datos. El área de trabajo también es un contenedor donde se recopilan y agregan datos.

## **Características de las áreas de trabajo de registros de Azure Monitor:**

- En un área de trabajo, puede aislar los datos concediéndoles derechos de acceso a distintos usuarios siguiendo las estrategias de diseño recomendadas de Microsoft.
- Los datos de un área de trabajo de registros de Azure Monitor se organizan en tablas. Cada tabla almacena distintos tipos de datos y tiene su propio conjunto exclusivo de propiedades en función del recurso que genera los datos. La mayoría de los orígenes de datos escriben en sus propias tablas en un área de trabajo de registros de Azure Monitor.
- Un área de trabajo le permite configurar opciones como el plan de tarifa, la retención y el límite de datos en función de los límites administrativos o las ubicaciones geográficas.
- Con el control de acceso basado en roles de Azure (Azure RBAC) puede conceder a los usuarios y grupos solo la cantidad de acceso que necesitan para trabajar con los datos de supervisión en un área de trabajo. Puede alinear el control de acceso del usuario con el modelo de funcionamiento de la organización de TI mediante el uso de una sola área de trabajo para almacenar los datos recopilados habilitada en todos los recursos.
- Las áreas de trabajo se hospedan en clústeres físicos. De forma predeterminada, el sistema crea y administra estos clústeres. Si el sistema ingiere más de 500 GB de datos al día, cree sus propios clústeres

dedicados para las áreas de trabajo para admitir un mayor control y una mayor tasa de ingesta.

Implementación	Descripción
Centralizado	Todos los registros se almacenan en un área de trabajo central y se administran mediante un único equipo. Azure Monitor proporciona acceso diferenciado por equipo. En este escenario, es fácil administrar, buscar en los recursos y correlacionar registros entre ellos. El área de trabajo puede aumentar significativamente en función de la cantidad de datos recopilados de varios recursos de la suscripción. Se necesita sobrecarga administrativa adicional para mantener el control de acceso a distintos usuarios. Este modelo se conoce como <i>concentrador y radio</i> .
Descentralizado	Cada equipo tiene su propia área de trabajo creada en un grupo de recursos que poseen y administran. Los datos de registro se separan por recurso. En este escenario, el área de trabajo se puede mantener seguro y el control de acceso es coherente con el acceso de los recursos. Una desventaja de este módulo es que puede ser difícil correlacionar los registros entre sí. Los usuarios que necesitan una visión amplia de muchos recursos no pueden analizar los datos de forma significativa.
Híbrido	Un enfoque híbrido puede ser complicado por los requisitos de cumplimiento de auditoría de seguridad. Muchas organizaciones implementan ambos modelos de implementación en paralelo. Habitualmente, esto genera una configuración compleja, cara y difícil de mantener con problemas en la cobertura de los registros.
Modo de acceso	Descripción
Contexto del área de trabajo	Un usuario puede revisar todos los registros del área de trabajo para los que tienen permiso. Las consultas se limitan a todos los datos de todas las tablas en el área de trabajo. Para acceder a los registros con el área de trabajo como ámbito, seleccione <b>Registros</b> en el menú de Azure Monitor del Azure Portal.
Contexto del recurso	Un usuario accede al área de trabajo para un recurso, un grupo de recursos o una suscripción determinados. Al seleccionar <b>Registros</b> en un menú de recursos de Azure Portal, pueden ver los registros solo para los recursos de todas las tablas a las que tienen acceso. El ámbito de las consultas solo se limita a los datos asociados a dicho recurso. Este modo también permite Azure RBAC pormenorizado.

**Azure Workbooks** es una característica de Azure Monitor. Los libros proporcionan un lienzo flexible para el análisis de datos y la creación de informes visuales completos en el Azure Portal. Los clientes usan libros para explorar el uso de una aplicación, para realizar el análisis de la causa principal, reunir un cuaderno de estrategias operativo y muchas otras tareas.

### Características de los libros (workbooks):

- Azure Workbooks le permite acceder a varios orígenes de datos desde Azure y combinarlos en experiencias interactivas unificadas.
- Los autores de los libros pueden transformar los datos ingeridos para proporcionar información sobre la disponibilidad, el rendimiento, el uso y el estado general de los componentes subyacentes.
- Puede analizar los registros de rendimiento de las máquinas virtuales para identificar grandes instancias de CPU o de memoria insuficiente y mostrar los resultados como una cuadrícula en un informe interactivo.

**Azure insights** le ayuda a identificar problemas de rendimiento en la arquitectura de Tailwind Traders. Tenga en cuenta estas características sobre la información:

- Azure insights proporciona una experiencia de supervisión personalizada para determinadas aplicaciones y servicios.
- Azure insights recopila y analiza tanto los registros como las métricas.
- Muchas conclusiones se proporcionan como características de Azure Monitor. Estos son algunos ejemplos:

Conclusión	Descripción
<a href="#">Application Insights</a>	Supervise la aplicación web activa en cualquier plataforma mediante este servicio extensible de Administración y supervisión del rendimiento de la aplicación (APM) que está disponible en Azure Monitor.
<a href="#">Container Insights</a>	Supervise el rendimiento de las cargas de trabajo de contenedor implementadas en Azure Container Instances o en clústeres de Kubernetes administrados hospedados en Azure Kubernetes Service (AKS).
<a href="#">Información de redes</a>	Obtenga información completa sobre el estado y las métricas de todos los recursos de red. Use la funcionalidad de búsqueda avanzada para identificar las dependencias de recursos. Búsqueda por el nombre del sitio web para localizar los recursos que hospedan su sitio web.
<a href="#">Información de grupos de recursos</a>	Clasifica y diagnostica cualquier problema que encuentren sus recursos individuales, a la vez que ofrece un contexto en cuanto al estado y el rendimiento del grupo de recursos como un todo.
<a href="#">Información sobre máquinas virtuales</a>	Supervise las máquinas virtuales de Azure, los conjuntos de escalado de máquinas virtuales y otras máquinas virtuales. Analice el rendimiento y el estado de las máquinas virtuales Windows y Linux, y supervise sus procesos y dependencias en otros recursos y procesos externos.
<a href="#">Información de Azure Cache for Redis</a>	Revise un informe unificado e interactivo del rendimiento general, los errores, la capacidad y el mantenimiento operativo.
<a href="#">Información sobre Azure Cosmos DB</a>	Obtenga información sobre el rendimiento general, los errores, la capacidad y el estado operativo de todos los recursos de Azure Cosmos DB en una experiencia interactiva unificada.
<a href="#">Información detallada de Azure Key Vault</a>	Supervise sus almacenes de claves usando un informe unificado del rendimiento, los errores, la latencia y las solicitudes de Key Vault.
<a href="#">Información sobre Azure Storage</a>	Supervise de manera completa las cuentas de Storage al ofrecer un informe unificado del rendimiento, la capacidad y la disponibilidad de los servicios de Storage.

**Azure Data Explorer** es una plataforma de análisis de macrodatos que facilita el análisis de grandes volúmenes de datos casi en tiempo real. Azure Data Explorer incluye características que le ayudarán a configurar una solución de un extremo a otro para ingerir y administrar los datos, ejecutar consultas y generar visualizaciones.

## **Características de Azure Data Explorer:**

- El Explorador de datos de Azure es un servicio de exploración de datos altamente escalable y rápido para datos de telemetría y registro.
- Azure Data Explorer ayuda a controlar varios flujos de datos, por lo que puede recopilar, almacenar y analizar los datos de todos los recursos.
- Analiza grandes volúmenes de datos diversos desde cualquier origen de datos, como sitios web, aplicaciones, dispositivos de IoT, etc.
- Use Azure Data Explorer para diagnósticos, supervisión, informes, aprendizaje automático y otras tareas de análisis.

**El objetivo de tiempo de recuperación (RTO)** es la cantidad máxima de tiempo disponible para poner los recursos en línea después de una interrupción o un problema. Si ese proceso tarda más tiempo del indicado en RTO, podría haber consecuencias como penalizaciones financieras, trabajo que no se puede realizar, etc. El RTO se puede especificar para toda la solución, que incluye todos los recursos, así como para componentes individuales como instancias de SQL Server y bases de datos. El objetivo de punto de recuperación (RPO) es el momento específico al que se debe recuperar una base de datos y equivale a la cantidad máxima de pérdida de datos que la empresa está dispuesta a aceptar. Uno de los aspectos cruciales para el RTO y el RPO es conocer el costo del tiempo de inactividad. Si define ese número y el efecto global de la inactividad o la falta de disponibilidad para la empresa, es más fácil definir soluciones. Por ejemplo, si la empresa pudiera perder 10 000 USD por hora o ser sancionada por una agencia estatal si algo no se pudiera procesar, es una forma mensurable que ayuda a definir el RTO y el RPO. El gasto en la solución debe ser proporcional a la cantidad (o el costo) del tiempo de inactividad. Si la solución de HADR cuesta X, pero cuando se produce un problema solo le afecta durante unos segundos en lugar de horas o días, se paga solo. Desde un punto de vista no empresarial, el RTO se debe definir en el nivel de componente (por ejemplo, SQL Server), así como en toda la arquitectura de la aplicación. La calidad de la capacidad de recuperarse de una interrupción depende del eslabón más débil. Por ejemplo, si SQL Server y sus bases de datos se pueden poner en línea en 5 minutos, pero los servidores de aplicaciones tardan 20 en hacerlo, el RTO general sería de 20 minutos, no de 5. El entorno de SQL Server podría seguir teniendo un RTO de 5 minutos; no cambiará el tiempo total de recuperación.

**RPO** trata específicamente con datos e influye de manera directa en el diseño de cualquier solución de HADR, así como en las directivas y los procedimientos administrativos. Las características que se usen deben admitir el RTO y los RPO que se definan. Por ejemplo, si las copias de seguridad del registro de transacciones se programan cada 30 minutos, pero hay un RPO de 15 minutos, una base de datos solo se puede recuperar a la última copia de seguridad del registro de transacciones disponible, lo que en el peor de los casos sería de 30 minutos. Este intervalo asume que no hay otros problemas y que las copias de seguridad se han probado y se sabe que son correctas. Aunque es difícil probar cada copia de seguridad generada para cada base de datos del entorno, las copias de seguridad son simplemente archivos en un sistema de archivos. Si no se realizan restauraciones periódicas, como mínimo, no hay ninguna garantía de que sean correctas. La ejecución de comprobaciones durante el proceso de copia de seguridad puede proporcionar cierto grado de confianza.

Las características específicas que se usen, como un grupo de disponibilidad Always On o una instancia de clúster de conmutación por error (FCI) de Always On también afectarán a los RTO y RPO. Todos los RTO y RPO se deben documentar y revisar formalmente de forma periódica o según sea necesario. Una vez que se hayan documentado, puede considerar qué tecnologías y características puede usar para la arquitectura.

### **Diferencias entre infraestructura como servicios (IAS) y Plataforma como Servicio (PAS)**

En lo que respecta a la disponibilidad, la elección de IaaS o PaaS marca la diferencia. Con IaaS, tiene una máquina virtual, lo que significa que hay un sistema operativo con una instalación de SQL Server. El administrador o el grupo responsable de SQL Server podría elegir entre las soluciones de alta disponibilidad y recuperación ante desastres (HADR) y dispondría de gran control sobre cómo se configura la solución.

Con las implementaciones basadas en PaaS como Azure SQL Database, las soluciones de HADR se integran en la característica y, a menudo, solo es necesario habilitarlas. Hay opciones mínimas que se pueden configurar.

Debido a estas diferencias, la elección de IaaS o PaaS puede influir en el diseño final de la solución de HADR.

**Una instancia de SQL Server** es la instalación completa de SQL Server (archivos binarios, todos los objetos dentro de la instancia, incluidos los inicios de sesión, los trabajos de Agente SQL Server y las bases de datos). La protección de nivel de instancia significa que toda la instancia se tiene en cuenta en la característica de disponibilidad.

**Una base de datos de SQL Server** contiene los datos que usan los usuarios finales y las aplicaciones. Existen bases de datos del sistema en las que se basa SQL Server, así como bases de datos creadas para uso por parte de los usuarios finales y las aplicaciones. Una instancia de SQL Server siempre tiene sus propias bases de datos del sistema. La protección de nivel de base de datos significa que todo lo que incluye la base de datos, o se captura en el registro de transacciones para una base de datos de usuario o aplicación, se cuenta como parte de la característica de disponibilidad.

**La principal diferencia entre una FCI y un GD** es que el GD proporciona protección de nivel de base de datos. La réplica principal es la instancia que participa en un GD que contiene las bases de datos de lectura o escritura. Una réplica secundaria es donde la principal envía las transacciones por medio del transporte de registros para mantenerla sincronizada. El movimiento de datos entre una réplica principal puede ser sincrónico o asincrónico.

**El trasvase de registros** existe desde los inicios de SQL Server. La característica se basa en la copia de seguridad, copia y restauración, y es uno de los métodos más sencillos a fin de lograr HADR para SQL Server. **El trasvase de registros** se usa principalmente para la recuperación ante desastres, pero también sirve para mejorar la disponibilidad local. El mecanismo de trasvase de registros es simple: en primer lugar, se realiza una copia de seguridad completa de la base de datos de origen en el servidor principal, se restaura en un estado de carga (en espera o sin recuperación) en otra instancia conocida como servidor secundario o en modo de espera activa. Esta nueva copia de la base de datos se conoce como base de datos secundaria. Después, un proceso automatizado integrado en SQL Server creará automáticamente una copia de seguridad del registro de transacciones de la base de datos principal, la copiará en el servidor en espera y, por último, la restaurará en el modo de espera.

Azure proporciona tres opciones principales para mejorar la disponibilidad de las implementaciones de IaaS:

- **Conjuntos de disponibilidad**
- **Zonas de disponibilidad**
- **Azure Site Recovery**

Las tres opciones son externas a la máquina virtual (VM) y desconocen el tipo de carga de trabajo que se ejecuta dentro de ella.

**Los conjuntos de disponibilidad** proporcionan tiempo de actividad frente al mantenimiento relacionado con Azure y puntos únicos de error en un solo centro de datos. Los conjuntos de disponibilidad se separan en dominios de error y de actualización para admitir los dos tipos de actualización en la infraestructura subyacente de Azure. **Los dominios de error** son conjuntos de servidores dentro de un centro de datos, que usan la misma fuente de alimentación y la misma red; puede haber hasta tres dominios de error en un centro de datos. **Los dominios de actualización** indican grupos de máquinas virtuales y hardware físico subyacente que se pueden reiniciar al mismo tiempo. Los diferentes dominios de actualización garantizan la separación.

Los conjuntos de disponibilidad y las zonas no protegen frente a errores en el invitado, como un bloqueo del sistema operativo o RDBMS; por este motivo es necesario implementar soluciones adicionales, como GD o FCI, para asegurarse de cumplir los RTO y RPO. Los conjuntos de disponibilidad y las zonas están diseñados para limitar el impacto de los problemas del entorno en el nivel de Azure, como los errores de centro de datos o de hardware físico, y las interrupciones de la red y la alimentación.

**Las zonas de disponibilidad** tienen en cuenta los errores de nivel de centro de datos en Azure. Cada región de Azure se compone de muchos centros de datos con conexiones de red de baja latencia entre ellos. Al implementar recursos de máquina virtual en una región que admite Availability Zones, tiene la opción de implementarlos en la zona 1, 2 o 3. **Una zona** es una ubicación física única, es decir, un centro de datos, dentro de una región de Azure.

**Azure Site Recovery** proporciona disponibilidad mejorada para las máquinas virtuales en el nivel de Azure y puede funcionar con máquinas virtuales en las que se hospeda SQL Server. Azure Site Recovery replica una máquina virtual de una región de Azure en otra para crear una solución de recuperación ante desastres para esa máquina virtual. Azure Site Recovery tiene un RTO mensual determinado de dos horas.

**Azure Database for MySQL** tiene un acuerdo de nivel de servicio que garantiza una disponibilidad del 99,99 %, lo que significa que el tiempo de inactividad es prácticamente nulo. Para Azure Database for MySQL, si se produce un problema de nivel de nodo, como un error de hardware, se iniciará un mecanismo integrado de conmutación por error. Todos los cambios transaccionales en la base de datos MySQL se escriben de forma sincrónica en el almacenamiento en el momento de la confirmación. Si se produce una interrupción en el nivel de nodo, el servidor de bases de datos crea automáticamente otro nodo y adjunta el almacenamiento de datos. Azure Database for PostgreSQL usa un modelo similar a MySQL en su modelo de implementación estándar; pero Azure PostgreSQL también ofrece una solución de Hiperescala de escalabilidad horizontal denominada **Citus**. **Citus** proporciona escalabilidad horizontal y alta disponibilidad adicional para un grupo de servidores.

Si solo necesita alta disponibilidad y no recuperación ante desastres, la configuración de un grupo de disponibilidad (GD) es uno de los métodos más extendidos con independencia de dónde se use SQL Server.

## **¿Por qué merece la pena tener en cuenta esta arquitectura?**

- Esta arquitectura protege los datos mediante el uso de más de una copia en diferentes máquinas virtuales (VM).
- Esta arquitectura le permite cumplir el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) con una pérdida de datos entre mínima y nula si se implementa de forma correcta.
- Esta arquitectura proporciona un método sencillo y estandarizado para que las aplicaciones accedan a las réplicas principales y secundarias (si se van a utilizar elementos como las réplicas de solo lectura).
- Esta arquitectura proporciona disponibilidad mejorada durante escenarios de revisión.
- Esta arquitectura no necesita almacenamiento compartido, por lo que hay menos complicaciones que cuando se usa una instancia de clúster de comutación por error (FCI).

Las **FCI (Clúster de Comutación por Error)** no proporcionan muchas de las mismas protecciones que para el hardware físico, ya que es poco frecuente que una máquina virtual tenga un problema. Las FCI se han diseñado para la protección frente a errores de tarjeta de red o de disco, que probablemente no se produzcan en Azure. Las FCI se han diseñado para la protección frente a errores de tarjeta de red o de disco, que probablemente no se produzcan en Azure.

## **¿Por qué merece la pena tener en cuenta esta arquitectura?**

- Las FCI siguen siendo una solución de disponibilidad popular.
- La historia del almacenamiento compartido mejora con características como los discos compartidos de Azure.
- En esta arquitectura se cumple con la mayoría del RTO y el RPO de alta disponibilidad (aunque la recuperación ante desastres no se controla).
- Esta arquitectura proporciona un método sencillo y estandarizado para que las aplicaciones accedan a la instancia en clúster de SQL Server.
- Esta arquitectura proporciona disponibilidad mejorada durante escenarios de revisión.

Si usa GD, una opción consiste en configurar el GD en varias regiones de Azure, o bien como una posible arquitectura híbrida. Esto significa que todos los nodos que contienen las réplicas participan en el mismo WSFC. En este caso, se asume que la conectividad de red es correcta, especialmente si se trata de una configuración híbrida. Una de las consideraciones más importantes sería el recurso de testigo para el WSFC. Para esta arquitectura sería necesario que AD DS y DNS estuvieran disponibles en todas las regiones y, potencialmente, también en el entorno local si se trata de una solución híbrida.

## ¿Por qué merece la pena tener en cuenta esta arquitectura?

- Esta arquitectura es una solución probada; no es diferente a tener dos centros de datos en la actualidad en una topología de GD.
- Esta arquitectura funciona con las ediciones Standard y Enterprise de SQL Server.
- Los GD proporcionan redundancia de forma natural con copias adicionales de los datos.
- En esta arquitectura se usa una característica que proporciona alta disponibilidad y recuperación ante desastres

**Un GD distribuido** es una característica exclusiva de la edición Enterprise que se presentó en SQL Server 2016. Es diferente de un GD tradicional. En lugar de tener un WSFC subyacente en el que todos los nodos contienen réplicas que participan en un GD como se ha descrito en el ejemplo anterior, un GD distribuido se compone de varios GD. La réplica principal que contiene la base de datos de lectura y escritura se conoce como réplica principal global. La réplica principal del segundo GD se denomina reenviador y mantiene la sincronización de la réplica secundaria de ese GD. Básicamente se trata de un grupo de disponibilidad de grupos de disponibilidad.

Esta arquitectura facilita trabajar con aspectos como el cuórum, ya que cada clúster mantendría el suyo propio, lo que significa que también tiene su propio testigo. Un GD distribuido funcionará si usa Azure para todos los recursos, o bien si utiliza una arquitectura híbrida.

## ¿Por qué merece la pena tener en cuenta esta arquitectura?

- Esta arquitectura separa el **WSFC** (Clúster de conmutación por error de Windows Server) como un único punto de error si todos los nodos pierden la comunicación
- En esta arquitectura, una réplica principal no sincroniza todas las réplicas secundarias.
- Esta arquitectura puede proporcionar conmutación por recuperación de una ubicación a otra.

**El trasvase de registros** es uno de los métodos de HADR más antiguos para configurar la recuperación ante desastres para SQL Server. Como se ha descrito antes, la unidad de medida es la copia de seguridad del registro de transacciones. A menos que se planee el cambio a un estado de espera semiactiva para garantizar que los datos no se pierdan, lo más probable es que se produzca pérdida de datos. En lo que respecta a la recuperación ante desastres, siempre es mejor asumir cierta pérdida de datos, aunque sea mínima.

## **¿Por qué merece la pena tener en cuenta esta arquitectura?**

- El trasvase de registros es una característica probada y que se usa desde hace más de 20 años.
- Es fácil de implementar y administrar, ya que se basa en la copia de seguridad y la restauración.
- El trasvase de registros es tolerante a redes que no son sólidas.
- Cumple la mayoría de los objetivos de RTO y RPO para la recuperación ante desastres.
- El trasvase de registros es una buena manera de proteger las FCI.

Para aquellos que no quieran implementar una solución de recuperación ante desastres basada en SQL Server, Azure Site Recovery es una opción posible.

## **¿Por qué merece la pena tener en cuenta esta arquitectura?**

- Azure Site Recovery funcionará con algo más que simplemente SQL Server.
- Azure Site Recovery puede cumplir el RTO y posiblemente el RPO.
- Se proporciona como parte de la plataforma Azure.

Aunque una arquitectura se puede implementar en una o varias regiones de Azure, muchas organizaciones necesitan o quieren soluciones que abarquen tanto el entorno local como Azure, o bien posiblemente Azure y otra nube pública. Este tipo de arquitectura se conoce como **solución híbrida**. La infraestructura de Azure proporciona alta disponibilidad y recuperación ante desastres.

Las aplicaciones se consideran confiables si son de la siguiente manera:

- Resistentes a los errores de los componentes.
- De alta disponibilidad y con la capacidad de ejecutarse en un estado correcto sin un tiempo de inactividad significativo.

Para lograr la resistencia y la alta disponibilidad deseadas, primero debe definir sus requisitos.

La definición de los requisitos implica lo siguiente:

- Identificar sus necesidades empresariales.
- Crear un plan de resistencia para satisfacer esas necesidades.

Use la siguiente tabla de consideraciones como guía sobre este proceso.

Consideración	Descripción
¿Cuáles son sus cargas de trabajo y su utilización?	Una carga de trabajo es una funcionalidad o tarea independiente que está separada de forma lógica de otras tareas, en términos de requisitos de lógica de negocios y de almacenamiento de datos. Es probable que cada carga de trabajo tenga requisitos diferentes de disponibilidad, escalabilidad, coherencia de los datos y recuperación ante desastres.
¿Cuáles son los patrones de uso de sus cargas de trabajo?	Los patrones de uso pueden determinar sus requisitos. Identifique las diferencias en los requisitos durante los períodos críticos y no críticos. Para garantizar el tiempo de actividad, planifique la redundancia entre varias regiones en caso de que se produzca un error en una región. Por el contrario, para minimizar los costos durante los períodos no críticos, puede ejecutar la aplicación en una única región.
¿Cuáles son las métricas de disponibilidad?	El tiempo medio de recuperación (MTTR) y el tiempo medio entre errores (MTBF) son las métricas usadas normalmente. MTBF es lo que razonablemente es previsible esperar que dure un componente entre dos interrupciones. MTTR es el tiempo medio necesario para restaurar un componente después de un error. Use estas métricas para determinar dónde debe agregar la redundancia y definir los acuerdos de nivel de servicio (SLA) para los clientes.
¿Cuáles son las métricas de recuperación?	El objetivo de tiempo de recuperación (RTO) es el tiempo máximo aceptable que una de sus aplicaciones puede no estar disponible después de un incidente. El objetivo de punto de recuperación (RPO) es la duración máxima de la pérdida de datos que es aceptable durante un desastre. Tenga en cuenta también el objetivo de nivel de recuperación (RLO). Esta métrica determina la granularidad de la recuperación. En otras palabras, si debe poder recuperar una granja de servidores, una aplicación web, un sitio o simplemente un elemento específico. Para determinar estos valores, realice una evaluación de riesgos. Asegúrese de comprender el coste y el riesgo del tiempo de inactividad o la pérdida de datos en su organización.
¿Cuáles son los objetivos de disponibilidad de la carga de trabajo?	Para ayudar a garantizar que la arquitectura de la aplicación cumple los requisitos empresariales, defina los SLA objetivo para cada carga de trabajo. Analice el costo y la complejidad que supone satisfacer los requisitos de disponibilidad además de las dependencias de la aplicación.
¿Cuáles son sus SLA?	En Azure, el Acuerdo de Nivel de Servicio describe los compromisos de Microsoft en cuanto a tiempo de actividad y conectividad. Si el Acuerdo de Nivel de Servicio de un servicio determinado es del 99,9 %, significa que lo esperable es que el servicio esté disponible un 99,9 % del tiempo.

**Azure Backup** usa recursos de Azure para el almacenamiento a corto y largo plazo. Azure Backup minimiza o incluso elimina la necesidad de mantener medios físicos de copia de seguridad. Algunos ejemplos de soportes físicos de copia de seguridad son las cintas, las unidades de disco duro y los DVD.

<b>Tipo de copia de seguridad</b>	<b>Descripción</b>
Configuración local	Copia de seguridad de archivos, carpetas y del estado del sistema mediante el agente Microsoft Azure Recovery Services (MARS). También puede usar System Center Data Protection Manager (DPM) o el agente Microsoft Azure Backup Server (MABS) para proteger las máquinas virtuales locales (Hyper-V y VMware) y otras cargas de trabajo locales.
Azure Virtual Machines	Copia de seguridad de máquinas virtuales Windows o Linux completas (mediante extensiones de copia de seguridad) o copia de seguridad de archivos, carpetas y estados del sistema mediante el agente MARS.
Archivos de Azure	Copia de seguridad de recursos compartidos de archivos de Azure en una cuenta de almacenamiento.
SQL Server en máquinas virtuales de Azure	Copia de seguridad de bases de datos de SQL Server que se ejecutan en máquinas virtuales de Azure.
Bases de datos de SAP HANA en máquinas virtuales de Azure	Copia de seguridad de bases de datos de SAP HANA que se ejecutan en máquinas virtuales de Azure.
Nube de Microsoft	Azure Backup puede reemplazar su solución de copia de seguridad local o externa existente por una solución basada en la nube confiable, segura y rentable.

**Azure Backup** organiza los datos de copia de seguridad en una entidad de almacenamiento llamada *almacén*. **Un almacén** contiene copias de seguridad, puntos de recuperación y directivas de copia de seguridad. Hay dos tipos de almacenes: Azure Backup y Azure Recovery Services. Las principales diferencias son los tipos de orígenes de datos y los productos de Azure compatibles.

- **Almacén de Azure Backup:** los almacenes de Azure Backup solo se usan con Azure Backup. Los orígenes de datos admitidos incluyen servidores Azure Database for PostgreSQL, blobs de Azure y discos de Azure.
- **Almacén de Azure Recovery Services:** los almacenes de Azure Recovery Services se pueden usar con Azure Backup o Azure Site Recovery. Los orígenes de datos admitidos incluyen máquinas virtuales de Azure, SQL o SAP HANA en una máquina virtual de Azure y recursos compartidos de archivos de Azure. Puede hacer copia de seguridad de los datos en un almacén de Recovery Services desde Azure Backup Server, Azure Backup Agent y System Center Data Protection Manager.

Azure Backup proporciona una copia de seguridad operativa de blobs de Azure, que es una solución de copia de seguridad local para Azure Blob Storage. En este método de copia de seguridad, los datos de copia de seguridad se almacenan en la cuenta de almacenamiento de Azure de origen en lugar de transferirse a un almacén de Azure Backup.

### **Las características para la copia de seguridad y la recuperación de recursos:**

- La copia de seguridad operativa de blobs de Azure proporciona una solución de *copia de seguridad continua*. No es necesario programar las copias de seguridad.
- Todos los cambios de una copia de seguridad de blobs operativos se conservan durante un tiempo especificado y se pueden restaurar desde un momento dado seleccionado.
- La característica de eliminación temporal le permite proteger los datos frente a eliminaciones accidentales o daños. Durante el período de retención, puede restaurar un objeto de blob eliminado temporalmente al estado que tenía cuando se eliminó. La eliminación temporal está disponible para blobs y contenedores.
- El período de retención de blobs o contenedores eliminados se puede especificar entre 1 y 365 días. El período de retención predeterminado es de siete días.
- La solución de copia de seguridad operativa admite el control de versiones de blobs. Puede restaurar una versión anterior de un blob o recuperar los datos después de una modificación o eliminación incorrectas.
- La característica de recuperación a un momento dado para blobs en bloques le permite protegerse frente a eliminaciones accidentales o daños. Durante el período de retención, puede restaurar los blobs en bloques del estado actual a un estado en un momento anterior.
- La característica de bloqueo de recursos impide que se eliminen o modifiquen recursos por error. Puede establecer el bloqueo de recursos para prohibir la eliminación o permitir solo la lectura.

Puede implementar la característica de **eliminación temporal** para proteger un blob individual, una instantánea, un contenedor o una versión de blob de eliminaciones o sobreescrituras accidentales. La eliminación temporal mantiene los datos eliminados en el sistema durante un período de retención especificado. Durante el período de retención, puede restaurar un objeto eliminado temporalmente a su estado en el momento en que se eliminó.

Hay diferentes opciones para implementar la eliminación temporal y el control de versiones de blobs:

- Implemente la eliminación temporal de blobs para restaurar un archivo eliminado específico, como un blob, una instantánea o una versión de blob.
- Use la eliminación temporal de contenedores para restaurar un contenedor y su contenido.
- Agregue control de versiones de blobs para conservar automáticamente las versiones anteriores de un blob. Puede restaurar una versión anterior de un blob o usar la característica para recuperar los datos. El control de versiones de blobs es útil cuando hay varios autores que editan los mismos archivos.

Puede proteger los datos y evitar cambios accidentales mediante bloqueos de recursos. Esta característica impide que se eliminen o modifiquen recursos por error. Hay dos niveles de bloqueo: **CanNotDelete** y **ReadOnly**.

- **CanNotDelete** permite que los usuarios autorizados lean y modifiquen un recurso, pero no pueden eliminarlo sin quitar primero el bloqueo.
- **ReadOnly** permite a los usuarios autorizados leer un recurso, pero no pueden eliminarlo ni cambiarlo. Aplicar este bloqueo es como restringir a todos los usuarios autorizados a los permisos concedidos por el rol *Lector* en RBAC de Azure.

**Azure Files** proporciona la capacidad de tomar instantáneas de recursos compartidos de recursos compartidos de archivos. Las instantáneas de recursos compartidos proporcionan un nivel de seguridad adicional y ayudan a reducir el riesgo de daños en los datos o su eliminación accidental. También puede usar instantáneas de recurso compartido de archivos como copia de seguridad general para la recuperación ante desastres.

- Las instantáneas de recursos compartidos capturan el estado del recurso compartido en ese momento dado.
- Las instantáneas se pueden crear manualmente mediante Azure Portal, la API REST, las bibliotecas cliente, la CLI de Azure y PowerShell.
- Las instantáneas se pueden automatizar mediante directivas de copia de seguridad y Azure Backup.
- Las instantáneas se encuentran en el nivel raíz de un recurso compartido de archivos y se aplican a todas las carpetas y archivos que contiene. La recuperación se proporciona a nivel de archivo.
- Las instantáneas son incrementales. Solo se almacenan las diferencias entre las instantáneas.
- Despues de que se crea la instantánea de recurso compartido, puede leerla, copiarla o eliminarla, pero no modificarla.

- No se puede eliminar un recurso compartido que tenga instantáneas de recurso compartido. Para eliminar el recurso compartido, debe eliminar todas las instantáneas de recurso compartido.

**Azure Backup** proporciona copias de seguridad de máquinas virtuales de Azure independientes y aisladas. Puede usar Azure Backup para realizar copias de seguridad de instantáneas y restaurar los datos de las máquinas virtuales en caso de daño o eliminación accidental.

- Azure Backup permite una configuración y un escalado sencillos para máquinas virtuales Windows y Linux.

Azure Backup cuenta con ofertas especializadas para cargas de trabajo de base de datos como SQL Server y SAP HANA. Estas ofertas se basan en la carga de trabajo, proporcionan un RPO (objetivo de punto de recuperación) de 15 minutos y permiten la copia de seguridad y la restauración de bases de datos individuales.

- El trabajo de copia de seguridad de una máquina virtual conlleva dos fases:
  - En primer lugar, se toma una instantánea de máquina virtual.
  - En segundo lugar, la instantánea de máquina virtual se transfiere al almacén de Recovery Services.

La transferencia de los datos de copia de seguridad al almacén de Recovery Services no tiene ningún efecto sobre las cargas de trabajo de producción.

- Las copias de seguridad de máquinas virtuales de Azure almacenadas en un almacén de Recovery Services proporcionan la administración integrada de puntos de recuperación.
- Las copias de seguridad de máquinas virtuales están optimizadas para que pueda restaurar fácilmente una copia de seguridad completa o desde un punto de recuperación específico.
- Las copias de seguridad de instantáneas admiten distintos niveles de coherencia, como **aplicación, sistema y bloqueo**.
- Las copias de seguridad de máquinas virtuales se cifran en reposo con Storage Service Encryption (SSE). Azure Backup también puede hacer una copia de seguridad de las máquinas virtuales de Azure cifradas mediante Azure Disk Encryption (ADE).

Tanto SQL Database como SQL Managed Instance usan tecnología de SQL Server para crear copias de seguridad completas cada semana, copias de seguridad diferenciales cada 12 o 24 horas y copias de seguridad del registro de transacciones cada 5 o 10 minutos. La frecuencia de las copias de seguridad del registro de transacciones se basa en el tamaño de proceso y en la cantidad de actividad de la base de datos. Cuando una base de datos se restaura, el servicio averigua qué copia de seguridad completa, diferencial o del registro de transacciones es necesario restaurar.

- **Copias de seguridad completas:** En una copia de seguridad completa, se realiza una copia de seguridad de todo lo que se encuentra en la base de datos y en los registros de transacciones. SQL Database realiza una copia de seguridad completa una vez a la semana.
- **Copias de seguridad diferenciales:** En una copia de seguridad diferencial, se realiza una copia de seguridad de todo lo que ha cambiado desde la última copia de seguridad completa. SQL Database realiza una copia de seguridad diferencial cada 12 o 24 horas.
- **Copias de seguridad transaccionales:** En una copia de seguridad transaccional, se realiza una copia de seguridad del contenido de los registros de transacciones. Si se ha producido un error en el registro de transacciones más reciente o está dañado, la opción es volver a la copia de seguridad del registro de transacciones anterior. Las copias de seguridad transaccionales permiten a los administradores restaurar hasta un momento específico, lo que incluye el momento en el que se han eliminado los datos por error. Copias de seguridad del registro de transacciones cada 5 o 10 minutos.

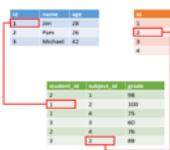
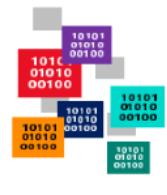
Las copias de seguridad automáticas de Azure SQL Database están disponibles para su restauración durante un máximo de **35 días**. Este período es suficiente para los fines de la administración diaria.

**Azure Site Recovery** proporciona características de BCDR en las aplicaciones tanto locales como en Azure y en otros proveedores de servicios en la nube. El servicio ofrece planes que ayudan a automatizar la recuperación ante desastres. Puede definir cómo se conmutan por error las máquinas virtuales y el orden en que se reinician después de una comutación por error correcta.

Característica	Descripción
Replicación de máquinas virtuales de Azure	Configure la recuperación ante desastres de las máquinas virtuales de Azure y la conmutación por error de una región primaria a una región secundaria.
Replicación de máquinas virtuales locales	Replique los servidores físicos y las máquinas virtuales locales en Azure o en un centro de datos local secundario.
Replicación de cargas de trabajo	Replique cualquier carga de trabajo que se ejecute en máquinas virtuales de Azure compatibles, máquinas virtuales de Hyper-V y VMware locales y servidores físicos Windows o Linux.
Automatización de tareas de BCDR	Automatice las tareas de BCDR y reduzca aún más el objetivo de tiempo de recuperación. Puede usar Azure Site Recovery para configurar conmutaciones por error periódicas de prueba y supervisar la eficacia general del proceso de recuperación.
Mantenimiento de la resistencia de los datos	Use Azure Site Recovery para organizar la replicación sin interceptar los datos de la aplicación. Cuando se produce la conmutación por error, las máquinas virtuales de Azure se crean en función de los datos replicados. Cuando se hace la replicación en Azure, los datos se almacenan en Azure Storage y se obtiene la resistencia proporcionada por ese servicio.
Cumplimiento de los objetivos RTO y RPO	Mantenga el RTO y el RPO dentro de los límites definidos de la organización. Azure Site Recovery proporciona replicación continua para máquinas virtuales de Azure y máquinas virtuales de VMware, y una frecuencia de replicación de tan solo 30 segundos para Hyper-V.
Mantenimiento de aplicaciones consistentes después de la conmutación por error	Mediante las instantáneas consistentes entre aplicaciones, puede realizar la replicación a partir de puntos de recuperación específicos. Estas instantáneas capturan los datos de disco, los datos en memoria y todas las transacciones en proceso.
Prueba sin interrupciones	Ejecute pruebas de recuperación ante desastres, sin que ello afecte a la replicación en curso.
Ejecución de conmutaciones por error flexibles	Ejecute conmutaciones por error planeadas para las interrupciones esperadas sin pérdida de datos. Ejecute conmutaciones por error no planeadas con una pérdida de datos mínima y conmute por recuperación al sitio primario cuando vuelva a estar disponible.
Personalización de planes de recuperación	Cree planes de recuperación para personalizar y secuenciar la conmutación por error y la recuperación de las aplicaciones de varios niveles que se ejecutan en varias máquinas virtuales. Agrupe las máquinas virtuales en un plan de recuperación y agregue scripts y acciones manuales según sea necesario. Integre planes de recuperación con runbooks de Azure Automation.
Integración con tecnologías de BCDR	Integre Azure Site Recovery con otras tecnologías de BCDR. Use Site Recovery para proteger el back-end de SQL Server de las cargas de trabajo corporativas. Debido a su compatibilidad nativa con SQL Server AlwaysOn, puede administrar la conmutación por error de los grupos de disponibilidad.
Acceso a la integración de Azure Automation	Descargue desde la biblioteca de Azure Automation e integre scripts específicos de la aplicación con Azure Site Recovery.

# AZ-305: Diseño de soluciones de almacenamiento de datos

El primer paso del diseño de Azure Storage consiste en determinar qué tipos de datos son necesarios para la organización. En general, los datos se pueden clasificar de tres maneras diferentes: **estructurados, semiestructurados y no estructurados**. La mayoría de las organizaciones necesitan proporcionar opciones de almacenamiento para todos los tipos de datos.

Estructurados	Semiestructurados	Datos no estructurados
 Los datos estructurados se almacenan en un formato relacional que tiene un esquema compartido. Los datos estructurados suelen estar en una tabla de base de datos con filas, columnas y claves.	 Los datos semiestructurados están menos organizados. Los campos de datos no encajan fácilmente en tablas, filas ni columnas. Los datos semiestructurados contienen etiquetas que aclaran cómo se organizan los datos. Los datos se definen mediante un lenguaje de serialización.	 Los datos no estructurados son los menos organizados. Estos datos son una combinación de información que se almacena juntos, pero los datos no tienen una relación clara. El formato de datos no estructurados se conoce como <i>no relacional</i> .
<ul style="list-style-type: none"><li>- Bases de datos relacionales, como registros médicos, agendas de teléfonos y cuentas financieras.</li><li>- Datos de aplicación para un sitio web de comercio electrónico.</li></ul>	<ul style="list-style-type: none"><li>- Archivos de Lenguaje de marcado de hipertexto (HTML).</li><li>- Archivos de notación de objetos JavaScript (JSON).</li><li>- Archivos de lenguaje de marcado extensible (XML).</li></ul>	<ul style="list-style-type: none"><li>- Archivos multimedia, como fotos, videos y audio.</li><li>- Archivos de Office, como documentos de Word y diapositivas de PowerPoint.</li><li>- Archivos de texto, como PDF, TXT y RTF.</li></ul>

**Una cuenta de almacenamiento de Azure agrupa** todos los servicios de Azure Storage. La cuenta de almacenamiento proporciona un espacio de nombres único al que se puede acceder desde cualquier lugar (suponiendo que tenga los permisos correctos) del mundo a través de HTTPS. Los datos de la cuenta de almacenamiento son duraderos y altamente disponibles, seguros y escalables a gran escala. Una cuenta de almacenamiento representa una colección de valores de configuración, como la ubicación, la estrategia de replicación o el propietario de la suscripción.

Cuenta de almacenamiento	Servicios admitidos	Uso recomendado
<a href="#">Uso general estándar v2</a>	Blob Storage (incluido Data Lake Storage), Queue Storage, Table Storage y Azure Files	Cuenta de almacenamiento estándar para la mayoría de los escenarios, incluidos blobs, recursos compartidos de archivos, colas, tablas y discos (blobs en páginas).
<a href="#">Blobs en bloques Premium</a>	Blob Storage (incluido Data Lake Storage)	Cuenta de almacenamiento Premium para blobs en bloques y blobs anexos. Se recomienda para las aplicaciones con altas tasas de transacciones. Use blobs en bloques Premium si trabaja con objetos más pequeños o requiere una latencia de almacenamiento constantemente baja. Este almacenamiento está diseñado para escalarse con las aplicaciones.
<a href="#">Recursos compartidos de archivos Premium</a>	Azure Files	Cuenta de almacenamiento Premium solo para recursos compartidos de archivos. Se recomienda para empresas y aplicaciones de escalado de alto rendimiento. Use recursos compartidos de archivos Premium si necesita compatibilidad con el Bloque de mensajes del servidor (SMB) y los recursos compartidos de archivos NFS.
<a href="#">Blobs en páginas Premium</a>	Solo blobs en páginas	Cuenta de almacenamiento de alto rendimiento Premium solo para blobs en páginas. Los blobs en páginas son ideales para almacenar estructuras de datos dispersas y basadas en índices, como los sistemas operativos, los discos de datos para máquinas virtuales y las bases de datos.

Azure Storage siempre almacena varias copias de los datos. Esta redundancia garantiza que los datos están protegidos frente a eventos planeados y no planeados. Estos eventos pueden incluir errores transitorios de hardware, cortes de red o de energía y desastres naturales masivos. **La redundancia del almacenamiento** garantiza que su cuenta de almacenamiento cumple los objetivos de disponibilidad y durabilidad.

### **Características sobre la redundancia de datos en Azure Storage:**

- La redundancia se logra mediante la replicación de datos en una región primaria.
- Al crear una cuenta de almacenamiento, seleccione la región principal de la cuenta.
- La región primaria admite dos opciones de replicación: almacenamiento con redundancia local (LRS) y almacenamiento con redundancia de zona (ZRS).
- La replicación también se puede realizar en una región secundaria. Se recomienda usar una región secundaria con aplicaciones que requieran una alta durabilidad.
- La región secundaria emparejada se determina en función de la región primaria y no se puede cambiar.
- La región secundaria suele estar en una ubicación geográfica alejada de la región primaria. Esta distancia ayuda a protegerse de desastres circunscritos a una región.
- La región secundaria admite dos opciones de replicación: almacenamiento con redundancia geográfica (GRS) y almacenamiento con redundancia de zona geográfica (GZRS).

Azure Storage ofrece dos opciones para replicar los datos en la región primaria: almacenamiento con redundancia local y almacenamiento con redundancia de zona.

- El **almacenamiento con redundancia local** es la opción de redundancia de coste más bajo y que ofrece la menor durabilidad. LRS protege los datos frente a errores en la estantería de servidores y en la unidad. Sin embargo, si se produce un error en el centro de datos, todas las réplicas de una cuenta de almacenamiento que usen LRS pueden perderse o quedar irrecuperables.
- El **almacenamiento con redundancia de zona** replica de forma sincrónica en tres zonas de disponibilidad de Azure en la región primaria. Con ZRS, los datos son accesibles para las operaciones de escritura y lectura incluso si una zona deja de estar disponible.

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

- La principal diferencia entre GRS y GZRS es la forma en que los datos se replican en la región primaria. Dentro de la región secundaria, los datos siempre se replican sincrónicamente con LRS.

Hay dos puntos principales que se deben tener en cuenta en un plan de implementación para **Azure Blob Storage**. En primer lugar, debe identificar qué *nivel de acceso a blobs* de Azure satisface los requisitos de disponibilidad, latencia y costo de almacenamiento de la organización. La segunda consideración es decidir si necesita acceso al almacenamiento inmutable.

Hay cuatro opciones de acceso: **Premium Blob Storage** y los niveles de **acceso frecuente, esporádico y de archivo**. Las cuatro opciones admiten la disponibilidad y la latencia, pero tienen costos diferentes en función del nivel de soporte técnico. Todas las opciones también admiten almacenamiento inmutable, pero el almacenamiento se implementa de forma diferente para los niveles de acceso frecuente, esporádico y de archivo.

De comparación	Nivel de acceso frecuente	Nivel de acceso esporádico	Nivel de acceso esporádico	Nivel de acceso de archivo
Disponibilidad	99,9 %	99%	99%	99%
Disponibilidad (lecturas de RA-GRS)	99,99%	99,9 %	99,9 %	99,9 %
Latencia (tiempo hasta el primer byte)	milisegundos	milisegundos	milisegundos	horas
Duración mínima del almacenamiento	N/D	30 días	90 días	180 días

- **Premium Blob Storage** es más adecuado para cargas de trabajo con gran cantidad de E/S que requieren una latencia de almacenamiento baja y coherente. Premium Blob Storage utiliza unidades de estado sólido (SSD) para lograr tiempos de respuesta rápidos y coherentes. Este almacenamiento es mejor para cargas de trabajo que realizan muchas transacciones pequeñas. Un ejemplo sería una aplicación de asignación que requiere actualizaciones frecuentes y rápidas.
- El **nivel de acceso frecuente** tiene los costos de acceso más bajos, pero mayores costos de almacenamiento que los niveles de acceso esporádico y de archivo. El nivel de acceso frecuente está optimizado para lecturas y escrituras frecuentes de objetos en la cuenta de almacenamiento. Un buen caso de uso son los datos que se están procesando activamente. De forma predeterminada, las nuevas cuentas de almacenamiento se crean en el nivel de acceso frecuente.
- El **nivel de acceso esporádico** tiene menores costos de almacenamiento y mayores costos de acceso en comparación con el almacenamiento de acceso frecuente. El nivel de acceso esporádico está optimizado para almacenar grandes cantidades de datos a los que se accede con poca frecuencia. Este nivel está diseñado para datos que permanecen en el nivel de acceso esporádico durante al menos 30 días. Un caso de uso para el nivel de acceso esporádico son los conjuntos de datos de copia de

seguridad y recuperación ante desastres a corto plazo y los contenidos multimedia antiguos. Este contenido no se debe ver con frecuencia, pero debe estar disponible inmediatamente.

- **El nivel de acceso de archivo** es el más rentable de todos para almacenar datos, pero el acceso a esos datos es más costoso que acceder a los datos de otros niveles. El nivel de acceso de archivo es un nivel sin conexión que está optimizado para los datos que pueden tolerar varias horas de latencia de recuperación. Los datos deben permanecer en el nivel de archivo durante al menos 180 días o estar sujetos a un cargo por eliminación temprana. Los datos del nivel de archivo incluyen copias de seguridad secundarias, datos sin procesar originales e información de cumplimiento requerida legalmente.

**El almacenamiento inmutable** de Azure Blob Storage permite a los usuarios almacenar los datos críticos para la empresa en un estado WORM (escribir una vez, leer muchas). Mientras se encuentren en un estado WORM, los datos no se podrán modificar ni eliminar durante el tiempo especificado por el usuario. Con la configuración de directivas de inmutabilidad para los datos de blobs, puede impedir que sus datos se sobrescriban y eliminen. Las directivas se aplican en el nivel de contenedor y los registros de auditoría están disponibles.

Azure Blob Storage admite dos formas de directivas de inmutabilidad para implementar el almacenamiento inmutable:

- **Las directivas de retención con duración definida** permiten a los usuarios establecer directivas para almacenar los datos durante un intervalo especificado. Cuando hay una directiva de retención basada en el tiempo, los objetos se pueden crear y leer, pero no modificar ni eliminar. Una vez expirado el período de retención, los objetos se pueden eliminar pero no sobrescribir. Los niveles de acceso frecuente, esporádico y de archivo admiten almacenamiento inmutable mediante directivas de retención de tiempo.
- **Las directivas de suspensión legal** almacenan datos inmutables hasta que se borra explícitamente la suspensión legal. Cuando se establece una suspensión legal, los objetos se pueden crear y leer, pero no modificar ni eliminar. Premium Blob Storage usa suspensiones legales para admitir el almacenamiento inmutable.

**Azure Files** proporciona recursos compartidos de archivos totalmente administrados y basados en la nube que están hospedados en Azure. Puede acceder a los archivos compartidos mediante el protocolo Bloque de mensajes del servidor (SMB) estándar del sector, el protocolo Network File System (NFS) y la API de REST de Azure Files. Puede montar un recurso compartido de archivos de Azure Files o conectarse a él simultáneamente en todos los sistemas operativos principales.

Se puede usar Azure Files para agregar o reemplazar los servidores de archivos o los dispositivos de almacenamiento conectado a la red (NAS) locales existentes de la empresa. Estas son algunas de las razones por las que su organización debe usar Azure Files:

- Los desarrolladores pueden almacenar aplicaciones y archivos de configuración en un recurso compartido de archivos y conectar nuevas máquinas virtuales a los archivos compartidos. Esta acción reduce el tiempo necesario para poner nuevas máquinas en producción.
- Con los recursos compartidos de archivos de Azure, las empresas no tienen que comprar e implementar costoso hardware redundante ni administrar las actualizaciones de software. Los recursos compartidos son multiplataforma y puede conectarse a ellos desde Windows, Linux o macOS.
- El recurso compartido de archivos hereda toda la resistencia de la plataforma de Azure, lo que hace que los archivos tengan redundancia global. También tiene la posibilidad de usar la característica de instantáneas integradas y de configurar copias de seguridad automáticas mediante almacenes de Recovery Services.
- Todos los datos se cifran en tránsito mediante HTTPS y se almacenan cifrados cuando están en reposo.

Los recursos compartidos de archivos de Azure se pueden usar de dos maneras. Puede montar directamente recursos compartidos de archivos de Azure sin servidor (SMB) o almacenar en caché recursos compartidos de archivos de Azure a nivel local mediante Azure File Sync.

- **Montaje directo de recursos compartidos de archivos de Azure:** dado que Azure Files proporciona acceso SMB, puede montar recursos compartidos de archivos de Azure de forma local o en la nube. El montaje usa el cliente SMB estándar disponible en Windows, macOS y Linux. Dado que los recursos compartidos de archivos de Azure no tienen servidor, la implementación en escenarios de producción no requiere la administración de un servidor de archivos o un dispositivo NAS. El montaje directo significa que no es necesario aplicar revisiones de software ni intercambiar discos físicos.
- **Almacenamiento en caché del recurso compartido de archivos de Azure local con Azure File Sync:** Azure File Sync permite centralizar los recursos compartidos de archivos de la organización. Azure Files proporciona la flexibilidad, el rendimiento y la compatibilidad de un servidor de archivos local. Azure File Sync transforma una instancia de Windows Server local (o en la nube) en una caché rápida de su recurso compartido de archivos de Azure.

Azure Files ofrece cuatro niveles de almacenamiento. Estos niveles permiten adaptar los recursos compartidos de archivos a los requisitos de rendimiento y precio de su escenario.

- **Premium:** los recursos compartidos de archivos están respaldados por unidades de estado sólido (SSD) y proporcionan un alto rendimiento coherente y una latencia baja. Se usa para las cargas de trabajo que más consumen E/S. Las cargas de trabajo adecuadas incluyen bases de datos, hospedaje de sitios web y entornos de desarrollo. Se puede usar con los protocolos Bloque de mensajes del servidor (SMB) y Network File System (NFS).
- **Optimizado para transacciones:** se utiliza para cargas de trabajo con muchas transacciones que no necesitan la latencia que ofrecen los recursos compartidos de archivos premium. Los recursos compartidos de archivos se ofrecen en el hardware de almacenamiento estándar con el respaldo de unidades de disco duro (HDD).
- **Nivel de acceso frecuente:** optimizado para el almacenamiento para escenarios de uso compartido de archivos de uso general, como recursos compartidos entre equipos. Se ofrece en hardware de almacenamiento estándar con el respaldo de HDD.
- **Nivel de acceso esporádico:** optimizado para el almacenamiento rentable para escenarios de almacenamiento de archivo en línea. Se ofrece en hardware de almacenamiento con el respaldo de HDD.

**Azure NetApp Files**, es un servicio NAS de nivel empresarial totalmente administrado y de alta disponibilidad. Azure NetApp Files puede controlar las cargas de trabajo más exigentes, de alto rendimiento y de baja latencia. Puede migrar cargas de trabajo que se consideran "no migrables".

De comparación	Azure Blob Storage	Azure Files	Azure NetApp Files
Descripción	<p>Azure Blob Storage es más adecuado para cargas de trabajo de acceso secuencial de lectura intensa a gran escala en las que los datos se ingieren una vez y se modifican más adelante.</p> <p>Blob Storage ofrece el costo total de propiedad más bajo, si hay poco o ningún mantenimiento.</p>	<p>Azure Files es un servicio de alta disponibilidad que está optimizado para cargas de trabajo de acceso aleatorio.</p> <p>En el caso de los recursos compartidos de NFS, Azure Files proporciona compatibilidad completa con el sistema de archivos POSIX y se puede usar fácilmente desde plataformas de contenedor, como Azure Container Instance (ACI) y Azure Kubernetes Service (AKS) con el controlador CSI integrado, además de plataformas basadas en máquinas virtuales.</p>	<p>Azure NetApp Files es un servicio de archivos totalmente administrado en la nube, con tecnología de NetApp, con funcionalidades de administración avanzadas.</p> <p>Azure NetApp Files es adecuado para cargas de trabajo que requieren acceso aleatorio y proporciona una amplia compatibilidad con protocolos y funcionalidades de protección de datos.</p>
Casos de uso	Datos analíticos a gran escala, informática de alto rendimiento sensible al rendimiento, copia de seguridad y archivo, conducción autónoma, representación multimedia o secuenciación genómica.	Archivos compartidos, bases de datos, directorios principales, aplicaciones tradicionales, ERP, CMS, migraciones NAS que no requieren administración avanzada y aplicaciones personalizadas que requieren almacenamiento de archivos de escalabilidad horizontal.	Migración de NAS empresarial local que requiere funcionalidades de administración Enriquecidas, cargas de trabajo sensibles a la latencia como SAP HANA, proceso de alto rendimiento con uso intensivo de IOPS o latencias, o cargas de trabajo que requieren acceso simultáneo a varios protocolos.
Protocolos disponibles	<ul style="list-style-type: none"> <li>- NFS 3.0</li> <li>- REST</li> <li>- Data Lake Storage Gen2</li> </ul>	<ul style="list-style-type: none"> <li>- SMB</li> <li>- NFS 4.1</li> <li>- REST</li> </ul>	<ul style="list-style-type: none"> <li>- NFS 3.0 y 4.1</li> <li>- SMB</li> </ul>
Rendimiento (por volumen)	Hasta 20 000 IOPS, con un rendimiento de 15 GiB/s	Hasta 100 000 IOPS, con un rendimiento de 10 GiB/s	Hasta 460 000 IOPS, un rendimiento de 4,5 GiB/s por volumen normal y un rendimiento de 10 GiB/s por volumen grande

Las máquinas virtuales usan discos de datos para almacenar datos como archivos de base de datos, contenido estático del sitio web o código de aplicación personalizado. El número de discos de datos que puede agregar depende del tamaño de la máquina virtual. Cada disco de datos tiene una capacidad máxima de **32 767 GB**.

De comparación	Disco Ultra	SSD Premium	SSD estándar	HDD estándar
Tipo de disco	SSD	SSD	SSD	HDD
Escenario	Cargas de trabajo intensivas de E/S (como SAP HANA), bases de datos de nivel superior como SQL Server y Oracle y otras cargas de trabajo con gran cantidad de transacciones	Cargas de trabajo delicadas de producción y rendimiento	Servidores web, aplicaciones empresariales poco usadas, desarrollo y pruebas	Copia de seguridad, no crítico, acceso poco frecuente
Rendimiento máx.	2000 Mbps	900 Mbps	750 Mbps	500 Mbps
IOPS máx.	160 000	20.000	6,000	2\,000

Hay varios tipos de cifrado disponibles para los discos administrados.

- **Azure Disk Encryption (ADE)** cifra los discos duros virtuales (VHD) de la máquina virtual. Si el disco duro virtual está protegido con ADE, solo la máquina virtual que posee el disco tendrá acceso a la imagen de disco.
- **El cifrado del lado del servidor (SSE)** se ejecuta en los discos físicos del centro de datos. Si alguien accede directamente al disco físico, los datos se cifrarán. Cuando se accede a los datos desde el disco, se descifran y se cargan en la memoria. Esta forma de cifrado también se conoce como *cifrado en reposo* o cifrado de Azure Storage.
- **El cifrado en el host** garantiza que los datos almacenados en el host de máquina virtual se cifren en reposo y fluyan cifrados al servicio Storage. Los discos con cifrado en el host habilitado no se cifran con SSE. En su lugar, el servidor que hospeda la máquina virtual proporciona el cifrado de los datos, y los datos cifrados fluyen a Azure Storage.

**Azure Storage** proporciona un modelo de seguridad en capas que permite proteger y controlar el nivel de acceso a las cuentas de almacenamiento. El modelo consta de varias opciones de seguridad de almacenamiento, como directivas de firewall, claves administradas por el cliente y puntos de conexión.

- La línea de base de seguridad de Azure para Azure Storage concede acceso limitado a los recursos de Azure Storage. La línea de base de seguridad de Azure proporciona una lista completa de maneras de proteger el almacenamiento de Azure.
- La firma de acceso compartido (SAS) proporciona acceso delegado seguro a los recursos de la cuenta de almacenamiento. Con una SAS, tiene control granular sobre la forma en que un cliente puede tener acceso a los datos.
- Las directivas y reglas de firewall limitan el acceso a la cuenta de almacenamiento. Las solicitudes se pueden limitar a intervalos o direcciones IP específicos, o a una lista de subredes de una red virtual de

Azure. El firewall de Azure Storage proporciona control de acceso para el punto de conexión público de la cuenta de almacenamiento.

- Los puntos de conexión de servicio de red virtual restringen el acceso de red y proporcionan conexión directa al almacenamiento de Azure. Puede proteger las cuentas de almacenamiento en la red virtual y habilitar direcciones IP privadas en la red virtual para llegar al punto de conexión de servicio. Con los puntos de conexión privado, puede crear una interfaz de red especial para un servicio de Azure en la red virtual.
- La transferencia segura permite que una cuenta de almacenamiento de Azure acepte solicitudes de conexiones seguras. Cuando se requiere una transferencia segura, se rechazan las solicitudes originadas en conexiones no seguras. Microsoft recomienda que siempre requiera una transferencia segura para todas las cuentas de almacenamiento.
- Los datos de la cuenta de almacenamiento se cifran automáticamente. **El cifrado de Azure Storage ofrece dos maneras de administrar las claves de cifrado en el nivel de cuenta de almacenamiento:**
  - Claves administradas por Microsoft: de forma predeterminada, Microsoft administra las claves que se usan para cifrar la cuenta de almacenamiento.
  - Claves administradas por el cliente: opcionalmente, puede elegir administrar las claves de cifrado de la cuenta de almacenamiento. Las claves administradas por el cliente deben almacenarse en Azure Key Vault.

**Los datos relacionales** son un tipo de datos estructurados que tienen un esquema compartido. A menudo se almacenan en tablas de base de datos con filas, columnas y claves, y se usan para el almacenamiento de aplicaciones, como los sitios web de comercio electrónico.

**Azure SQL Database** es una opción de implementación de PaaS de Azure SQL que abstrae tanto el sistema operativo como la instancia de SQL Server. Una base de datos Azure SQL es un servicio totalmente administrado. No es necesario encargarse de tareas complejas de base de datos, como configurar y administrar la alta disponibilidad, los ajustes y las copias de seguridad. El servicio actualiza automáticamente cada base de datos SQL para ejecutar la versión más reciente de SQL Server. Las funcionalidades de SQL Server más recientes se obtienen sin tener que realizar ninguna actualización manual.

#### **Características de la opción de implementación de SQL Database:**

- Es un servicio de base de datos relacional, inteligente y de alta escalabilidad creado para la nube con el acuerdo de nivel de servicio de mayor disponibilidad del sector.
- SQL Database es la única opción de implementación que admite escenarios en los que se necesitan bases de datos muy grandes

(actualmente, de hasta 100 TB) o escalado automático para las cargas de trabajo imprevisibles (sin servidor).

- Se puede crear un **grupo de bases de datos elásticas de SQL Database**, donde todas las bases de datos del grupo comparten el mismo conjunto de recursos de proceso y almacenamiento. Cada base de datos puede usar los recursos que necesite, dentro de los límites establecidos, según la carga actual.
- Principalmente, hay dos opciones de precios de SQL Database: DTU y núcleo virtual. También hay disponible una opción sin servidor para una base de datos única.
  - **Núcleo virtual:** se elige el número de núcleos virtuales para tener un mayor control sobre los costes de proceso. Esta opción admite la Ventaja híbrida de Azure para SQL Server y la capacidad reservada (pago por adelantado).
  - **DTU:** una DTU (unidad de transacción de base de datos) es una medida combinada de recursos de proceso, almacenamiento y E/S. La opción de DTU es una opción de compra sencilla y preconfigurada.
  - **Sin servidor:** nivel de proceso para bases de datos únicas en SQL Database. El modelo sin servidor escala automáticamente el proceso en función de la demanda de la carga de trabajo, y se factura única y exclusivamente según la cantidad de proceso usado.

**Azure SQL Managed Instance** es una opción de implementación PaaS de Azure SQL. Al igual que Azure SQL Database, Azure SQL Managed Instance es un servicio totalmente administrado. Ofrece una instancia de SQL Server, pero quita gran parte de la sobrecarga que supone la administración de una máquina virtual.

#### **Características de SQL Managed Instance:**

- SQL Managed Instance se puede usar para realizar migraciones mediante lift-and-shift a Azure sin tener que rediseñar las aplicaciones.
- Azure SQL Managed Instance es ideal para aquellos clientes que estén interesados en características con ámbito de instancia, como Agente SQL Server, Common Language Runtime (CLR), Correo electrónico de base de datos, las transacciones distribuidas y Machine Learning Services.
- SQL Managed Instance usa núcleos virtuales. Puede definir el número máximo de núcleos de CPU y el almacenamiento máximo asignados a la instancia administrada. Todas las bases de datos dentro de la instancia administrada comparten los recursos asignados a esa instancia.
- La mayoría de las funciones disponibles en SQL Server están disponibles en SQL Managed Instance.

- **Considerar las características con ámbito de instancia.** Use características con ámbito de instancia de Azure SQL Managed Instance como Service Broker, CLR, Agente SQL Server y servidores vinculados. Migrar los datos relacionales y estructurados a Azure sin tener que rediseñar las aplicaciones.
- **Considerar la escalabilidad de la instancia.** Agregue escalabilidad a la instancia habilitando el modo de núcleos virtuales. Puede definir el número máximo de núcleos de CPU y el almacenamiento máximo de la instancia, por lo que todas las bases de datos de la instancia comparten los mismos recursos.

**SQL Server en Azure Virtual Machines** es una versión de SQL Server que se ejecuta en una máquina virtual de Azure. Este servicio permite usar versiones completas de SQL Server en la nube sin tener que administrar los equipos locales. Las máquinas virtuales de Azure tienen muchos tamaños y se pueden ejecutar en diversas regiones geográficas. Cada máquina virtual de SQL Server se puede crear para satisfacer requisitos de sistema operativo y versión específicos, lo que las convierte en una buena opción para controlar diferentes cargas de trabajo de SQL Server.

#### **Características de SQL Server en Azure Virtual Machines:**

- Si ejecuta SQL Server en Azure Virtual Machines, tendrá acceso a todas las funcionalidades de SQL Server.
- Todas sus aptitudes de SQL Server deben tener una equivalencia directa durante la migración, y Azure puede ayudarle a automatizar las tareas de copia de seguridad y revisiones de seguridad.
- A diferencia de las opciones de implementación de Azure SQL Database y Azure SQL Managed Instance, en este caso el usuario es quien tiene que encargarse de actualizar la versión del sistema operativo y SQL Server.

Comparación	SQL Database	Instancia administrada de SQL	SQL Server en Azure Virtual Machines
Escenarios	La mejor opción para las aplicaciones en la nube modernas, hiperescala o las configuraciones sin servidor	La mejor opción para la mayoría de las migraciones mediante lift-and-shift a las características de ámbito de instancia en la nube	La mejor opción para realizar migraciones rápidas y para aplicaciones que requieren un acceso de nivel de sistema operativo
Características	<p><b>Base de datos única</b></p> <ul style="list-style-type: none"> <li>- Almacenamiento de hiperescala (bases de datos de hasta 100 TB)</li> <li>- Proceso sin servidor</li> <li>- Servicio totalmente administrado</li> </ul> <p><b>Grupo elástico</b></p> <ul style="list-style-type: none"> <li>- Uso compartido de recursos entre varias bases de datos para la optimización de precios</li> <li>- Administración de rendimiento simplificada de varias bases de datos</li> <li>- Servicio totalmente administrado</li> </ul>	<p><b>Instancia única</b></p> <ul style="list-style-type: none"> <li>- Área expuesta de SQL Server (inmensa mayoría)</li> <li>- Redes virtuales nativas</li> <li>- Servicio totalmente administrado</li> </ul> <p><b>Grupo de instancias</b></p> <ul style="list-style-type: none"> <li>- Aprovisionamiento previo de los recursos de proceso para la migración</li> <li>- Migración rentable</li> <li>- Hospedaje de instancias más pequeñas (2vCore)</li> <li>- Servicio totalmente administrado</li> </ul>	<p><b>Azure Virtual Machines</b></p> <ul style="list-style-type: none"> <li>- Acceso a SQL Server</li> <li>- Acceso al servidor de nivel de sistema operativo</li> <li>- Compatibilidad exhaustiva con versiones de SQL Server</li> <li>- Compatibilidad exhaustiva con versiones del sistema operativo</li> <li>- Secuencia de archivos, Coordinador de transacciones distribuidas de Microsoft (DTC) y modelo de recuperación simple</li> <li>- SQL Server Integration Services (SSIS), SQL Server Reporting Services (SSRS) y SQL Server Analysis Services (SSAS)</li> </ul>

**Azure SQL Database** admite la escalabilidad dinámica. Esto es, los recursos asignados a las bases de datos (como la potencia de CPU, la memoria, el rendimiento de E/S y el almacenamiento) se pueden cambiar fácilmente con un tiempo de inactividad mínimo. Use Azure Portal para escalar una base de datos de Azure SQL sin cambiar la infraestructura existente ni comprar hardware nuevo.

#### Características de escalabilidad dinámica de una base de datos de Azure SQL:

- Elija modelos de DTU o de núcleo virtual y defina la cantidad máxima de recursos que se asignarán a cada base de datos con la implementación de una sola base de datos.
- Use grupo de bases de datos elásticas, adquiera recursos para el grupo y establezca los límites de recursos mínimo y máximo de las bases de datos que componen el grupo.
- Implemente el escalado vertical u horizontal:
  - **Vertical:** aumente o disminuya el tamaño de proceso de una base de datos individual.
  - **Horizontal:** agregue o quite bases de datos para ajustar la capacidad o el rendimiento general.
- Aplique el escalado horizontal bien mediante la partición de datos, bien mediante el aprovisionamiento de escalado horizontal de lectura.

Implemente el escalado vertical usando grupos de bases de datos elásticas de SQL Database. Las bases de datos de un grupo de bases de datos elásticas comparten los recursos asignados. El escalado vertical permite cambiar el tamaño de proceso de un conjunto de bases de datos. Cuando el promedio de uso es bajo, pero hay picos de uso elevado y poco frecuente, puede asignar suficiente capacidad en el grupo para administrar los picos.

Modelo de DTU	Modelo de núcleos virtuales
Niveles Básico, Estándar y Premium	Niveles De uso general y Crítico para la empresa

**El escalado horizontal** se administra con la biblioteca de cliente de la Base de datos elástica de SQL Database. Hay dos formas de aplicar escalado horizontal: mediante aprovisionamiento de escalado horizontal de lectura y mediante particionamiento.

- **Particionamiento:** particione los datos de un conjunto completo de bases de datos SQL que están estructuradas de forma idéntica. Un conjunto consta de una réplica principal de lectura y escritura y réplicas secundarias de solo lectura. Las bases de datos grandes se pueden dividir en componentes más pequeños para mejorar su rendimiento y que sean más fáciles de administrar.
- **Escalado horizontal de lectura:** aplique equilibrio de carga a las cargas de trabajo de solo lectura de un conjunto de bases de datos SQL. Descargue las cargas de trabajo de solo lectura mediante la capacidad de proceso de una réplica de solo lectura, en lugar de ejecutar cargas de trabajo en la réplica de lectura y escritura. Aíslle algunas cargas de trabajo de solo lectura de las cargas de trabajo de lectura y escritura sin afectar al rendimiento. En la siguiente tabla se muestra la compatibilidad con el aprovisionamiento de escalado horizontal de lectura en Azure SQL Database y Azure SQL Managed Instance:

Instancia administrada de Azure SQL	Azure SQL Database
Niveles Básico, Estándar y De uso general: el escalado horizontal de lectura no está disponible	Niveles Básico, Estándar y De uso general: el escalado horizontal de lectura no está disponible
Nivel Crítico para la empresa: el escalado horizontal de lectura se aprovisiona automáticamente.	Niveles Crítico para la empresa y Premium: el escalado horizontal de lectura se aprovisiona automáticamente.
Ningún nivel aplicable	Nivel Hiperescala: la escalabilidad horizontal de lectura está disponible si hay al menos una réplica secundaria creada.

Vamos a analizar un escenario empresarial de uso el escalado horizontal mediante particionamiento. Necesita resolver un problema de base de datos en una aplicación que accede a la base de datos que tiene un nivel alto de rendimiento de transacciones, hasta el punto de exceder la funcionalidad de la base de datos. Está buscando una manera de configurar el rendimiento y la disponibilidad de la base de datos. Una posible solución es el escalado horizontal, o la **creación de particiones horizontales mediante particionamiento**. Esta técnica distribuye grandes cantidades de datos estructurados de manera idéntica entre un conjunto de bases de datos independientes.

El particionamiento es útil en muchas situaciones. A continuación se muestran algunos ejemplos:

- La cantidad total de datos es demasiado grande para adaptarse a las restricciones de una única base de datos.
- El rendimiento de las transacciones de la carga de trabajo total supera las capacidades de una base de datos individual.
- Los datos de cada cliente o inquilino deben estar aislados físicamente entre sí.
- Dentro de una organización, hay una separación geográfica de datos por motivos de cumplimiento.

Los niveles Premium y Crítico para la empresa de Azure SQL Database y Azure SQL Managed Instance tienen un **grupo de disponibilidad Always On**. Este grupo es para la recuperación ante desastres y la alta disponibilidad de la aplicación. Hay una réplica principal de lectura y escritura y varias réplicas secundarias de solo lectura. Las réplicas secundarias se aprovisionan con el mismo tamaño de proceso que la réplica principal. Establezca la opción de la cadena de conexión para decidir si la conexión se enruta a la réplica de escritura o a una réplica de solo lectura.

Escenario	Solución de escalado
Administración y escalado de varias bases de datos de Azure SQL que tienen requisitos de recursos variables e impredecibles	Grupos de bases de datos elásticas y escalado vertical. Use grupos de bases de datos elásticas para asegurarse de que las bases de datos obtienen los recursos de rendimiento que necesitan cuando lo necesitan. Los grupos elásticos proporcionan un mecanismo de asignación de recursos simples dentro de un presupuesto predecible. No se realizan cargos por base de datos para los grupos elásticos. Se le cobra por cada hora que un grupo exista en la eDTU o los núcleos virtuales más altos, con independencia del uso o de si el grupo estuvo activo durante menos de una hora.
Diferentes secciones de una base de datos residen en diferentes ubicaciones geográficas por motivos de cumplimiento	Escalado horizontal y particionamiento. Use el particionamiento para dividir los datos en varias bases de datos y escalarlos de forma independiente. Shard Map Manager es una base de datos especial que mantiene la información de asignación global acerca de todas las particiones (bases de datos) de un conjunto de particiones. Los metadatos permiten a una aplicación conectarse a la base de datos correcta en función del valor de la clave de particionamiento.
Compatibilidad de dependencias de inteligencia empresarial comercial o herramientas de integración de datos, en las que varias bases de datos contribuyen a filas en un único resultado general para su uso en Excel, Power BI o Tableau	Herramientas de bases de datos elásticas y consultas elásticas. Use la característica de consulta elástica de herramientas de bases de datos elásticas para acceder a los datos distribuidos entre varias bases de datos. La consulta elástica está disponible en el nivel Estándar. Las consultas se pueden realizar en T-SQL, que abarca varias bases de datos en Azure SQL Database. Ejecute consultas entre bases de datos para acceder a tablas remotas y para conectar herramientas de Microsoft y de terceros (Excel, Power BI, Tableau, etc.) para realizar consultas entre capas de datos. Puede escalar consultas horizontalmente a capas de datos de gran tamaño y visualizar los resultados en informes de inteligencia empresarial.

Azure SQL proporciona distintos niveles de funcionalidades y opciones de disponibilidad de base de datos según los niveles de servicio. El nivel de servicio determina la arquitectura subyacente de la base de datos o instancia administrada que implemente.

Existen dos modelos de precios para las bases de datos de Azure SQL y las instancias administradas: **las unidades de transacción de base de datos** y **los núcleos virtuales**.

Las bases de datos SQL y las instancias administradas en el nivel de servicio De uso general (o Estándar) tienen la misma arquitectura de disponibilidad.

### **La arquitectura de disponibilidad del nivel De uso general (o nivel Estándar de DTU) de núcleo virtual:**

- La aplicación se conecta al nombre del servidor, que se conecta a una puerta de enlace **GW** que indica a la aplicación a qué servidor se debe conectar. La aplicación se ejecuta en una máquina virtual.
- En el nivel De uso general se usa el almacenamiento remoto. La réplica principal usa un disco SSD conectado localmente para la base de datos temporal, **tempdb**.
- Los archivos de datos y de registro se almacenan en Azure Premium Storage, que es el almacenamiento con redundancia local. Varias copias se almacenan en una zona de una región.
- Los archivos de copia de seguridad se almacenan en Azure Standard Storage, que, de forma predeterminada, es RA-GRS. Es un almacenamiento con redundancia global con copias en varias regiones.

Todo Azure SQL se basa en **Azure Service Fabric**, que actúa como la columna vertebral de Azure. Si Azure Service Fabric determina que es necesario realizar una comutación por error, este es similar a la de una instancia de clúster de comutación por error (FCI). Service Fabric busca un nodo con capacidad de reserva y pone en marcha una nueva instancia de SQL Server.

En el nivel Crítico para la empresa (o Premium), se suele lograr el rendimiento y disponibilidad máximos de todos los niveles de servicio Azure SQL. Este nivel está pensado para aplicaciones críticas que necesitan una latencia baja y un tiempo de inactividad mínimo.

### **La arquitectura de disponibilidad del nivel Crítico para la empresa de núcleo virtual (o nivel Premium de DTU):**

- La disponibilidad de la base de datos en el nivel de Crítico para la empresa es lo mismo a implementar un grupo de disponibilidad Always On en segundo plano.
- A diferencia del nivel De uso general, todos los archivos de datos y de registro se ejecutan en un disco SSD conectado directamente, lo que reduce significativamente la latencia de red.
- En este nivel hay tres réplicas secundarias. Una réplica secundaria se puede usar como punto de conexión de solo lectura (sin cargo extra). Una transacción puede completar una confirmación cuando al menos una réplica secundaria ha protegido el cambio de su registro de transacciones.

El nivel de **servicio Hiperescala** solo está disponible en Azure SQL Database. Este nivel de servicio tiene una arquitectura única porque emplea una capa por niveles de servidores de páginas y cachés para expandir la posibilidad de acceder rápidamente a páginas de bases de datos sin tener que acceder directamente al archivo de datos.

## La arquitectura de disponibilidad del nivel Hiperescala de núcleo virtual:

- En la arquitectura del nivel Hiperescala se usan servidores de página emparejados. Puede escalar horizontalmente para colocar todos los datos en capas en caché.
- La arquitectura de Hiperescala admite bases de datos de hasta 100 TB.
- En este nivel se usan instantáneas, lo que permite hacer copias de seguridad de base de datos casi instantáneas, independientemente del tamaño de la base de datos.
- Las restauraciones de bases de datos tardan minutos, en lugar de horas o días.
- Puede escalar o reducir verticalmente en tiempo constante para acomodar las cargas de trabajo.

Niveles de núcleo virtual de SQL Database	Niveles de DTU de SQL Managed	Compatibilidad de disponibilidad de base de datos
Uso general	Estándar o Básico	Proporciona opciones equilibradas de proceso y almacenamiento para cargas de trabajo empresariales.
Crítico para la empresa	Premium	Cumple los requisitos de baja latencia y permite la máxima resistencia a errores en las aplicaciones empresariales.
Hiperescala	Ningún nivel aplicable	Proporciona almacenamiento de gran escalabilidad y cumple los requisitos de escalado de lectura de las cargas de trabajo empresariales.

La clasificación de los datos almacenados por confidencialidad y escenario empresarial permite a las organizaciones determinar los riesgos inherentes a los datos.

Existen tres principios básicos para lograr una seguridad de la información adecuada: **detección, clasificación y protección de los datos**. En esta unidad, revisaremos diferentes estados de datos y métodos de cifrado para poner en práctica estos principios en una solución bien protegida.

Los datos pueden estar en tres estados básicos: **en reposo**, **en movimiento** y **en proceso**.

- Los **datos en reposo** son datos en un dispositivo de almacenamiento que no se están moviendo ni usando. Los datos en reposo pueden incluir mensajes de correo electrónico archivados almacenados en la bandeja de entrada de Outlook o los archivos de un portátil que no están en uso.
- Los **datos en movimiento** (también denominados *datos en tránsito*) son datos que se mueven de un dispositivo a otro dentro de una red privada o una red pública, como Internet. Los datos en movimiento también pueden ser datos que se están leyendo (usando), pero que no cambian. Los datos en movimiento pueden incluir mensajes de correo electrónico en tránsito, navegar por sitios web de Internet o usar aplicaciones de empresa como un organigrama.
- Los **datos en proceso** son datos que se han abierto y se están modificando. Los datos en proceso pueden incluir escribir un mensaje de correo electrónico, guardar los archivos de trabajo o hacer un pedido en un sitio web.

Estado de los datos	Encryption method	Nivel de cifrado
Datos en reposo	Cifrado de datos transparente (TDE)	Always Encrypted
Datos en movimiento	Capas de sockets seguros y Seguridad de la capa de transporte (SSL/TLS)	Always Encrypted
Datos en curso	Enmascaramiento de datos dinámicos	Los datos específicos no se cifran, los datos restantes sí se cifran.

Las organizaciones de gran tamaño, los gobiernos y las entidades militares usan la clasificación de datos para administrar la integridad de sus datos. El proceso de clasificación de datos ha resultado en atributos de metadatos comunes que nos permiten etiquetar los datos como *públicos*, *confidenciales* o *restringidos*. Una vez clasificados los datos, se pueden poner en marcha medidas de protección para datos muy confidenciales.

- El TDE cifra el almacenamiento de una base de datos completa mediante una clave simétrica denominada clave de cifrado de base de datos (DEK). TDE usa la DEK de dos formas:
  - **TDE administrado por el servicio:** la DEK está protegida por un certificado de servidor integrado.
  - **TDE administrado por el cliente:** el cliente es quien proporciona el protector de TDE que cifra la DEK. El protector de TDE se almacena en un sistema de administración de claves bajo propiedad y administración del cliente.

TDE se puede usar con bases de datos en un grupo de disponibilidad de **Always On**. Se debe hacer una copia de seguridad del certificado usado para cifrar la base de datos (y restaurarlo) en los demás servidores del grupo de disponibilidad que hospedan copias de la base de datos.

Azure SQL Database, Azure SQL Managed Instance y Azure Synapse Analytics usan siempre el cifrado de **Capa de sockets seguros** y **Seguridad de la capa de transporte (SSL/TLS)** en todas las conexiones. Esto nivel de cifrado garantiza que todos los datos se cifren "en tránsito" entre el cliente y el servidor. El protocolo Seguridad de capa de transporte (TLS) lo usan todos los controladores que Microsoft proporciona o admite para conectarse a bases de datos de Azure SQL Database o Instancia administrada de Azure SQL.

Escenario	Possible solución de seguridad
Proteger el acceso a una red virtual de Azure desde varias estaciones de trabajo situadas en el entorno local	Uso de VPN de sitio a sitio
Proteger el acceso a una red virtual de Azure desde una estación de trabajo situada en el entorno local	Uso de VPN de punto a sitio
Mover los conjuntos de datos grandes a través de un vínculo de red de área extensa (WAN) de alta velocidad dedicado	Uso de Azure ExpressRoute
Interactuar con Azure Storage a través de Azure Portal	Todas las transacciones se realizan mediante HTTPS. También se puede usar la API REST de Azure Storage a través de HTTPS para interactuar con Azure Storage y Azure SQL Database.

El cifrado de los datos en uso consiste en proteger los datos y la información confidencial mientras se usa o se cambia. Los métodos de cifrado tienen como destino escenarios de uso y el acceso mínimo necesario.

Los datos en uso emplean una característica de seguridad basada en directivas denominada **enmascaramiento dinámico de datos**. Esta característica oculta la información confidencial del conjunto de resultados de una consulta de campos designados de una base de datos, sin modificar los datos de esta última. El enmascaramiento dinámico de datos ayuda a impedir el acceso no autorizado a datos confidenciales, lo que permite a los usuarios designar la cantidad de los datos confidenciales que se revelarán con una repercusión mínima en el nivel de aplicación.

**Azure SQL Edge** es un motor de base de datos relacional optimizado orientado a implementaciones de IoT Edge. Azure SQL Edge se basa en el mismo motor que SQL Server y Azure SQL. Los desarrolladores con aptitudes de SQL Server pueden reutilizar su código para compilar soluciones específicas del perímetro en Azure SQL Edge. Azure SQL Edge proporciona funcionalidades para transmitir, procesar y analizar datos relacionales y no relacionales.

- Azure SQL Edge es una aplicación Linux contenedizada. La superficie de memoria de inicio es inferior a 500 MB.
  - Puede diseñar y compilar aplicaciones que se ejecutan en muchos dispositivos IoT. Capture flujos de datos continuos en tiempo real o integre datos en una solución de datos de la organización integral.
- 
- Acceda a un motor de streaming integrado como ayuda para obtener información de los flujos de datos.
    - Lleve a cabo tareas de transformación, agregación en ventanas, detección de anomalías simple y clasificación de los flujos de datos entrantes.
    - Use el almacenamiento de series temporales para los datos indexados por tiempo, que se pueden agregar y almacenar en la nube para analizarlos en el futuro.
  - Azure SQL Edge interactúa con los componentes del perímetro de red, incluidas puertas de enlace perimetrales, dispositivos IoT y servidores perimetrales.

Azure SQL Edge está disponible en dos ediciones que tienen conjuntos de características idénticos. Las ediciones ofrecen diferentes derechos de uso y la cantidad de memoria y núcleos accesibles en el sistema host.

Desarrollador de Azure SQL Edge	Azure SQL Edge
Cada contenedor de desarrollador de Azure SQL Edge está limitado a un máximo de cuatro núcleos y 32 GB de memoria.	Cada contenedor de Azure SQL Edge está limitado a un máximo de ocho núcleos y 64 GB de memoria.
Solo desarrollo	Producción

La seguridad es un problema principal al implementar aplicaciones de IoT en el perímetro. Dado que Azure SQL Edge se basa en SQL Server, una de las plataformas de base de datos más seguras disponibles, tiene las mismas características de seguridad que SQL Server Enterprise. Las mismas directivas y prácticas de seguridad se extienden de la nube al perímetro.

Para garantizar la protección de las implementaciones de Azure SQL Edge hay que realizar cuatro pasos:

1. **Seguridad del sistema y la plataforma.** Este paso de seguridad incluye el host físico de Docker, el sistema operativo del host y los sistemas de red que conectan el dispositivo físico a aplicaciones y clientes.
2. **Autenticación y autorización.** La autenticación SQL hace referencia a la autenticación de un usuario al conectarse a Azure SQL Edge con su nombre de usuario y contraseña. La autorización hace referencia a los permisos asignados a un usuario dentro de una base de datos en Azure SQL Edge.
3. **Seguridad de objetos de base de datos.** Los objetos de base de datos o *elementos protegibles* son el servidor, la base de datos y otros objetos de la base de datos. El cifrado mejora la seguridad. La protección de datos con cifrado de datos transparente (TDE) permite satisfacer muchas normativas de seguridad. "Always Encrypted" separa los usuarios que poseen los datos de los que los administran.
4. **Seguridad de aplicaciones.** Los procedimientos recomendados de seguridad de Azure SQL Edge incluyen la escritura de aplicaciones cliente seguras.

Azure SQL Edge presenta dos opciones de implementación:

- **Implementación conectada.** Para una implementación conectada, Azure SQL Edge está disponible en Azure Marketplace y se puede implementar como un módulo para Azure IoT Edge.
- **Implementación desconectada.** Una implementación desconectada se realiza a través de imágenes de contenedor de Azure SQL Edge. Estas imágenes se pueden extraer de Docker Hub e implementar como un contenedor de Docker independiente o en un clúster de Kubernetes.

**Azure Cosmos DB** es un servicio de bases de datos NoSQL totalmente administrado para el desarrollo de aplicaciones modernas. Como se trata de un servicio totalmente administrado, Azure Cosmos DB le libera de tener que administrar las bases de datos gracias a las funcionalidades de administración, actualizaciones y aplicación de revisiones automáticas. También controla la administración de la capacidad con opciones de escalado automático y sin servidor rentables que responden a las necesidades de la aplicación para hacer coincidir la capacidad con la demanda.

- Azure Cosmos DB tiene tiempos de respuesta de milisegundos de un solo dígito y una velocidad garantizada a cualquier escala.
- Las aplicaciones que se escriben para Azure Table Storage pueden migrarse a Table API de Azure Cosmos DB con pocos cambios de código.
- Table API de Azure Cosmos DB y Table Storage comparten el mismo modelo de datos de tablas y exponen las mismas operaciones de creación, eliminación, actualización y consulta a través de sus SDK.

Característica	Azure Table Storage	Table API de Azure Cosmos DB
Latency	Rápido, pero no hay límites máximos en la latencia.	Latencia de milisegundos de un solo dígito para lecturas y escrituras, con respaldo de < lecturas de latencia de 10 ms y <escrituras de latencia de 15 ms en el percentil 99, a cualquier escala y en cualquier lugar del mundo.
Rendimiento	Modelo de rendimiento variable. Las tablas tienen un límite de escalabilidad de 20 000 operaciones.	Altamente escalable con rendimiento reservado dedicado por tabla respaldado por los SLA. Las cuentas no tienen ningún límite superior de rendimiento y admiten > 10 millones de operaciones por segundo y por tabla (en modo de rendimiento aprovisionado).
Distribución global	Una sola región, con una región de lectura secundaria legible opcional para alta disponibilidad.	Distribución global inmediata desde 1 a más de 30 regiones.
Indexación	Índice principal solo en PartitionKey y RowKey. No hay índices secundarios.	Indexación automática y completa en todas las propiedades, sin administración de índices.
Consultar	La ejecución de consultas usa el índice de la clave principal y, en caso contrario, examina.	Las consultas pueden aprovechar la indexación automática en las propiedades para reducir el tiempo de consulta.
Coherencia	Seguro dentro de la región principal.	Cinco niveles de coherencia bien definidos para compensar la disponibilidad, la latencia, el rendimiento y la coherencia.
Precios	Modelo de precios basado en el consumo	Disponible en los modelos de precios tanto de capacidad aprovisionada como basados en el consumo.
SLA	Disponibilidad del 99,99 %	Acuerdo de Nivel de Servicio con disponibilidad del 99,99 % para todas las cuentas de una sola región y todas las cuentas de varias regiones con coherencia moderada, y disponibilidad de lectura del 99,999 % para todas las cuentas de base de datos de varias regiones.

**Azure Data Factory** es un servicio de integración de datos basado en la nube que ayuda a crear y programar flujos de trabajo controlados por datos. Puede usar Azure Data Factory para orquestar el movimiento de datos y transformar los datos a escala. Los flujos de trabajo controlados por datos, o *canalizaciones*, ingieren datos de almacenes de datos dispares. Azure Data Factory es un proceso de integración de datos ETL (extracción, transformación y carga de datos). Este proceso de integración combina datos de varios orígenes de datos en un único almacén de datos.

Hay cuatro pasos principales para crear e implementar un flujo de trabajo controlado por datos en la arquitectura de Azure Data Factory:

1. **Conectar y recopilar.** En primer lugar, ingiera los datos para recopilar todos los datos de distintos orígenes en una ubicación centralizada.
2. **Transformar y enriquecer.** Posteriormente, transforme los datos mediante un servicio de proceso como Azure Databricks y Azure HDInsight Hadoop.
3. **Proporcionar integración continua y entrega continua (CI/CD), y publicación.** Admita CI/CD mediante el uso de GitHub y Azure DevOps para entregar el proceso ETL de forma incremental antes de publicar los datos en el motor de análisis.
4. **Supervisión.** Finalmente, usar Azure Portal para supervisar la canalización para las actividades programadas y para los errores.

Azure Data Factory tiene los siguientes componentes que funcionan conjuntamente para proporcionar la plataforma para el movimiento y la integración de datos.

- **Canalizaciones y actividades:** las canalizaciones proporcionan una agrupación lógica de actividades que realizan una tarea. Una actividad es un único paso de procesamiento en una canalización. Azure Data Factory admite el movimiento de datos, la transformación de datos y las actividades de control.
- **Conjuntos de datos:** los conjuntos de datos son estructuras de datos dentro de los almacenes de datos.
- **Servicios vinculados:** los servicios vinculados definen la información de conexión necesaria para que Azure Data Factory se conecte a recursos externos.
- **Flujos de datos:** los flujos de datos permiten a los ingenieros de datos desarrollar lógica de transformación de datos sin necesidad de escribir código. Las actividades de flujo de datos pueden ponerse en marcha mediante las capacidades de programación, control, flujo y supervisión existentes de Azure Data Factory.
- **Entornos de ejecución de integración:** los entornos de ejecución de integración sirven de puente entre la actividad y los objetos de servicios vinculados. Hay tres tipos de entornos de ejecución de integración: Azure, auto hospedado y Azure-SSIS.

**Un lago de datos** es un repositorio de datos que se almacenan en su formato natural, normalmente como blobs o archivos. **Azure Data Lake Storage** es una solución de lago de datos completa, escalable y rentable para el análisis de macrodatos integrada en Azure. Azure Data Lake Storage combina un sistema de archivos con una plataforma de almacenamiento para ayudar a identificar rápidamente conclusiones en los datos. La solución se basa en funcionalidades de Azure Blob Storage para proporcionar optimizaciones para cargas de trabajo de análisis. Esta integración habilita las funcionalidades de rendimiento de análisis, alta disponibilidad, seguridad y durabilidad de Azure Storage.

## **Características Azure Data Lake Storage:**

- Azure Data Lake Storage puede almacenar cualquier tipo de datos usando el formato nativo de estos datos. Gracias a la compatibilidad con cualquier formato de datos y tamaños de datos masivos, Azure Data Lake Storage puede trabajar con datos estructurados, semiestructurados y no estructurados.
- La solución está diseñada principalmente para trabajar con Hadoop y todos los marcos que usan Sistema de archivos distribuido (HDFS) de Apache Hadoop como capa de acceso a los datos. Los marcos de análisis de datos que usan HDFS como capa de acceso a datos pueden acceder directamente.
- Azure Data Lake Storage admite alto rendimiento para el movimiento de datos y los análisis que precisan de muchas entradas y salidas.
- El modelo de control de acceso de Azure Data Lake Storage admite el control de acceso basado en roles de Azure y las listas de control de acceso (ACL) de Portable Operating System Interface for Unix (POSIX).
- Azure Data Lake Storage utiliza modelos de replicación de blobs de Azure. Estos modelos proporcionan redundancia de datos en un único centro de datos con almacenamiento con redundancia local (LRS).
- Azure Data Lake Storage ofrece almacenamiento masivo y acepta numerosos tipos de datos para el análisis.
- El precio de Azure Data Lake Storage se establece en los niveles de Azure Blob Storage.

Hay tres pasos importantes para usar Azure Data Lake Storage:

1. **Ingesta de datos.** Azure Data Lake Storage ofrece muchos métodos distintos de ingestión de datos:
  - Para los datos no planeados, puede usar herramientas como AzCopy, la CLI de Azure, PowerShell y Explorador de Azure Storage.
  - En el caso de los datos relacionales, se puede usar el servicio Azure Data Factory. Puede transferir datos desde cualquier origen, como Azure Cosmos DB, SQL Database, instancias administradas de Azure SQL, etc.
  - Para los datos de streaming, puede usar herramientas como Apache Storm en Azure HDInsight, Azure Stream Analytics, etc.
2. **Acceso a los datos almacenados.** La manera más fácil de acceder a los datos es usar Explorador de Azure Storage. Explorador de Storage es una aplicación independiente con una interfaz gráfica de usuario (GUI) para acceder a los datos de Azure Data Lake Storage. También puede usar PowerShell, la CLI de Azure, la CLI de HDFS u otros SDK de lenguaje de programación para acceder a los datos.
3. **Configuración del control de acceso.** Controle quién puede acceder a los datos almacenados en Azure Data Lake Storage mediante la implementación de un mecanismo de autorización. Puede elegir Azure RBAC o ACL.

*Provisión de un almacenamiento de datos en la nube para administrar grandes volúmenes de datos.*

Azure Data Lake Storage se ejecuta en hardware virtual en la plataforma Azure. El almacenamiento es escalable, rápido y confiable sin incurrir en cargos masivos. Separa los costos de almacenamiento de los costos de proceso. A medida que crece el volumen de datos, solo cambian los requisitos de almacenamiento.

*Admite una colección variada de tipos de datos, como archivos JSON, CSV, archivos de registro u otros formatos diversos.*

Azure Data Lake Storage habilita la democratización de datos para su organización mediante el almacenamiento de todos los formatos de datos (incluidos los datos sin procesar) en una sola ubicación. La eliminación de silos de datos permite a los usuarios usar herramientas como Azure Data Explorer para acceder a todos los elementos de datos de su cuenta de almacenamiento y trabajar con ellos.

*Possibilidad de almacenamiento e ingestión de datos en tiempo real.*

Azure Data Lake Storage puede ingerir datos en tiempo real directamente desde una instancia de Apache Storm en Azure HDInsight, Azure IoT Hub, Azure Event Hubs o Azure Stream Analytics. También funciona con datos semiestructurados y permite ingerir todos los datos en tiempo real en la cuenta de almacenamiento.

Comparación	Azure Data Lake	Azure Blob Storage
Tipos de datos	Conveniente para almacenar grandes volúmenes de datos de texto	Adecuado para almacenar datos no estructurados no basados en texto, como fotos, vídeos y copias de seguridad
Redundancia geográfica	Debe configurar manualmente la replicación de datos	De forma predeterminada, proporciona almacenamiento con redundancia geográfica
Espacios de nombres	Compatibilidad con espacios de nombres jerárquicos	Compatibilidad con espacios de nombres planos
Compatibilidad con Hadoop	Los servicios de Hadoop pueden usar datos almacenados en Azure Data Lake	Con Azure Blob Filesystem Driver, las aplicaciones y los marcos pueden acceder a los datos en Azure Blob Storage
Seguridad	Admite el acceso pormenorizado	No admite el acceso pormenorizado

**Azure Databricks** es una plataforma de macrodatos y aprendizaje automático totalmente administrada y basada en la nube, que permite a los desarrolladores acelerar la inteligencia artificial y la innovación. Azure Databricks proporciona a los equipos de ingeniería y ciencia de datos una sola plataforma para el procesamiento de macrodatos y el aprendizaje automático. La plataforma Apache Spark administrada de Azure Databricks facilita la ejecución de cargas de trabajo de Spark a gran escala. Azure Databricks se basa completamente en **Apache Spark** y es una excelente herramienta para los usuarios que ya están familiarizados con el marco de informática de clúster de código abierto.

Azure Databricks tiene un plano de control y un plano de datos:

- **Plano de control:** hospeda trabajos de Databricks, cuadernos con resultados de consulta y el administrador de clústeres. El plano de control también tiene la aplicación web, el repositorio metastore de Hive y listas de control de acceso de seguridad (ACL) y sesiones de usuario. Microsoft administra estos componentes en colaboración con Azure Databricks, y estos no residen en la suscripción de Azure.
- **Plano de datos:** contiene todos los clústeres de tiempo de ejecución de Azure Databricks hospedados en el área de trabajo. Todo el procesamiento y el almacenamiento de datos existen en la suscripción local. No se produce ningún procesamiento de datos en la suscripción administrada por Microsoft o Databricks.

Azure Databricks ofrece tres entornos para desarrollar aplicaciones que consumen muchos datos.

- **Databricks SQL:** Azure Databricks SQL proporciona una plataforma fácil de usar para los analistas que quieren ejecutar consultas SQL en su lago de datos. Permite crear varios tipos de visualización para explorar los resultados de las consultas desde diferentes perspectivas, así como crear y compartir paneles.
- **Ingeniería y ciencia de datos de Databricks:** Ingeniería y ciencia de datos de Databricks es un *área de trabajo* interactiva que permite la colaboración entre ingenieros de datos, científicos de datos e ingenieros de aprendizaje automático. Para una canalización de macrodatos, los datos (estructurados o sin formato) se ingieren en Azure mediante Azure Data Factory en lotes o transmitidos casi en tiempo real con Apache Kafka, Azure Event Hubs o Azure IoT Hub. Los datos llegan a un lago de datos para un almacenamiento persistente a largo plazo en Azure Blob Storage o Azure Data Lake Storage. Como parte del flujo de trabajo de análisis, use Azure Databricks para leer datos de varios orígenes de datos y convertirlos en información importante mediante Spark.
- **Databricks Machine Learning:** Azure Databricks Machine Learning es un entorno integrado de aprendizaje automático de un extremo a otro. Incorpora servicios administrados para el seguimiento de experimentos, el entrenamiento de modelos, el desarrollo y la administración de características, y el servicio de características y modelos.

**Azure Synapse Analytics** combina características de análisis de macrodatos, almacenamiento de datos empresariales e integración de datos. El servicio le permite ejecutar consultas en datos o datos sin servidor a escala. Azure Synapse admite la ingestión de datos, la exploración, la transformación y la administración, y admite el análisis de todas las necesidades de inteligencia empresarial y aprendizaje automático.

**Azure Synapse Analytics** implementa una arquitectura de procesamiento paralelo masivo (MPP) y tiene las siguientes características.

- La arquitectura de Azure Synapse Analytics incluye un *nodo de control* y un grupo de *nodos de ejecución*.

El nodo de control es el cerebro de la arquitectura. Es el front-end que interactúa con todas las aplicaciones. Los nodos de proceso proporcionan la eficacia de cálculo. Los datos que se van a procesar se distribuyen uniformemente entre los nodos.

- Las consultas se envían en forma de instrucciones Transact-SQL y Azure Synapse Analytics las ejecuta.
- Azure Synapse usa una tecnología denominada PolyBase que permite recuperar y consultar datos de orígenes relacionales y no relacionales.

Puede guardar los datos leídos como tablas SQL en el servicio Azure Synapse.

### Azure Synapse Analytics se compone de cinco elementos:

- **Grupo de Azure Synapse SQL:** Synapse SQL ofrece modelos de recursos dedicados y sin servidor con los que trabajar con la arquitectura basada en nodos. Para obtener un rendimiento y un costo predecibles, puede crear grupos de SQL dedicados. En el caso de cargas de trabajo irregulares o no planificadas, puede usar el punto de conexión SQL sin servidor siempre disponible.
- **Grupo de Azure Synapse Spark:** este grupo es un clúster de servidores que ejecutan Apache Spark para procesar datos. Para escribir la lógica de procesamiento de datos, se usa uno de los cuatro lenguajes admitidos: Python, Scala, SQL y C# (a través de .NET para Apache Spark). Apache Spark para Azure Synapse integra el motor de macrodatos de código abierto de Apache Spark, que se usa para la preparación de datos, la ingeniería de datos, ETL y el aprendizaje automático.
- **Canalizaciones de Azure Synapse:** las canalizaciones de Azure Synapse aplican las funcionalidades de Azure Data Factory. Las canalizaciones son un servicio de integración de datos y ETL basado en la nube que le permite crear flujos de trabajo orientados a datos a fin de coordinar el movimiento y la transformación de datos a escala. Puede incluir actividades que transformen los datos a medida que se transfieran o combinar los datos de varios orígenes.
- **Azure Synapse Link:** este componente permite conectarse a Azure Cosmos DB. Se puede usar para realizar análisis casi en tiempo real de los datos operativos almacenados en una base de datos de Azure Cosmos DB.
- **Azure Synapse Studio:** este elemento es un IDE basado en Web que se puede usar de forma centralizada para trabajar con todas las funcionalidades de Azure Synapse Analytics. Puede usar Azure Synapse Studio para crear grupos de SQL y Spark, definir y ejecutar canalizaciones, y configurar vínculos a orígenes de datos externos.

<i>Descriptivo</i>	¿Qué pasa?	Azure Synapse aplica la funcionalidad de grupo de SQL dedicado, que permite crear un almacenamiento de datos persistente para analizar <i>qué va a suceder</i> posteriormente. Puede usar el grupo de SQL sin servidor a fin de preparar los datos de los archivos almacenados en un lago de datos para crear un almacenamiento de datos de forma interactiva.
<i>Diagnostic</i>	¿Por qué está sucediendo?	Puede usar la funcionalidad de grupo de SQL sin servidor en Azure Synapse para explorar de forma interactiva los datos de un lago de datos. Los grupos de SQL sin servidor permiten de forma rápida que un usuario busque datos adicionales que puedan ayudarle a comprender <i>por qué</i> sucede algo.
<i>Predictivo</i>	¿Qué es probable que suceda?	Azure Synapse Analytics usa su motor de Apache Spark integrado y grupos de Azure Synapse Spark para el análisis predictivo. Combina esta acción con otros servicios, como Azure Machine Learning Services y Azure Databricks, para ayudarle a obtener respuestas sobre <i>qué sucederá en el futuro</i> .
<i>Prescriptivo</i>	¿Qué hay que hacer?	Puede usar datos prescriptivos en tiempo real o casi en tiempo real para ayudarle a identificar soluciones para las <i>acciones necesarias</i> . Azure Synapse Analytics proporciona esta funcionalidad tanto mediante Apache Spark como de Azure Synapse Link, y mediante la integración de tecnologías de streaming como Azure Stream Analytics.

**Una ruta** de datos de acceso medio admite el análisis de datos a medida que fluye a través del sistema. El flujo de datos se procesa casi en tiempo real. Los datos se guardan en el almacenamiento intermedio y se insertan en los clientes de análisis.

- La plataforma Azure proporciona muchas opciones para procesar los eventos, y una opción popular es Azure Stream Analytics.
- Stream Analytics puede ejecutar análisis complejos a escala para ventanas de saltos de tamaño constante, ventanas deslizantes y ventanas de salto. El servicio admite la ejecución de agregaciones de flujos y la combinación de orígenes de datos externos. Para un procesamiento complejo, el rendimiento se puede ampliar mediante el procesamiento en cascada de varias instancias de Azure Event Hubs, trabajos de Stream Analytics y Azure Functions.
- El almacenamiento intermedio se puede implementar con varios servicios en la plataforma Azure, como Azure SQL Database y Azure Cosmos DB.

**La ruta de datos de acceso medio** es donde se produce el procesamiento de la secuencia para descubrir patrones a lo largo del tiempo. Sin embargo, es posible que tenga que calcular el uso durante algún período de tiempo en el pasado. También es posible que necesite diferentes áreas dinámicas y agregaciones, y que necesite fusionar estos resultados con los resultados de la ruta de datos de acceso medio para presentar una vista unificada al usuario. Una ruta de datos de acceso esporádico puede ayudar a realizar estas tareas.

- Una ruta de datos de acceso esporádico consta de una capa por lotes y capas de servicio que proporcionan una vista a largo plazo del sistema.
- La capa por lotes crea vistas de agregados calculados previamente para permitir respuestas rápidas a consultas durante largos períodos. La plataforma Azure proporciona diversas opciones tecnológicas para esta capa.
- La ruta de datos de acceso esporádico incluye un almacén de datos a largo plazo para la solución y Azure Storage es un enfoque común. Azure Storage incluye Azure Blobs (objetos), Azure Data Lake Storage Gen2, Azure Files, Azure Queues y Azure Tables.
- El almacenamiento en frío puede producirse en Blobs, Data Lake Storage Gen2, Azure Tables, o una combinación de ellos.
- Para almacenar grandes cantidades de datos no estructurados, las mejores opciones son Blob Storage, Azure Files o Azure Data Lake Storage Gen2. El almacenamiento de rutas de datos de acceso esporádico es ideal para los mensajes originales que contienen datos no procesados recibidos por las aplicaciones de IoT.

**La ruta de datos de acceso frecuente** se usa normalmente para procesar o mostrar datos en tiempo real. Esta ruta de acceso se emplea para las operaciones de streaming y alertas en tiempo real. Una ruta de datos de acceso frecuente es donde están los datos sensibles a la latencia, donde los resultados deben estar listos en segundos o menos y donde fluyen para un consumo rápido por parte de los clientes de análisis.

*Compatibilidad flexible con los requisitos de datos que cambian con frecuencia. Permite procesar o mostrar datos en tiempo real.*

Ruta de datos de acceso frecuente

*Admite datos que rara vez se usan, como los datos almacenados por motivos legales o de cumplimiento. Permite el consumo de datos para el análisis a largo plazo y el procesamiento por lotes.*

Ruta de datos de acceso esporádico

*Almacena o muestra un subconjunto reciente de datos. Permite el consumo de datos para el procesamiento por lotes y análisis pequeños.*

Ruta de datos de acceso medio

El proceso de consumir flujos de datos, analizarlos y derivar información procesable se denomina **procesamiento de flujos**. **Azure Stream Analytics** es un motor de procesamiento de eventos complejos y de análisis en tiempo real totalmente administrado (oferta de PaaS). Ofrece la posibilidad de realizar análisis en tiempo real de varios flujos de datos procedentes de orígenes como datos de dispositivos IoT, sensores, secuencias de clics y fuentes de redes sociales.

Azure Stream Analytics sirve para los siguientes conceptos:

- **Flujos de datos:** los flujos de datos son datos continuos generados por aplicaciones, dispositivos IoT o sensores. Los flujos de datos se analizan y se extrae información útil. Algunos ejemplos son la supervisión de flujos de datos de equipos industriales y de fabricación y la supervisión de los datos de canalización de agua por parte de proveedores de servicios públicos. Los flujos de datos ayudan a comprender el cambio con el tiempo.
- **Procesamiento de eventos:** hace referencia al consumo y análisis de un flujo de datos continuo para extraer información útil de los eventos que se producen dentro del flujo. Un ejemplo es un automóvil que pasa a través de una cabina de peaje, que debe incluir información temporal, como una marca de tiempo que indica cuándo se produjo el evento.

Un trabajo de Azure Stream Analytics consta de una entrada, una consulta y una salida. Puede hacer las tareas siguientes con la salida del trabajo:

- Enrutar los datos a sistemas de almacenamiento, como Azure Blob Storage, Azure SQL Database, Azure Data Lake Store y Azure Cosmos DB.
- Enviar datos a Power BI para la visualización en tiempo real.
- Almacenar datos en un servicio de Data Warehouse, como Azure Synapse Analytics, para entrenar un modelo de aprendizaje automático basado en datos históricos o realizar análisis por lotes.
- Desencadenar flujos de trabajo de bajada personalizados mediante el envío de los datos a servicios como Azure Functions, temas de Azure Service Bus o colas de Azure.

<i>Análisis de los flujos de telemetría en tiempo real desde dispositivos IoT.</i>	Recopile datos del sensor en tiempo real en Azure Stream Analytics mediante la creación de sistemas de automatización que retransmitan la temperatura, la humedad y los entornos de ejecución del ventilador. Puede realizar ajustes para mantener la temperatura óptima del edificio y reducir los costos.
<i>Creación de registros web y análisis de secuencias de clics.</i>	Un minorista de bienes de consumo puede ofrecer sugerencias de productos en tiempo real a los usuarios en función del análisis de comercio electrónico.
<i>Creación de análisis geoespaciales.</i>	Prepare análisis de orígenes de datos geoespaciales, como sensores, redes sociales, imágenes satélite y dispositivos móviles. Puede predecir eventos meteorológicos extremos, como incendios forestales y huracanes, para ayudar a las aerolíneas en sus planificaciones de rutas. Puede enviar alertas móviles a los clientes para detectar condiciones meteorológicas adversas en función de su geolocalización.
<i>Ejecución remota y mantenimiento predictivo de activos de gran valor.</i>	Supervise activos de alto valor, como equipos industriales, mediante la recopilación de datos operativos en Azure Stream Analytics. Puede maximizar la vida útil de su equipo a través del mantenimiento predictivo. Los datos recopilados desde transformadores de energía eléctrica pueden ser utilizados por empresas de servicios públicos para evitar la interrupción del funcionamiento.
<i>Ánalisis en tiempo real de datos de puntos de venta.</i>	Detecte transacciones fraudulentas de tarjetas de crédito e identifique la actividad sospechosa en el punto de venta. Puede detectar transacciones inusualmente elevadas o actividad en alguna ubicación inusual en función de la información de contacto del titular de la tarjeta de crédito. Los desencadenadores de alertas se pueden configurar para los datos recopilados en Azure Stream Analytics.

## AZ-305: Diseño de soluciones de infraestructura

Azure ofrece varios servicios de proceso. **Proceso** hace referencia al modelo de hospedaje para los recursos informáticos en los que las aplicaciones se ejecutan.

- **Azure Virtual Machines:** implemente y administre máquinas virtuales dentro de una red virtual de Azure.
- **Azure Batch:** aplique este servicio administrado para ejecutar aplicaciones de informática en paralelo y de alto rendimiento (HPC) a gran escala.
- **Azure App Service:** hospede aplicaciones web, back-end de aplicaciones móviles, API RESTful o procesos empresariales automatizados con este servicio administrado.
- **Azure Functions:** use este servicio administrado para ejecutar código en la nube, sin preocuparse por la infraestructura.
- **Azure Logic Apps:** configure esta *plataforma* basada en la nube para crear y ejecutar flujos de trabajo automatizados similares a las funcionalidades de Azure Functions.
- **Azure Container Instances:** ejecute contenedores en Azure de forma rápida y sencilla sin crear máquinas virtuales ni depender de un servicio de nivel superior.
- **Azure Kubernetes Service (AKS):** ejecute aplicaciones en contenedor con este servicio de Kubernetes administrado.

Al planear nuevas instancias de servicios de Azure y nuevas cargas de trabajo, tenga en cuenta los siguientes escenarios.

- **Control:** determine si necesita un control total sobre el software y las aplicaciones instalados.
- **Cargas de trabajo:** tenga en cuenta las cargas de trabajo que necesita admitir, como **las cargas de trabajo de HPC** o **las cargas de trabajo controladas por eventos**.
- **Arquitectura:** piense en qué arquitectura admite mejor su infraestructura, incluida la de **microservicio**, la **orquestación completa** y **sin servidor**.

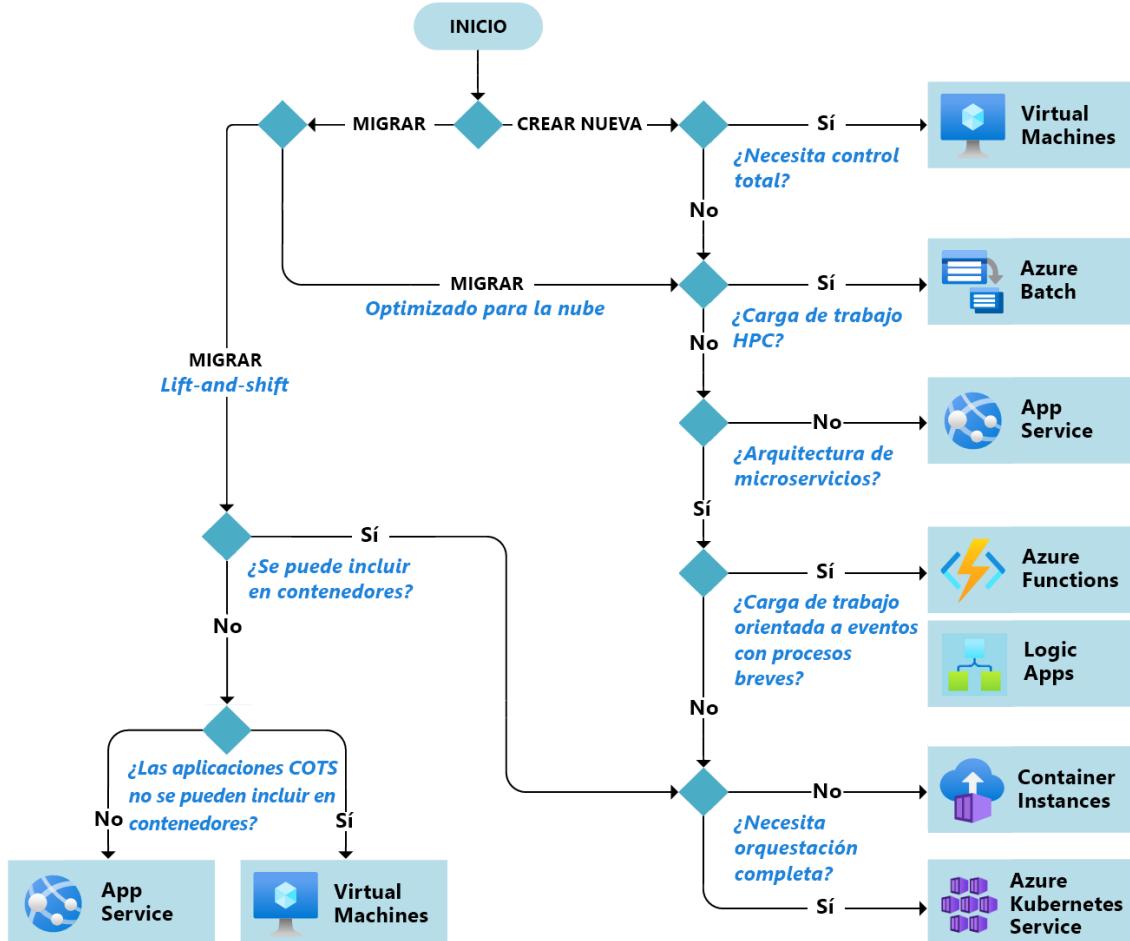
Una consideración importante para el servicio de proceso implica analizar las funcionalidades de migración.

- **Optimizada para la nube:** para migrar a la nube y refactorizar las aplicaciones para acceder a características nativas de la nube, considere la posibilidad de usar servicios de proceso optimizados para la nube.
- Lift and shift: en el caso de las migraciones de cargas de trabajo de **lift-and-shift**, tenga en cuenta los servicios de proceso que no requieren rediseños de aplicaciones ni cambios en el código.
- **En contenedores:** en el planeamiento de la migración, tenga en cuenta si el servicio de proceso necesita admitir aplicaciones en contenedores o aplicaciones comerciales (COTS).

**La opción de hospedaje** de la solución de proceso determina las responsabilidades del desarrollador y del proveedor de nube. Azure ofrece tres opciones de hospedaje en los servicios de proceso.

- La **infraestructura como servicio (IaaS)** permite crear máquinas virtuales individuales junto con los componentes de red y almacenamiento asociados. A continuación, puede implementar el software y las aplicaciones que quiera en esas máquinas virtuales. Este modelo es lo más parecido a un entorno local tradicional, salvo que Microsoft administra la infraestructura. El usuario sigue administrando las máquinas virtuales individuales. Azure Virtual Machines ofrece hospedaje IaaS.
- **Plataforma como servicio (PaaS)** proporciona un entorno de hospedaje administrado en el que puede implementar la aplicación sin necesidad de administrar las máquinas virtuales o los recursos de red. Los servicios de proceso de Azure que ofrecen hospedaje PaaS incluyen Azure Batch, App Service, Container Instances y Azure Kubernetes Service.
- Las **funciones como servicio (FaaS)** van más allá al eliminar la necesidad de preocuparse por el entorno de hospedaje. En un modelo de FaaS, se implementa el código y el servicio lo ejecuta automáticamente. Azure Functions y Logic Apps ofrecen hospedaje FaaS.

Azure proporciona un **diagrama de flujo** de decisión con instrucciones de alto nivel sobre cómo seleccionar el servicio de proceso de Azure adecuado para su escenario.



Las **máquinas virtuales de Azure** son la base del modelo de infraestructura como servicio (IaaS) de Azure. Virtual Machines puede usarse para desarrollar, probar e implementar aplicaciones en la nube, o para ampliar el centro de datos. Virtual Machines ofrece una manera rápida, escalable y flexible de agregar más capacidad de proceso a su empresa.

Hay dos escenarios principales en los que Azure Virtual Machines puede ser una solución de proceso ideal para una infraestructura. Virtual Machines se puede usar para **crear nuevas cargas de trabajo y migrar datos mediante el patrón lift-and-shift**.

- **Creación de nuevas cargas de trabajo:** Azure Virtual Machines es ideal cuando se crean nuevas cargas de trabajo y la demanda de las aplicaciones puede fluctuar. Es mas económico ejecutar las aplicaciones en una máquina virtual en Azure.
- **Migración mediante lift-and-shift:** si usa la migración mediante lift-and-shift (rehospedaje) para trasladar datos y aplicaciones desde una ubicación local, tener Azure Virtual Machines como destino en la nube es una estrategia eficaz.

Hay otros dos puntos que hay que tener en cuenta sobre la ubicación de la máquina virtual.

- La ubicación de la máquina puede limitar las opciones disponibles. Cada región tiene un hardware diferente disponible y algunas configuraciones no están disponibles en todas las regiones.
- Hay diferencias de precio entre las ubicaciones. Para buscar la opción más rentable, compruebe la configuración necesaria en distintas regiones.

Clasificación	Descripción	Escenarios
De uso general	Los tamaños de máquina virtual de uso general están diseñados para proporcionar una relación equilibrada entre CPU y memoria.	- Pruebas y desarrollo - Bases de datos pequeñas a medianas - Servidores web de tráfico bajo a medio
Optimizada para proceso	Las máquinas virtuales optimizadas para proceso están diseñadas para proporcionar una relación alta entre CPU y memoria.	- Servidores web de tráfico medio - Dispositivos de red - Procesos por lotes - Servidores de aplicaciones
Optimizada para memoria	Las máquinas virtuales optimizadas para memoria están diseñadas para proporcionar una relación alta entre memoria y CPU.	- Servidores de bases de datos relacionales - Cachés medianas a grandes - Análisis en memoria
Optimizada para almacenamiento	Las máquinas virtuales optimizadas para almacenamiento están diseñadas para tener un alto rendimiento de disco y E/S.	- Máquinas virtuales que ejecutan bases de datos
GPU	Las máquinas virtuales de GPU son máquinas virtuales especializadas específicas para la representación de gráficos pesados y la edición de vídeo.	- Entrenamiento e inferencia de modelos con aprendizaje profundo
Informática de alto rendimiento	Las de informática de alto rendimiento ofrecen las máquinas virtuales de CPU más rápidas y potentes con interfaces de red de alto rendimiento opcionales.	- Cargas de trabajo que requieren un rendimiento rápido - Redes de tráfico elevado

En una suscripción se facturan dos costos independientes por cada máquina virtual: **proceso** y **almacenamiento**. Al separar estos costos, los puede escalar por separado y pagar solo por lo que necesita.

- **Costos de proceso:** los gastos de proceso tienen un precio por horas, pero se facturan por minutos. Si la máquina virtual se implementa durante 55 minutos, solo se le cobrarán 55 minutos de uso. No se le cobrará por la capacidad de proceso si detiene y desasigna la máquina virtual. El precio por horas varía en función del tamaño de máquina virtual y del sistema operativo que seleccione.
- **Costos de almacenamiento:** se le cobra por separado por el uso de la máquina virtual de Azure Storage. El estado de la máquina virtual no tiene relación con los cargos de Azure Storage en los que se incurre. Siempre se le cobra por cualquier instancia de Azure Storage que usen los discos.

**Azure Managed Disks** controla la creación y administración de cuentas de almacenamiento de Azure en segundo plano. Especifique el tamaño del disco y el nivel de rendimiento (Estándar o Premium). Azure crea y administra el disco. Al agregar discos o escalar y reducir la máquina virtual no tendrá que preocuparse por el almacenamiento que se va a usar.

**Azure Batch** ejecuta aplicaciones a gran escala y de forma eficaz en la nube. Puede programar tareas de proceso intensivo y ajustar dinámicamente los recursos de la solución sin administrar la infraestructura. Azure Batch puede crear y administrar un grupo de nodos de ejecución (máquinas virtuales). Azure Batch también puede instalar la aplicación que desea ejecutar y programar trabajos para que se ejecuten en los nodos de ejecución. Azure Batch es similar a Azure Virtual Machines y se puede usar para crear nuevas cargas de trabajo y migrar datos.

- Azure Batch funciona bien con aplicaciones que se ejecutan de forma independiente (cargas de trabajo paralelas).
- Azure Batch es eficaz para las aplicaciones que necesitan comunicarse entre sí (cargas de trabajo estrechamente acopladas). Puede usar Batch para compilar un servicio que ejecute una simulación de Monte Carlo para una empresa de servicios financieros o un servicio que procese imágenes.
- Azure Batch permite trabajo por lotes paralelos a gran escala y de informática de alto rendimiento (HPC) con la capacidad de escalar a decenas, cientos o miles de máquinas virtuales. Cuando esté listo para ejecutar un trabajo, Azure Batch:
  - Iniciará un grupo de máquinas virtuales de proceso de forma automática.
  - Instalará aplicaciones y datos de almacenamiento provisional.
  - Ejecutará trabajos con tantas tareas como tenga.
  - Identifica los errores, vuelve a poner en cola el trabajo y reduce verticalmente el grupo a medida que se completa el trabajo.

- **El servicio** usa Azure como plataforma. La plataforma se usa para completar el trabajo de proceso intensivo y para recuperar los resultados. También puede supervisar los trabajos y el progreso de las tareas.
- **Azure Batch funciona como la plataforma de proceso subyacente al servicio.** Batch usa Azure Storage para capturar las aplicaciones o los datos necesarios para completar una tarea. Azure Batch escribe la salida en Azure Storage. En segundo plano, hay colecciones (grupos) de máquinas virtuales. Los grupos son los recursos en los que se ejecutan los trabajos y las tareas.

**Azure App Service** es un servicio basado en HTTP que permite compilar y hospedar aplicaciones web, trabajos en segundo plano, back-end móviles y API RESTful. Puede usar el lenguaje de programación que prefiera y crear implementaciones automatizadas desde GitHub, Azure DevOps o cualquier repositorio de Git. App Service ofrece escalado automático y alta disponibilidad.

- Azure App Service es un entorno de plataforma como servicio (PaaS). Se centra en el desarrollo del sitio web y la lógica de API. Azure controla la infraestructura para ejecutar y escalar las aplicaciones web.
- App Service admite el desarrollo en varios lenguajes y marcos, y ofrece una implementación y administración integradas con puntos de conexión protegidos.
- App Service ofrece equilibrio de carga integrado y administración del tráfico a escala global con alta disponibilidad.
- App Service proporciona funcionalidades integradas de autenticación y autorización (a veces denominadas *Autenticación sencilla*). Puede iniciar la sesión de los usuarios y acceder a los datos escribiendo poco o ningún código.

**Las máquinas virtuales** son una excelente manera de reducir los costos en comparación con las inversiones necesarias para el hardware físico. Sin embargo, cada máquina virtual todavía está limitada a un único sistema operativo. Los contenedores son una excelente opción si quiere ejecutar varias instancias de una aplicación en un solo equipo host. **Azure Container Instances** es una solución rápida y sencilla para ejecutar un contenedor en Azure. Los escenarios del uso de Azure Container Instance incluyen aplicaciones sencillas, automatización de tareas y trabajos de compilación.

**Azure Container Instances** ofrece muchas ventajas, como el inicio rápido, la facturación por segundo y el almacenamiento persistente. Estas ventajas hacen que Azure Container Instances sea una excelente solución de proceso para admitir nuevas cargas de trabajo y migrar datos mediante el patrón lift-and-shift.

- Azure Container Instances permite el inicio rápido. Puede iniciar contenedores en cuestión de segundos para obtener acceso inmediato a las aplicaciones.
- Azure Container Instances implementa la facturación por segundo. Solo se generan gastos mientras se ejecuta el contenedor.
- Azure Container Instances admite tamaños personalizados para los contenedores. Puede especificar valores exactos para núcleos de CPU y memoria y evitar costos de recursos no utilizados.
- Container Instances ofrece almacenamiento persistente. Los recursos compartidos de Azure Files pueden montarse directamente en un contenedor para recuperar y conservar el estado.
- Container Instances se puede usar con Linux y Windows. Programe contenedores Windows y Linux con la misma API

El recurso de nivel superior de Azure Container Instances es el **grupo de contenedores**.

**Un grupo de contenedores** es una colección de contenedores que se programan en la misma máquina host. Los contenedores de un grupo comparten un ciclo de vida, los recursos, la red local y los volúmenes de almacenamiento.

Los grupos de varios contenedores son útiles cuando quiere dividir una sola tarea funcional en varias imágenes de contenedor. Luego, estas imágenes las pueden entregar diferentes equipos y pueden tener diversos requisitos de recursos. Algunos escenarios de ejemplo son:

- Un contenedor para servir una aplicación web y un contenedor para extraer el contenido más reciente desde el control de código fuente.
- Un contenedor de aplicación y un contenedor de registro. El contenedor de registro recopila la salida de registros y métricas de la aplicación principal y los escribe en un almacenamiento a largo plazo.
- Un contenedor de aplicación y un contenedor de supervisión. El contenedor de supervisión realiza una solicitud a la aplicación periódicamente para asegurarse de que se está ejecutando y responde correctamente, y genera alertas si fuera necesario.
- Un contenedor de front-end y un contenedor de back-end. El front-end puede servir una aplicación web y el back-end, ejecutar un servicio para recuperar datos.

**Usar un registro privado.** Los contenedores se crean a partir de imágenes que están almacenadas en uno o varios repositorios. Estos repositorios pueden pertenecer a un registro público o a un registro privado. Un ejemplo de un registro privado es el Registro de confianza de Docker, que puede instalarse de forma local o en una nube privada virtual. Otro ejemplo es Azure Container Registry que se puede usar para compilar, almacenar y administrar artefactos e imágenes de contenedor.

**Garantice la integridad de la imagen a lo largo del ciclo de vida.** Parte de la administración de la seguridad a lo largo del ciclo de vida del contenedor es garantizar la integridad de las imágenes de contenedor. No se debe permitir que las imágenes con vulnerabilidades, aunque sean de menor importancia, se ejecuten en un entorno de producción. Mantenga un número pequeño de imágenes de producción para asegurarse de que se puedan administrar eficazmente.

**Supervisar la actividad de los recursos de contenedor.** Supervise la actividad de los recursos, como archivos, red y otros recursos, a los que acceden los contenedores. Supervisar el consumo y la actividad de los recursos resulta útil para la supervisión de rendimiento y como medida de seguridad.

Comparación	Azure Container Instances	Azure Virtual Machines
Aislamiento	Container Instances normalmente proporciona aislamiento ligero del host y otros contenedores, pero no proporciona un límite de seguridad tan sólido como el de una máquina virtual.	Una máquina virtual proporciona un aislamiento completo del sistema operativo host y otras máquinas virtuales. El aislamiento es útil cuando un límite de seguridad elevado es crítico, como el hospedaje de aplicaciones de empresas de la competencia en el mismo servidor o clúster.
Sistema operativo	Container Instances ejecuta la parte del modo de usuario de un sistema operativo y se puede personalizar para que contenga solo los servicios necesarios para la aplicación. Esta configuración da lugar a que se usen menos recursos del sistema.	Cada máquina virtual ejecuta un sistema operativo completo. Azure Virtual Machines normalmente requiere más recursos del sistema que Container Instances, como CPU, memoria y almacenamiento.
Implementación	Container Instances implementa contenedores individuales mediante Docker desde la línea de comandos. Se pueden implementar varios contenedores mediante un orquestador como Azure Kubernetes Service.	Puede implementar máquinas virtuales individuales mediante Windows Admin Center o el administrador de Hyper-V. Se pueden implementar varias máquinas virtuales mediante PowerShell o System Center Virtual Machine Manager.
Almacenamiento persistente	Container Instances usa Azure Disks para el almacenamiento local para un único nodo, o bien Azure Files (recursos compartidos SMB) para el almacenamiento compartido por varios nodos o servidores.	Con Azure Virtual Machines, puede usar un disco duro virtual (VHD) para el almacenamiento local de una sola máquina virtual o un recurso compartido de archivos SMB para el almacenamiento compartido por varios servidores.
Tolerancia a errores	Si se produce un error en un nodo de clúster en Azure Container Instances, el orquestador vuelve a crear rápidamente los contenedores que se ejecutan en él en otro nodo del clúster.	Una máquina virtual pueden conmutar por error a otro servidor de un clúster, y el sistema operativo de la máquina virtual se reinicia en el nuevo servidor.

**Kubernetes** es una plataforma de código abierto portátil y extensible para automatizar la implementación, el escalado y la administración de cargas de trabajo contenedorizadas. Esta plataforma de orquestación ofrece la misma facilidad de uso y flexibilidad que las ofertas de plataforma como servicio (PaaS) e infraestructura como servicio (IaaS). Kubernetes proporciona **administración y orquestación de contenedores**.

La administración de contenedores es el proceso de organización, adición, eliminación o actualización de un número significativo de contenedores. **La orquestación de contenedores** es un sistema que implementa y administra automáticamente aplicaciones contenedorizadas. El orquestador puede aumentar o disminuir dinámicamente las instancias implementadas de la aplicación administrada.

**Azure Kubernetes Service (AKS)** administra su entorno hospedado de Kubernetes y facilita la implementación y administración de aplicaciones en contenedores en Azure.

- Azure administra el clúster de Kubernetes de forma gratuita. Administre los nodos del agente en el clúster y pague solo por las máquinas virtuales en las que se ejecutan los nodos.
- Al crear el clúster, puede usar plantillas de Azure Resource Manager (ARM) para automatizar su creación. Con las plantillas de ARM, se especifican características como las redes avanzadas, la integración de Microsoft Entra y la supervisión.
- AKS proporciona las ventajas de Kubernetes de código abierto. No tiene la complejidad ni la sobrecarga operativa que ejecuta su propio clúster de Kubernetes personalizado.

Característica	Consideración	Solución
Administración de las identidades y la seguridad	<i>¿Ya usa los recursos de Azure existentes y Microsoft Entra ID?</i>	Puede configurar un clúster de Azure Kubernetes Service para que se integre con Microsoft Entra ID y reutilizar las identidades y la pertenencia a grupos existentes.
Registro y supervisión integrados	<i>¿Usa Azure Monitor?</i>	Azure Monitor ofrece la visibilidad del rendimiento del clúster.
Escalado automático de pods y nodos de clústeres	<i>¿Necesita escalar o reducir verticalmente un entorno de contenedorización grande?</i>	AKS admite dos opciones de escalado automático de clústeres. El <i>escalador automático horizontal del pod</i> supervisa la demanda de recursos de pods y aumenta los pods para que se ajusten a la demanda. El <i>escalador automático de clúster</i> busca pods que no puedan programarse debido a restricciones de los nodos. Escala automáticamente los nodos de clúster para implementar pods programados.
Actualizaciones del nodo de clúster	<i>¿Quiere reducir el número de tareas de administración de los clústeres?</i>	AKS administra las actualizaciones de software de Kubernetes y el proceso de acordonar los nodos y purgarlos.
Compatibilidad con volúmenes de almacenamiento	<i>¿La aplicación requiere almacenamiento persistente?</i>	AKS admite volúmenes de almacenamiento estáticos y dinámicos. Los pods se pueden adjuntar y volver a adjuntar a estos volúmenes de almacenamiento a medida que se crean o se reprograman en nodos distintos.
Compatibilidad con redes virtuales	<i>¿Necesita una comunicación de red de pod a pod o acceso a redes locales desde el clúster de AKS?</i>	Un clúster de AKS se puede implementar en una red virtual existente con facilidad.
Compatibilidad con la entrada con el enrutamiento de aplicación HTTP	<i>¿Necesita que las aplicaciones implementadas estén disponibles públicamente?</i>	El complemento de enrutamiento de aplicación HTTP facilita el acceso a las aplicaciones implementadas del clúster de AKS.
Compatibilidad con imágenes de Docker	<i>¿Ya usa las imágenes de Docker para los contenedores?</i>	De manera predeterminada, AKS es compatible con el formato de imagen del archivo de Docker.
Registro de contenedor privado	<i>¿Necesita un registro de contenedor privado?</i>	AKS se integra con Azure Container Registry (ACR). Sin embargo, no está limitado a ACR, ya que puede usar otros repositorios de contenedor, sean públicos o privados.

**Azure Functions** es una plataforma de aplicaciones sin servidor. Functions se usa cuando es necesario ejecutar un pequeño fragmento de código en la nube, sin tener que preocuparse por la infraestructura.

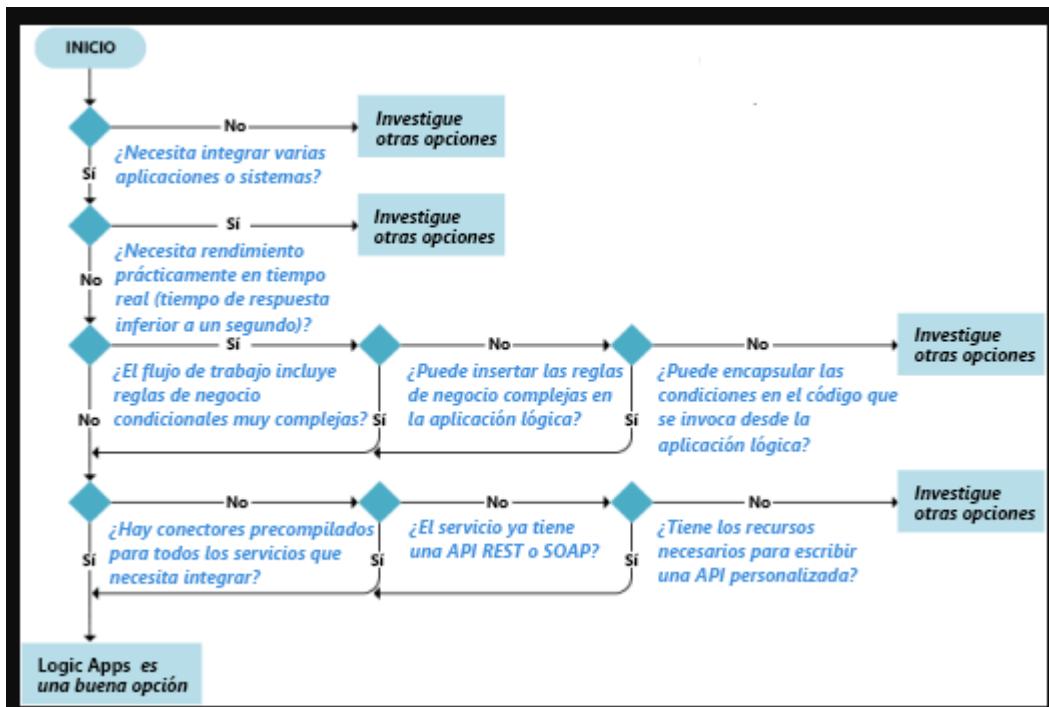
- Azure Functions proporciona escalabilidad intrínseca. Solo se le cobrarán los recursos que use.
- Con Azure Functions, puede escribir el código de función en el lenguaje que prefiera.
- Azure Functions admite *el proceso a petición* de dos maneras significativas:
  - Azure Functions permite implementar la lógica del sistema en bloques de código fácilmente disponibles. Estos bloques de código (funciones) se pueden ejecutar siempre que necesite responder a eventos críticos.
  - A medida que aumentan las solicitudes, Azure Functions satisface la demanda con tantos recursos e instancias de función como sean necesarios. A medida que se completan las solicitudes, los recursos y las instancias de aplicación adicionales se entregan automáticamente.
- Azure Functions es una solución ideal cuando se administran acciones definibles específicas desencadenadas por un evento. Una función puede procesar una llamada API y almacenar los datos procesados en Azure Cosmos DB. Una vez que se produce la transferencia de datos, otra función puede desencadenar una notificación.

**Azure Logic Apps** es otro tipo de solución de proceso sin servidor que ofrece una plataforma basada en la nube para crear y ejecutar *flujos de trabajo* automatizados. Los flujos de trabajo son procesos paso a paso que integran las aplicaciones, los datos, los servicios y los sistemas. Con Azure Logic Apps, puede desarrollar rápidamente soluciones de integración de alta escalabilidad para sus escenarios de negocio a negocio (B2B).

- Azure Logic Apps es un componente de Azure Integration Services. Logic Apps simplifica la forma de conectar sistemas heredados, modernos y de vanguardia entre entornos híbridos, locales y en la nube.
- Con Logic Apps, puede programar y enviar notificaciones por correo electrónico mediante Office 365 cuando se produzca un evento específico, como la carga de un nuevo archivo.
- Use Logic Apps para enrutar y procesar pedidos de clientes en sistemas locales y servicios en la nube.
- Implemente Logic Apps para mover archivos cargados desde un servidor SFTP o FTP a Azure Storage.
- Supervise tuits, análisis de opiniones con Logic Apps, y cree alertas o tareas para los elementos que se deben revisar

Azure Logic Apps es similar a Azure Functions como servicio de proceso, pero hay diferencias básicas. Azure Functions es una tecnología **orientada al código** que usa funciones duraderas. Azure Logic Apps es una tecnología **orientada al diseño**.

Comparación	Azure Functions	Azure Logic Apps
Desarrollo	Orientado al código	Diseño primero
Método	Escrutura de código y uso de la extensión Durable Functions	Creación de orquestaciones con una GUI o mediante la edición de archivos de configuración
Conectividad	- Amplia selección de tipos de enlaces integrados - Escritura de código para enlaces personalizados	- Gran colección de conectores - Enterprise Integration Pack para escenarios B2B - Creación de conectores personalizados
Supervisión	Azure Application Insights	Azure Portal, registros de Azure Monitor (Log Analytics)



Su primera decisión en el diseño de la arquitectura de la aplicación es planear cómo se comunicarán los componentes de la aplicación. Definir la estrategia de componentes le ayuda a elegir el servicio de Azure adecuado. La mayoría de los componentes de la aplicación se comunican mediante el envío de mensajes o eventos. Azure ofrece varios servicios para admitir las diferentes estrategias de comunicación.

Examinemos las características de **mensajes**.

- Los mensajes contienen datos sin procesar generados por un componente y consumidos por otro componente.
- Un mensaje contiene los datos, no solo una referencia a esos datos.

En una comunicación de mensajes, el componente emisor espera que los datos del mensaje sean procesados de una manera determinada por el componente de destino. La integridad del sistema global puede depender de que tanto el emisor como el receptor realicen un trabajo específico.

Ahora echemos un vistazo con más detalle a **eventos**.

- Los eventos pesan algo menos que los mensajes y son los que se usan con más frecuencia para difundir comunicaciones.
- Un evento tiene dos componentes, un *publicador* y *suscriptores*. El publicador de eventos envía el evento. Los suscriptores de eventos reciben eventos.

**Los eventos tienen las siguientes características:**

- Un evento es una notificación ligera que indica que ha ocurrido algo.
- Un evento puede enviarse a varios receptores o a ninguno.
- Un publicador de eventos no tiene expectativas sobre las acciones por parte de un componente receptor.
- A menudo, se pretende que un evento "efectúe una distribución ramificada" o tenga muchos suscriptores para cada editor.
- Un evento es una unidad discreta que no está relacionada con otros eventos, pero un evento podría formar parte de una serie relacionada y ordenada.

Azure ofrece dos soluciones basadas en mensajes, que son Azure Queue Storage y Azure Service Bus. Queue Storage almacena un gran número de mensajes en Azure Storage. Service Bus es un agente de mensajes que desacopla las aplicaciones y los servicios. Examinaremos las diferentes características y funcionalidades de estos servicios y consideraremos cómo elegir qué servicio implementar.

**Azure Event Hubs** es una plataforma de streaming de macrodatos totalmente administrada y un servicio de ingestión de eventos. Vamos a revisar las características del servicio:

- Azure Event Hubs admite la ingesta de datos en tiempo real y el procesamiento por lotes de microservicios en la misma secuencia.
- Puede enviar y recibir eventos en muchos lenguajes diferentes. También se pueden recibir mensajes de los Azure Event Hubs utilizando Apache Storm.
- Los eventos recibidos por Azure Event Hubs se agregan al final de su flujo de datos.
  - El flujo de datos ordena eventos según la hora en que se recibe el evento.
  - Los consumidores pueden buscar a lo largo del flujo de datos mediante desplazamientos de tiempo.
- Event Hubs implementa un modelo de *extracción* que lo diferencia de otros servicios de mensajería, como las colas de Azure Service Bus.
  - Event Hubs mantiene cada mensaje en su caché y permite su lectura.
  - Cuando un mensaje se lee desde Event Hubs, no se elimina. El mensaje permanece para otros consumidores.
- Event Hubs no tiene un mecanismo integrado para controlar los mensajes que no se procesan según lo previsto.
- Azure Event Hubs escala según el número de unidades de rendimiento (procesamiento) adquiridas. Las características de rendimiento varían para cada plan de tarifa, como Básica, Estándar o Premium.

**Una arquitectura controlada por eventos** permite conectarse a la aplicación principal sin necesidad de modificar el código existente. Cuando se produce un evento, puede reaccionar con código específico para responder al evento. Una aplicación controlada por eventos usa el principio de **enviar y olvidar**. Un evento se envía hacia el siguiente sistema, que puede ser otro servicio, un centro de eventos, una secuencia o un agente de mensajes.

Cuando se carga un nuevo vídeo de revisión o demostración de productos, es necesario notificar a todas las aplicaciones móviles en dispositivos de usuario de todo el mundo que están interesados en los productos. Azure **Event Grid** es una solución ideal para este requisito.

- El publicador de la revisión o el vídeo no necesita saber sobre los suscriptores interesados en los productos afectados.
- Queremos tener una relación de uno a varios donde podamos tener varios suscriptores. Los suscriptores pueden decidir opcionalmente si están interesados en los productos afectados.

**Azure Event Grid** es un servicio de enrutamiento de eventos totalmente administrado que se ejecuta en Azure Service Fabric. Event Grid está pensado para facilitar la compilación de aplicaciones basadas en eventos y sin servidor en Azure. Examine las siguientes características del servicio.

- Azure Event Grid agrega todos los eventos y proporciona enrutamiento desde cualquier origen hasta cualquier destino.
  - Event Grid distribuye eventos desde orígenes como cuentas de Azure Blob Storage y Azure Media Services.
  - Los eventos se distribuyen a controladores como Azure Functions y Webhooks de Azure DevOps.
  - El servicio administra el enrutamiento y la entrega de eventos de muchos orígenes. La administración ayuda a minimizar el coste y la latencia eliminando la necesidad de sondear.
- 
- Un origen de eventos, como Azure Blob Storage etiqueta los eventos con uno o más temas, y envía los eventos a Azure Event Grid.
  - Un controlador de eventos como Azure Functions se suscribe a temas en los que están interesados.
  - Event Grid examina las etiquetas de los temas para decidir qué eventos enviar a qué controladores.
  - Event Grid reenvía eventos relevantes a los suscriptores.
  - Event Grid envía un evento para indicar que algo ha sucedido o cambiado. Sin embargo, el objeto real que se cambió (archivo de texto, vídeo, audio, etc.) no forma parte de los datos del evento. En su lugar, Event Grid pasa una URL o un identificador para hacer referencia al objeto modificado.

Servicio de Azure	Propósito	Mensaje o evento	Escenario de uso
Azure Event Grid	Programación reactiva	Distribución de eventos (discretos)	<i>Reacción ante los cambios de estado</i>
Azure Event Hubs	Canalización de macrodatos	Streaming de eventos (serie)	<i>Realización de datos de telemetría y streaming de datos distribuidos</i>
Azure Service Bus	Mensajería empresarial de gran valor	Message	<i>Realización del procesamiento de pedidos y transacciones financieras</i>

El **almacenamiento en caché** es una técnica que tiene como objetivo mejorar el rendimiento y la escalabilidad de un sistema. El almacenamiento en caché copia temporalmente los datos a los que se accede con frecuencia en un almacenamiento rápido situado cerca de la aplicación. Cuando el almacenamiento rápido de datos está situado más cerca de una aplicación que su almacén de datos original, el almacenamiento en caché puede mejorar significativamente los tiempos de respuesta de las aplicaciones cliente al servir los datos más rápidamente.

El almacenamiento en caché es más eficaz cuando una instancia de cliente lee de forma repetida los mismos datos, en especial cuando todas las condiciones siguientes se aplican al almacén de datos original:

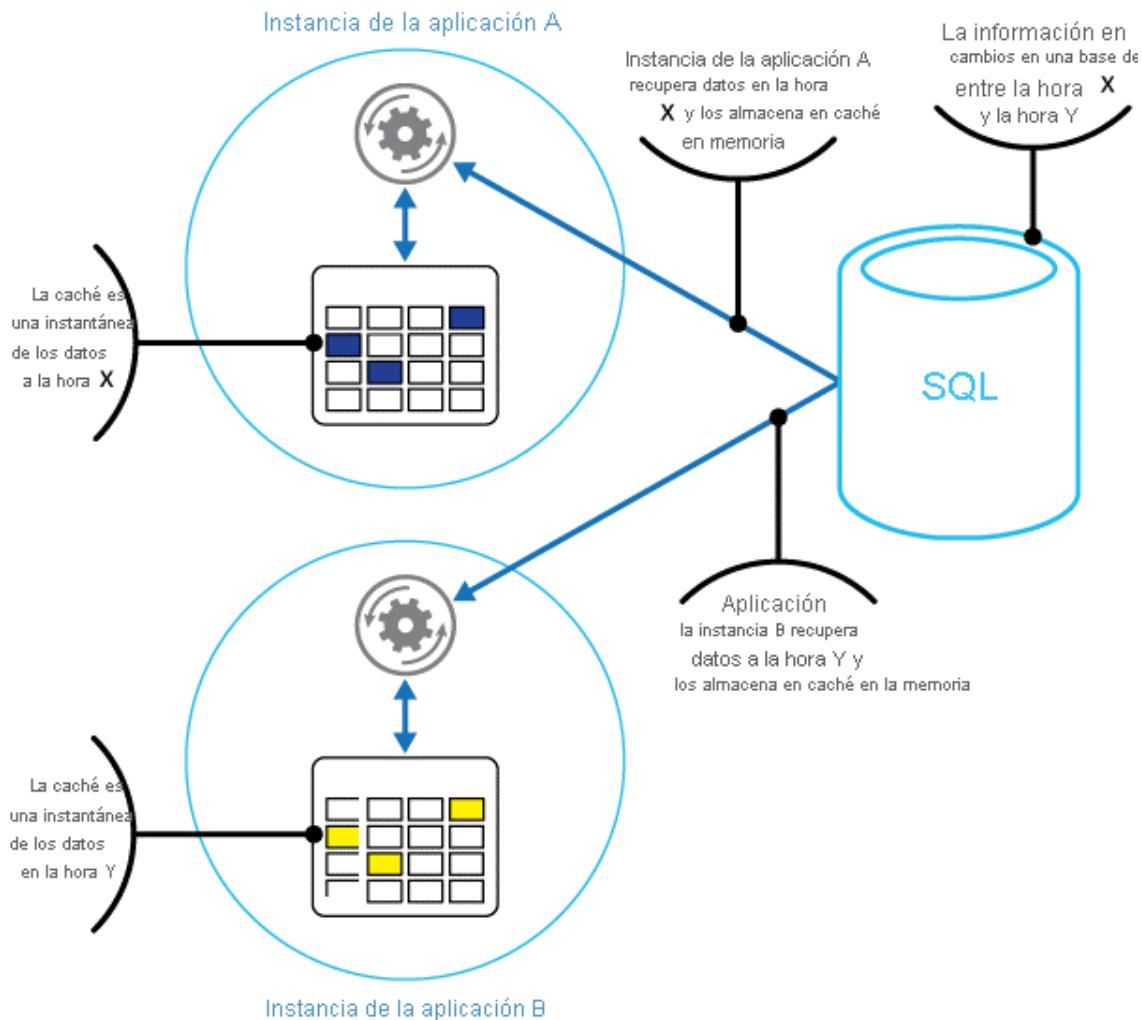
- El almacén de datos original permanece relativamente estático.
- Es lento en comparación con la velocidad de la caché.
- Está sujeto a un alto nivel de contención.
- Está lejos y la latencia de red puede dar lugar a un acceso lento al almacén.

**Azure Cache for Redis** proporciona un almacén de datos en memoria basado en el software de Redis. Redis mejora el rendimiento y la escalabilidad de una aplicación que use en gran medida los almacenes de datos de back-end. Es capaz de procesar grandes volúmenes de solicitudes de aplicación al mantener los datos a los que se accede con frecuencia en la memoria del servidor, donde se pueden realizar operaciones rápidas de lectura y escritura. Redis incorpora una solución crítica de almacenamiento de datos de baja latencia y alto rendimiento en las aplicaciones modernas.

Vamos a revisar las características del servicio:

- Azure Cache for Redis ofrece dos opciones de implementación para desarrolladores:
  - Código abierto de Redis (Redis de OSS)
  - Un producto comercial de Redis Labs (Redis Enterprise) como servicio administrado
- Azure Cache for Redis proporciona instancias de servidor Redis seguras y dedicadas y compatibilidad total con la API de Redis.
- Puede usar Azure Cache for Redis como caché de datos o contenidos distribuidos, almacén de sesiones o agente de mensajes.
- Implemente Azure Cache for Redis como independiente o con otros servicios de base de datos de Azure, como Azure SQL o Azure Cosmos DB.

Microsoft ofrece Azure Cache for Redis, que se hospeda en Azure, y cualquier aplicación de dentro o fuera de Azure pueden usarlo. En la ilustración siguiente se muestra cómo funciona Azure Cache for Redis en las aplicaciones.



La instancia de aplicación A tiene una memoria caché con una instantánea de los datos en el momento X. Recupera datos a la vez X y los almacena en caché en memoria. La instancia de aplicación B tiene una memoria caché con una instantánea de los datos en el momento Y. Recupera datos a la vez Y y los almacena en caché en memoria. La información de la base de datos SQL cambia entre el tiempo X y la hora Y.

Modelo	Escenario	Solución
Caché de datos	<i>Las bases de datos suelen ser demasiado grandes para cargarlas directamente en una caché.</i>	Es habitual usar el patrón <i>cache-aside</i> para cargar datos en la memoria caché solo cuando es necesario. Cuando el sistema realiza cambios en los datos, también puede actualizar la caché, que se distribuye luego a otros clientes. Además, el sistema puede establecer una fecha de expiración en los datos o usar una directiva de expulsión para desencadenar las actualizaciones de los datos en la memoria caché.
Caché de contenido	<i>Muchas páginas web se generan a partir de plantillas que usan contenido estático como encabezados, pies de página y banners. Estos elementos estáticos no deberían cambiar a menudo.</i>	El uso de una caché en memoria proporciona acceso rápido a contenido estático en comparación con los almacenes de datos de back-end. Este patrón reduce el tiempo de procesamiento y la carga del servidor, y permite que los servidores web tengan mayor capacidad de respuesta. Un caché de contenidos puede permitirle reducir el número de servidores necesarios para administrar las cargas. Azure Cache for Redis proporciona el proveedor de caché de salida de Redis, que admite este patrón con ASP.NET.
Almacén de sesión	<i>Un almacén de sesiones se usa normalmente con carros de la compra y otros datos de historial del usuario que una aplicación web puede querer asociar con las cookies del usuario. El almacenamiento de demasiados datos en una cookie puede tener un efecto negativo en el rendimiento, ya que aumenta su tamaño y no hay que olvidar que se pasa y se valida con cada solicitud.</i>	Una solución habitual usa la cookie como clave cuando se consultan datos en una base de datos. Es más rápido utilizar una caché en memoria como Azure Cache for Redis para asociar la información a un usuario que interactuar con una base de datos relacional completa.
Almacenamiento en cola de trabajos y mensajes	<i>Algunas operaciones de aplicación tardan mucho tiempo en completarse, lo que podría impedir que se inicien otros trabajos o mensajes no relacionados.</i>	Las aplicaciones agregan a menudo tareas a una cola cuando las operaciones asociadas a la solicitud tardan tiempo en ejecutarse. Las operaciones con ejecuciones más largas se ponen en cola para procesarse en secuencia, a menudo por parte de otro servidor. Este método de aplazar trabajo se denomina <i>puesta en cola de tareas</i> . Azure Cache for Redis proporciona una cola distribuida que habilita este patrón en la aplicación.
Transacciones distribuidas	<i>A veces, las aplicaciones requieren una serie de comandos en un almacén de datos de back-end para ejecutarse como una única operación atómica. Todos los comandos deben ejecutarse correctamente o revertirse al estado inicial.</i>	Azure Cache for Redis admite la ejecución de un lote de comandos como transacción única.

**La publicación de una API** es una excelente manera de aumentar la cuota de mercado, generar ingresos y fomentar la innovación. Sin embargo, mantener incluso una API supone importantes desafíos, como la incorporación de usuarios, la administración de revisiones y la implementación de la seguridad.

La red troncal del nuevo servicio es una gran colección de API publicadas, algunas de las cuales se usan en las siguientes entidades:

- Aplicación móvil de Tailwind Traders y sitio web en línea
- Dispositivos IoT en los vehículos de reparto
- Especialistas en productos de proveedor
- Equipos de desarrollo internos de Tailwind Traders
- Los empleados de Tailwind Traders, como los analistas de negocios

Cada API publicada reside en un servidor diferente. Cada API tiene su propio proceso para incorporar usuarios y sus propias directivas de seguridad, revisiones, análisis, etc. Busca una solución de Azure que pueda ayudar a reducir esta complejidad.

**Azure API Management** es una plataforma de servicios en la nube que le permite publicar, proteger, mantener y analizar todas las API. En el diagrama siguiente se muestra cómo Azure API Management actúa como puerta principal para las API de una organización y las enruta al servidor donde se implementan las API.

Las **plantillas de Azure Resource Manager (ARM)** son archivos que definen la infraestructura y la configuración de la implementación. Al escribir una plantilla de ARM, se toma un enfoque declarativo para el aprovisionamiento de recursos. Las plantillas de ARM describen cada recurso de la implementación, pero no cómo implementar los recursos.

- Las plantillas de ARM son *idempotentes*, lo que significa que puede implementar repetidamente la misma plantilla y obtener el mismo resultado.
- Cuando se envía una implementación de plantilla de ARM a Azure Resource Manager, los recursos de la plantilla de ARM se implementan en paralelo. Este proceso de características de orquestación permite que las implementaciones finalicen más rápido.
- El parámetro `WhatIf` disponible en PowerShell y en la CLI de Azure le permite obtener una vista previa de los cambios en el entorno antes de implementar la plantilla de ARM. Este parámetro detalla las creaciones, modificaciones y eliminaciones que realizará la plantilla.
- Las plantillas de ARM enviadas a Resource Manager se validan antes del proceso de implementación. Esta validación le avisa de los errores de la plantilla antes del aprovisionamiento de recursos.
- Puede dividir las plantillas de ARM en componentes más pequeños y vincularlos en la implementación.
- Las plantillas de ARM se pueden integrar en varias herramientas de CI/CD, como Azure DevOps y Acciones de GitHub.
- Con los scripts de implementación, puede ejecutar scripts de Bash o PowerShell desde las plantillas de ARM. A través de la extensibilidad, puede usar una sola plantilla para implementar una solución completa.

**Bicep** es un lenguaje de plantilla de ARM que se usa para implementar recursos de Azure mediante declaración. Bicep es un lenguaje específico del dominio, lo que significa que está diseñado para un escenario o dominio en particular. Bicep se usa para crear plantillas de ARM.

- Bicep es nativo del ecosistema de Azure. Cuando se lanzan o actualizan nuevos recursos de Azure, Bicep admitirá esas características desde el primer día.
- Las plantillas JSON y Bicep están totalmente integradas en la plataforma Azure. Con las implementaciones basadas en Resource Manager, puede supervisar el progreso de la implementación en Azure Portal.
- Bicep es un producto totalmente compatible con el soporte técnico de Microsoft.
- Todo el estado se almacena en Azure. Los usuarios pueden colaborar y tener la confianza de que sus actualizaciones se controlan según lo previsto.
- Si ya usa plantillas JSON como lenguaje de plantilla declarativa, no es difícil realizar la transición a Bicep. Puede usar la CLI de Bicep para descompilar cualquier plantilla en una plantilla de Bicep.

**Azure Automation** ofrece un servicio de automatización y configuración basado en la nube que admite una administración coherente en los entornos de Azure y que no son de Azure. Azure Automation le proporciona un control completo en tres áreas de servicio: automatización de procesos, administración de la configuración y administración de las actualizaciones.

Servicio	Descripción
Automatización de procesos	La automatización de procesos le permite automatizar tareas de administración en la nube frecuentes, lentas y propensas a errores. Este servicio le ayuda a centrarse en el trabajo que agrega valor empresarial. Al reducir los errores y aumentar la eficacia, también contribuye en la reducción de los costos operativos. El servicio le permite crear runbooks gráficamente, en PowerShell o usando Python.
Administración de configuración	La administración de la configuración permite el acceso a dos características, el seguimiento e inventario de cambios y la configuración del estado de automatización de Azure. El servicio admite el seguimiento de cambios entre servicios, demonios, software, registros y archivos del entorno. El seguimiento de cambios le ayuda a diagnosticar cambios no deseados y generar alertas.
Administración de actualizaciones	El servicio de administración de actualizaciones incluye la característica de administración de actualizaciones para sistemas Windows y Linux en entornos híbridos. Esta característica le permite crear implementaciones programadas para organizar la instalación de actualizaciones en una ventana de mantenimiento definida.

**Automation** es necesario en tres áreas generales de operaciones en la nube:

- Implementación y administración: proporcione una infraestructura repetible y coherente en forma de código.
- Respuesta: cree una automatización basada en eventos para diagnosticar y resolver problemas.
- Organización: organice e integre la automatización con otros servicios y productos de Azure o de terceros.

**Azure App Configuration** proporciona un servicio para administrar de forma centralizada la configuración y las marcas de características de la aplicación. Puede usar App Configuration para almacenar toda la configuración de la aplicación y proteger sus accesos en un solo lugar.

- Azure App Configuration es un servicio totalmente administrado que se puede configurar en cuestión de minutos y admite la integración nativa con marcos populares.
- App Configuration ofrece representaciones y asignaciones clave flexibles y reproducción a un momento dado de la configuración.
- App Configuration tiene una interfaz de usuario dedicada para la administración de marcas de características y admite el etiquetado de recursos con etiquetas.
- Puede comparar dos conjuntos de configuraciones en dimensiones definidas por el usuario.
- App Configuration proporciona seguridad mejorada a través de identidades administradas de Microsoft Entra para recursos de Azure.
- La información confidencial se puede cifrar en reposo y en tránsito.
- Azure App Configuration funciona tanto en entornos de desarrollo como en entornos de producción.

Un **entorno de desarrollo** de Azure App Configuration consta de Visual Studio, Visual Studio Code y la CLI de Azure. Estos componentes están vinculados a Microsoft Entra ID, App Configuration y Azure Key Vault.

Un **entorno de producción** de Azure App Configuration consta de identidades administradas por Azure y Microsoft Entra para recursos de Azure con servicios de Azure relacionados. Estos componentes están vinculados a Microsoft Entra ID, App Configuration y Key Vault.

A medida que planee la solución de red, hay varios requisitos que debe tener en cuenta.

- **Nomenclatura:** defina una convención de nomenclatura que pueda usar de forma coherente al asignar nombres a los recursos para facilitar la administración de varios recursos de red a lo largo del tiempo.
- **Regiones:** determine las regiones de Azure para los recursos según las ubicaciones físicas de los consumidores de los recursos. El ámbito de una red virtual es una sola región/ubicación. Sin embargo, se pueden conectar entre sí varias redes virtuales de diferentes regiones mediante el emparejamiento de red virtual.
- **Suscripciones:** planee cuántas suscripciones de Azure se necesitan para cumplir los requisitos de carga de trabajo, teniendo en cuenta que puede implementar varias redes virtuales dentro de cada suscripción y región de Azure.
- **Direcciones IP:** especifique un espacio de direcciones IP privado personalizado mediante direcciones públicas y privadas (RFC 1918). Azure asigna a los recursos de una red virtual una dirección IP privada desde el espacio de direcciones que asigne.
- **Segmentación:** segmente las redes virtuales con subredes en función de los requisitos de carga de trabajo y seguridad.
- **Filtrado:** defina la estrategia de filtrado de tráfico y seguridad de red para las cargas de trabajo.

**Una topología de red** en estrella tipo hub-and-spoke aísla las cargas de trabajo mientras se comparten servicios tales como los de identidad y seguridad. El centro de conectividad es una red virtual de Azure que actúa como punto central de conectividad. Los radios son redes virtuales que se conectan a la red virtual del centro mediante el emparejamiento de red virtual. Los servicios compartidos se implementan en el centro, mientras que las cargas de trabajo individuales se implementan como radios.

- Implemente una topología de red en estrella tipo hub-and-spoke en Azure para centralizar los servicios comunes tales como las conexiones a redes locales, los firewalls y el aislamiento entre redes virtuales. La red virtual del centro de conectividad proporciona un punto central de conectividad a redes locales y un lugar para el hospedaje de servicios que utilizan las cargas de trabajo hospedadas en redes virtuales de radio.
- Utilice redes virtuales de radio para aislar cargas de trabajo, donde cada radio se administra independientemente de otros radios. Cada carga de trabajo puede incluir varios niveles y varias subredes que se conectan a través de equilibradores de carga de Azure.
- Configure redes virtuales en estrella tipo hub-and-spoke en distintos grupos de recursos e incluso en distintas suscripciones. Cuando se emparejan redes virtuales en distintas suscripciones, las suscripciones pueden estar asociadas al mismo inquilino de Microsoft Entra o a uno diferente. Obtiene una administración descentralizada de cada carga de trabajo, mientras se comparten los servicios que se mantienen en la red del centro de conectividad.

Tres patrones de red comunes para organizar cargas de trabajo en Azure:

- Red virtual única
- Varias redes virtuales con emparejamiento
- Varias redes virtuales en una topología de red en estrella tipo hub-and-spoke

Cada patrón proporciona un tipo diferente de aislamiento y conectividad.

En el primer patrón, todos los componentes de la carga de trabajo (o, en algunos casos, toda la superficie de TI) se colocan en una sola red virtual. Esta opción es posible si trabaja en una sola región, ya que una red virtual no puede abarcar varias regiones.

Aquí se muestra cómo puede implementar un único patrón de red virtual:

- Una subred (Subnet 1) puede contener las cargas de trabajo de la base de datos.
- Otra subred (Subnet 2) puede contener las cargas de trabajo web.
- Para controlar el tráfico de subred, puede implementar grupos de seguridad de red para especificar que Subnet 1 solo puede comunicarse con Subnet 2, y Subnet 2 puede comunicarse con Internet.
- Puede aplicar la segmentación mediante una aplicación virtual de red desde Azure Marketplace o Azure Firewall.
- Puede modificar el patrón para admitir muchas cargas de trabajo. Puede seleccionar subredes que no permitan que una carga de trabajo se comunique con el back-end de otra carga de trabajo.

El segundo patrón amplía el patrón de red virtual única para admitir varias redes virtuales con posibles conexiones de emparejamiento. Esta opción permite agrupar aplicaciones en redes virtuales independientes o implementar una presencia en varias regiones de Azure.

El tercer patrón es una organización de red virtual más avanzada en la que elige una red virtual de una región concreta como el centro de conectividad de todas las demás redes virtuales de esa región. La conectividad entre la red virtual de concentrador y sus redes virtuales de radio se logra mediante el emparejamiento de Virtual Network. Todo el tráfico pasa a través de la red virtual del centro, y puede actuar como puerta de enlace a otros centros en regiones diferentes. Configura la posición de seguridad en los centros de conectividad para que puedan segmentar el tráfico entre las redes virtuales y controlarlo de una manera escalable.

Comparación	Red virtual única	Varias redes con emparejamiento	Varias redes en topología de red en estrella tipo hub-and-spoke
Conectividad y enrutamiento (cómo se comunican los segmentos)	El enrutamiento del sistema proporciona conectividad predeterminada a cualquier carga de trabajo de cualquier subred.	El enrutamiento del sistema proporciona conectividad predeterminada a cualquier carga de trabajo de cualquier subred.	No hay conectividad predeterminada entre las redes virtuales de radio. Se necesita un enrutador de nivel 3 (como Azure Firewall) en la red virtual del concentrador para habilitar la conectividad.
Filtrado de tráfico de nivel de red	El tráfico se permite de manera predeterminada. Se puede usar NSG para el filtrado.	El tráfico se permite de manera predeterminada. Se puede usar NSG para el filtrado.	De forma predeterminada, se deniega el tráfico entre las redes virtuales de radio. La configuración de Azure Firewall puede habilitar el tráfico seleccionado, como <a href="#">windowsupdate.com</a> .
Registro centralizado	Registros de NSG para la red virtual.	Agregue registros de NSG en todas las redes virtuales.	Azure Firewall registra en Azure Monitor todo el tráfico aceptado o denegado que se envía a través de un concentrador.
Puntos de conexión públicos abiertos involuntarios	DevOps puede abrir accidentalmente un punto de conexión público a través de reglas de NSG incorrectas.	DevOps puede abrir accidentalmente un punto de conexión público a través de reglas de NSG incorrectas.	Un punto de conexión público abierto accidentalmente en una red virtual de radio no habilitará el acceso. El paquete devuelto se descarta mediante un firewall con estado (enrutamiento asimétrico).
Protección de nivel de aplicación	NSG solo proporciona compatibilidad con la capa de red.	NSG solo proporciona compatibilidad con la capa de red.	Azure Firewall admite el filtrado de FQDN para HTTP/S y MSSQL para el tráfico saliente y entre redes virtuales.

Azure **enruta el tráfico de comunicación** entre los recursos internos locales y los recursos externos de Internet mediante **tablas de rutas**. Al crear una red virtual, Azure crea automáticamente una tabla de enrutamiento para cada subred de la red. Una tabla de enrutamiento contiene muchos tipos diferentes de rutas, incluidos los valores predeterminados del sistema, los puntos de conexión de servicio y la subred. La tabla también tiene entradas de ruta para el Protocolo de puerta de enlace de borde, rutas definidas por el usuario (UDR) y rutas de otras redes virtuales.

**Azure Virtual Network NAT** simplifica la conectividad a Internet solo de salida en las redes virtuales. Cuando se configura este servicio en una subred, toda la conectividad de salida usa las direcciones IP públicas estáticas que se hayan especificado. La conectividad saliente es posible sin que el equilibrador de carga ni las direcciones IP públicas estén conectados directamente a máquinas virtuales. Virtual Network NAT es un servicio totalmente administrado y muy resistente.

## **Características de las tablas de enrutamiento y los tipos de ruta:**

- **Rutas del sistema:** al crear una red virtual por primera vez sin definir ninguna subred, Azure crea entradas de rutas del sistema en la tabla de enrutamiento. Las rutas del sistema se definen para una ubicación específica cuando se crean. Las rutas del sistema no se pueden modificar después de crearlas, pero puede invalidar estas rutas mediante la configuración de rutas definidas por el usuario.
- **Rutas definidas por el usuario (personalizadas):** al crear una o varias subredes dentro de una red virtual, Azure crea entradas predeterminadas en la tabla de enrutamiento para permitir la comunicación entre estas subredes en una red virtual. Estas rutas se pueden modificar mediante rutas estáticas, que se almacenan como rutas definidas por el usuario (UDR) en Azure. Las UDR también se denominan *rutas personalizadas*. En Azure se pueden crear UDR para reemplazar las rutas de sistema predeterminadas de Azure o para agregar rutas adicionales a una tabla de enrutamiento de una subred.
- **Rutas de otras redes virtuales:** al crear un emparejamiento de red virtual entre dos redes virtuales, se agrega una ruta para cada intervalo de direcciones en el espacio de direcciones de cada red virtual emparejada.
- **Rutas de Protocolo de puerta de enlace de borde (BGP):** si la puerta de enlace de red local intercambia las rutas del Protocolo de puerta de enlace de borde (BGP) con una puerta de enlace de red virtual de Azure, se agrega una ruta por cada ruta que se propaga desde la puerta de enlace de red local. Estas rutas aparecen en la tabla de enrutamiento como rutas BGP.
- **Rutas de punto de conexión de servicio:** Azure agrega las direcciones IP públicas de determinados servicios a la tabla de rutas cuando se habilita un punto de conexión para el servicio. Los puntos de conexión de servicio se habilitan para subredes individuales dentro de una red virtual. Cuando se habilita un punto de conexión de servicio, la ruta solo se agrega a la tabla de enrutamiento para la subred que pertenece a este servicio. Azure administra automáticamente las direcciones en la tabla de rutas cuando cambian.
- **Orden de enrutamiento:** cuando haya entradas que compitan en una tabla de enrutamiento, Azure seleccionará el próximo salto en función de la coincidencia de prefijo más larga, de manera similar a la de los enruteadores tradicionales. Si hay varias entradas de próximo salto con el mismo prefijo de dirección, Azure selecciona rutas en un orden específico: UDR, rutas BGP y rutas del sistema.

- **Considere las rutas del sistema.** Defina rutas del sistema para ubicaciones y escenarios específicos que no espera modificar.
  - Enrutamiento del tráfico entre máquinas virtuales de la misma red virtual o entre redes virtuales emparejadas
  - Compatibilidad con la comunicación entre máquinas virtuales mediante una VPN de red virtual a red
  - Habilitación de la comunicación de sitio a sitio a través de Azure ExpressRoute o una instancia de Azure VPN Gateway
- **Considere las rutas definidas por el usuario.** Cree UDR personalizadas para reemplazar las rutas de sistema predeterminadas de Azure o para agregar rutas adicionales a una tabla de enrutamiento de una subred.
  - Habilitación del filtrado del tráfico de Internet a través Azure Firewall o la tunelización forzada
  - Flujo del tráfico entre subredes a través de una NVA
  - Definición de rutas para especificar cómo se deben enrutar los paquetes en una red virtual
  - Definición de rutas que controlen el tráfico de red y especifiquen el próximo salto en el flujo de tráfico
- **Considere la invalidación de rutas.** Planee invalidaciones de ruta para controlar el flujo de tráfico.

Una conexión de **Azure VPN Gateway** es un tipo de puerta de enlace de red virtual que envía tráfico cifrado entre una instancia de Azure Virtual Network y una ubicación local. El tráfico cifrado pasa a través de la red pública de Internet. Hay diferentes configuraciones disponibles para las conexiones de VPN Gateway, como, por ejemplo, de sitio a sitio, de punto a sitio o de red virtual a red.

**Azure ExpressRoute** utiliza una conexión privada y dedicada a través de un proveedor de conectividad de terceros. Esta conexión es privada. El tráfico no pasa por Internet. La conexión privada extiende la red local en Azure.

**Una topología de red en estrella de tipo hub-and-spoke** constituye una forma de aislar cargas de trabajo mientras se comparten servicios como los de identidad y seguridad. El centro es una red virtual en Azure que actúa como punto central de conectividad para la red local. Los radios son redes virtuales que se emparejan con el concentrador. Los servicios compartidos se implementan en el centro, mientras que las cargas de trabajo individuales se implementan como radios.

**Una arquitectura tipo hub-and-spoke** se puede lograr mediante una infraestructura de centro de conectividad administrada por el cliente o una infraestructura de centro de conectividad administrada por Microsoft. En cualquier caso, los radios se conectan al centro de conectividad mediante el emparejamiento de red virtual. El tráfico fluye entre los centros de datos locales y el centro de conectividad a través de una conexión a ExpressRoute o a VPN Gateway. El diferenciador principal de este enfoque es el uso de Azure Virtual WAN para reemplazar los centros de conectividad como un servicio administrado.

**Azure Virtual WAN** es un servicio de redes que ofrece conectividad entre ramas automatizada y optimizada a y mediante Azure. Las regiones de Azure sirven como centros que se pueden elegir para conectar las distintas ramas. Puede aplicar la red troncal de Azure para conectar también ramas y disfrutar de la conectividad de rama a red virtual. Azure Virtual WAN reúne muchos servicios de conectividad en la nube de Azure como la VPN de sitio a sitio, ExpressRoute y la VPN de usuario de punto a sitio en una única interfaz operativa. La conectividad con las redes virtuales de Azure se establece mediante el uso de conexiones de red virtual.

Comparación	Azure VPN Gateway	Azure ExpressRoute	ExpressRoute + conmutación por error de VPN	Azure Virtual WAN + red en estrella tipo hub-and-spoke
Ventajas	<ul style="list-style-type: none"> <li>- Fácil de configurar.</li> <li>- Ancho de banda alto disponible (hasta 10 Gbps en función de la SKU de VPN Gateway).</li> <li>- Admite el escalado dinámico del ancho de banda para ayudar a reducir los costos durante períodos de menor demanda (no compatible con todos los proveedores de conectividad).</li> <li>- Permite el acceso directo de la organización a las nubes nacionales (depende del proveedor de conectividad).</li> </ul>	<ul style="list-style-type: none"> <li>- Ancho de banda alto disponible (hasta 10 Gbps en función del proveedor de conectividad).</li> <li>- Admite el escalado dinámico del ancho de banda para ayudar a reducir los costos durante períodos de menor demanda (no compatible con todos los proveedores de conectividad).</li> <li>- Permite el acceso directo de la organización a las nubes nacionales (depende del proveedor de conectividad).</li> </ul>	<ul style="list-style-type: none"> <li>- Alta disponibilidad si se produce un error en el circuito ExpressRoute (conexión de reserva en la red de ancho de banda inferior).</li> </ul>	<ul style="list-style-type: none"> <li>- Reducción de la sobrecarga operativa reemplazando los centros existentes por un servicio totalmente administrado.</li> <li>- Ahorro de costos mediante el servicio administrado, que elimina la necesidad de NVA.</li> <li>- Seguridad mejorada a través de centros protegidos administrados centralmente con Azure Firewall y Virtual WAN.</li> <li>- Separación de las preocupaciones entre TI central (SecOps, InfraOps) y cargas de trabajo (DevOps).</li> </ul>
Desafíos	<ul style="list-style-type: none"> <li>- Requisito de dispositivo VPN local.</li> </ul>	<ul style="list-style-type: none"> <li>- Posible complejidad en la configuración.</li> <li>- Requisito de trabajo con un proveedor de conectividad de terceros.</li> <li>- Proveedor responsable de aprovisionar la conexión de red.</li> <li>- Requisito de enrutadores de ancho de banda alto en el entorno local.</li> </ul>	<ul style="list-style-type: none"> <li>- Complejo de configurar.</li> <li>- Necesidad de configurar la conexión VPN y el circuito ExpressRoute.</li> <li>- Requisito de hardware redundante (dispositivos VPN).</li> <li>- Requisito de conexión redundante de Azure VPN Gateway, con un coste.</li> </ul>	<p>Nota: Azure Virtual WAN está diseñado para reducir los desafíos de conectividad enumerados anteriormente.</p>
Escenarios	<p><i>Aplicaciones híbridas con tráfico ligero entre el hardware local y la nube.</i></p> <p><i>Possibilidad de cambiar una latencia ligeramente mayor por la flexibilidad y la capacidad de procesamiento de la nube.</i></p>	<p><i>Aplicaciones híbridas que ejecutan cargas de trabajo críticas a gran escala que requieren un alto grado de escalabilidad.</i></p>	<p><i>Aplicaciones híbridas que requieren un mayor ancho de banda de ExpressRoute y conectividad de red de alta disponibilidad.</i></p>	<p><i>La conectividad entre cargas de trabajo requiere control centralizado y acceso a los servicios compartidos.</i></p> <p><i>Una empresa requiere control centralizado sobre aspectos de seguridad, como un firewall y la administración segregada de las cargas de trabajo en cada radio.</i></p>

Azure ofrece varios servicios de equilibrio de carga para distribuir las cargas de trabajo en varios recursos informáticos. A medida que revise las opciones, hay varios factores que se deben tener en cuenta en la planeación.

Los servicios de equilibrio de carga de Azure pueden clasificarse en dos dimensiones:

- Global o regional
- HTTP(S) o no HTTP(S)

En Azure Portal, la pestaña **Ayudarme a elegir** destaca de manera predeterminada otras características de configuración:

- **Tipo de tráfico:** ¿está diseñando una aplicación web (HTTP/HTTPS)? ¿La aplicación es pública o es privada?
- **Global o regional:** ¿necesita equilibrar la carga de máquinas virtuales o contenedores dentro de una red virtual, o equilibrar la carga de la unidad de escalado/las implementaciones entre regiones, o ambas cosas?
- **Disponibilidad:** ¿el SLA de servicio cumple sus requisitos?
- **Costo:** ¿ha definido sus expectativas de costo? Puede revisar las opciones de precios de Azure. Además del costo del propio servicio, tenga en cuenta el de las operaciones de administración de una solución basada en ese servicio.
- **Características y límites:** ¿cuáles son las limitaciones generales de cada servicio? Puede revisar los límites del servicio.

**Azure Content Delivery Network** ofrece una solución global para la entrega rápida de contenido de banda ancha a los usuarios. Content Delivery Network permite almacenar en caché el contenido en nodos físicos colocados estratégicamente en todo el mundo.

**Azure Front Door** le permite definir, administrar y supervisar el enruteamiento global del tráfico web gracias a la optimización para obtener el mejor rendimiento y la conmutación por error global instantánea para lograr una alta disponibilidad. Con Front Door, las aplicaciones empresariales y de consumidor globales (de varias regiones) se pueden transformar en aplicaciones modernas personalizadas, sólidas y de alto rendimiento, API y contenido que lleguen a un público global mediante Azure.

**Azure Traffic Manager** es un equilibrador de carga de tráfico basado en DNS que le permite distribuir el tráfico de forma óptima a servicios de regiones de Azure globales, al tiempo que proporciona una alta disponibilidad y capacidad de respuesta. Traffic Manager proporciona diversos métodos de enruteamiento de tráfico para distribuir el tráfico, como la prioridad, la ponderación, el rendimiento, el método geográfico, el multivalor y la subred.

**Azure Load Balancer** proporciona equilibrio de carga de nivel 4 con latencia baja y rendimiento alto para todos los protocolos UDP y TCP.

**Azure Application Gateway** es un equilibrador de carga de tráfico web que permite administrar el tráfico a las aplicaciones web. Application Gateway es un controlador de entrega de aplicaciones (ADC) como servicio que ofrece diversas funcionalidades de equilibrio de carga de capa 7 para las aplicaciones. Hay dos métodos principales de enruteamiento de tráfico: **enrutamiento basado en rutas de acceso** y **enrutamiento de varios sitios**.

**Azure DDoS Protection** ofrece técnicas defensivas contra las amenazas de DDoS más sofisticadas. El servicio proporciona funcionalidades mejoradas de mitigación de DDoS a su aplicación y los recursos implementados en las redes virtuales. Además, los clientes que usan Azure DDoS Protection tienen acceso a la compatibilidad con la respuesta rápida de DDoS para implicar a expertos de DDoS durante un ataque activo.

**Azure Private Link** le permite acceder a los servicios PaaS de Azure (por ejemplo, Azure Storage y SQL Database) y a los servicios hospedados en Azure que son propiedad de los clientes, o a los servicios de los asociados, a través de un punto de conexión privado de la red virtual. El tráfico entre la red virtual y el servicio viaja por la red troncal de Microsoft. Ya no es necesario exponer el servicio a la red pública de Internet. Puede crear su propio servicio de vínculo privado en la red virtual y enviarlo a los clientes. Private Link se usa para acceder a servicios PaaS como Azure Storage, Azure SQL, App Services y mucho más.

**Azure Firewall** es un servicio de seguridad de red administrado y basado en la nube que protege los recursos de Azure Virtual Network. Se trata de un firewall como servicio con estado completo que incorpora alta disponibilidad y escalabilidad a la nube sin restricciones. Azure Firewall usa una dirección IP pública estática para los recursos de red virtual, lo que permite que los firewalls externos identifiquen el tráfico procedente de la red virtual. Azure Firewall proporciona protección entrante para protocolos que no son HTTP/S (por ejemplo, RDP, SSH y FTP), protección de nivel de red saliente para todos los puertos y protocolos, y protección de nivel de aplicación para HTTP/S saliente.

**Azure Web Application Firewall** proporciona protección a las aplicaciones web frente a vulnerabilidades de seguridad web comunes, como la inyección de SQL y el scripting entre sitios. Web Application Firewall ofrece protección frente a las diez principales vulnerabilidades OWASP a través de reglas administradas. Configure reglas administradas por el cliente para una protección adicional basada en el intervalo IP de origen y los atributos de solicitud (encabezados, cookies, campos de datos de formularios, parámetros de cadena de consulta). Evitar ataques similares en el código de la aplicación puede ser todo un desafío. El proceso puede requerir un mantenimiento riguroso, revisión y supervisión en varias capas de la topología de la aplicación. Un firewall de aplicaciones web centralizado permite simplificar la administración de la seguridad. **Un firewall de aplicaciones** web también proporciona a los administradores de la aplicación un mejor control de la protección contra amenazas e intrusiones.

Un **NSG (Network Security Group)** contiene una lista de reglas de lista de control de acceso (ACL) que permiten o deniegan el tráfico de red a subredes, tarjetas de interfaz de red (NIC) o ambas. Los grupos de seguridad de red se pueden asociar con subredes o con NIC individuales conectadas a una subred. Cuando un NSG está asociado a una subred, las reglas de ACL se aplican a todas las máquinas virtuales de esa subred.

Contiene dos tipos de reglas: de entrada y de salida. La prioridad de una regla debe ser única dentro de cada conjunto. Cada regla tiene propiedades de protocolo, intervalos de puertos de origen y destino, prefijos de direcciones, dirección de tráfico, prioridad y tipo de acceso. Todos los grupos de seguridad de red contienen un conjunto de reglas predeterminadas. Las reglas predeterminadas no se pueden eliminar, pero dado que se les asigna la prioridad más baja, puede invalidarlas con reglas personalizadas.

**Los puntos de conexión de servicio** de Azure Virtual Network extienden el espacio de direcciones privadas de la red virtual y la identidad de la red virtual a los servicios de Azure a través de una conexión directa. Puede usar puntos de conexión para proteger los recursos de servicio de Azure fundamentales con acceso a solo sus redes virtuales. El tráfico desde la red virtual al servicio de Azure siempre permanece en la red troncal de Microsoft Azure. Los puntos de conexión de servicio son fáciles de configurar y tienen menos sobrecarga de administración que otras estrategias

**Azure Bastion** es un servicio PaaS totalmente administrado por la plataforma que se implementa en las redes virtuales. Azure Bastion proporciona una conexión RDP/SSH segura e ininterrumpida a las máquinas virtuales directamente en Azure Portal a través de TLS. Azure Bastion ayuda a protegerse contra el examen de puertos. Los puertos RDP y SSH de las máquinas virtuales no se exponen públicamente, como tampoco las direcciones IP públicas. Cuando se conecta a través de Azure Bastion, las máquinas virtuales no necesitan una dirección IP pública. El tráfico iniciado de Azure Bastion a las máquinas virtuales de destino permanece en la red virtual o entre las redes virtuales emparejadas. Azure Bastion se encuentra en el perímetro de la red virtual y ayuda a protegerse frente a vulnerabilidades de seguridad de día cero. Por tanto, no debe preocuparse por proteger cada una de las máquinas virtuales de la red virtual. La plataforma de Azure mantiene Azure Bastion actualizado.

**El acceso a la red JIT(Just-in-Time)** le permite bloquear el tráfico entrante a las máquinas virtuales. Puede implementar JIT para reducir la exposición a ataques, a la vez que proporciona acceso fácil para conectarse a las máquinas virtuales cuando sea necesario.

- Cuando se habilita el acceso a la máquina virtual JIT, se seleccionan los puertos de las máquinas virtuales para los que se bloquea el tráfico entrante. Esta configuración garantiza que existan reglas para "denegar todo el tráfico entrante" para los puertos seleccionados en el grupo de seguridad de red y reglas de Azure Firewall. Estas reglas restringen el acceso a los puertos de administración de las máquinas virtuales de Azure y los defienden frente a ataques.
- En caso de que ya existan otras reglas relativas a los puertos seleccionados, las reglas existentes tendrán prioridad sobre las nuevas reglas para "denegar todo el tráfico entrante". Si no hay ninguna regla existente en los puertos seleccionados, las nuevas reglas tendrán prioridad principal en los grupos de seguridad de red y Azure Firewall.
- Cuando un usuario solicita acceso a una máquina virtual, Security Center comprueba que este tenga permisos de control de acceso basado en roles (RBAC de Azure) para esa máquina virtual. Si se aprueba la solicitud, los grupos de seguridad de red y Azure Firewall permiten el tráfico entrante a los puertos seleccionados desde la dirección IP (o el intervalo) correspondiente durante el tiempo especificado. Una vez transcurrido el tiempo, los grupos de seguridad de red se devuelven a sus estados anteriores. Las conexiones que ya están establecidas no se interrumpen.

**Microsoft Cloud Adoption Framework** para Azure proporciona recomendaciones, instrucciones de procedimientos recomendados, documentación y herramientas para ayudarle a impulsar la adopción de Azure en su organización. Cloud Adoption Framework admite metodologías para definir la estrategia, planear y preparar la migración y establecer la estructura organizativa a fin de alinear los equipos y los roles. Puede migrar y modernizar cargas de trabajo existentes y desarrollar nuevas soluciones híbridas o nativas de nube. Puede emplear herramientas de Cloud Adoption Framework para controlar el entorno y las cargas de trabajo, así como administrar las operaciones para soluciones híbridas y en la nube.

El proceso de adopción de la migración debe constar de tres fases principales o esfuerzos para cada carga de trabajo: **Evaluación, Implementación y Lanzamiento**. La tabla y la ilustración siguientes resumen los esfuerzos de adopción de la migración, según la metodología de Migración de Microsoft Cloud Adoption Framework.

Esfuerzo	Descripción
<i>Evaluar</i>	Evalúe las cargas de trabajo para determinar los costos, la modernización y las herramientas de implementación necesarias.
<i>Implementar</i>	Después de evaluar las cargas de trabajo, la función existente de la carga de trabajo se replica (o mejora) en la nube.
<i>Versión</i>	Una vez que las cargas de trabajo se implementan (replican) en la nube, puede probar, optimizar y documentar las cargas de trabajo migradas. Cuando esté a punto, puede lanzar las cargas de trabajo a los usuarios. Durante el trabajo de <i>Lanzamiento</i> , asegúrese de entregar las cargas de trabajo a los equipos de gobernanza, administración de operaciones y seguridad para que las cargas de trabajo tengan soporte continuo.

**El marco de migración** de Azure puede ayudarle a desarrollar el plan y a trabajar con la migración. El marco se compone de cuatro fases: ***Evaluación, Migración, Optimización y Supervisión***.

En la primera fase, evaluará el **entorno local actual**:

- Identifique las aplicaciones y sus servidores, servicios y datos relacionados que están dentro del ámbito de la migración.
- Empiece a implicar a las partes interesadas, como el departamento de TI y los grupos empresariales pertinentes.
- Cree un inventario completo y un mapa de dependencias de los servidores, servicios y aplicaciones que tiene previsto migrar.
- Calcule el ahorro de costos mediante la calculadora de costo total de propiedad (TCO) de Azure.
- Identifique las herramientas y servicios adecuados que puede usar para realizar las cuatro fases.

Hay cinco patrones de estrategia generales para migrar cargas de trabajo a la nube, normalmente denominados las cinco R de racionalización: **Rehospedaje, Refactorización, Rediseño, Recompilación y Reemplazo.**

- **Rehospedaje:** a este patrón también se le conoce como *migración mediante lift-and-shift*. Esta estrategia no requiere cambios en el código y permite migrar las cargas de trabajo existentes a Azure rápidamente. Cada carga de trabajo se migra tal cual, sin el riesgo ni los costos asociados a los cambios de código.
- **Refactorización:** a esta estrategia también se le llama *reempaquetado*. La refactorización requiere una mínima cantidad de cambios en las aplicaciones para que puedan conectarse a la plataforma como servicio (PaaS) de Azure y usar las ofertas en la nube. Puede migrar sus aplicaciones existentes a Azure App Service o Azure Kubernetes Service (AKS). O bien podría refactorizar bases de datos relacionales y no relacionales en otras opciones. Puede refactorizar en Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL y Azure Cosmos DB, (si su aplicación se puede reempaquetar fácilmente para funcionar en Azure).
- **Rediseño:** esta estrategia para la migración se centra en modificar y ampliar la función de las aplicaciones y el código base con el fin de optimizar la arquitectura de aplicación para la escalabilidad en la nube. Puede dividir una aplicación monolítica en un grupo de microservicios que funcionen en conjunto y se escalen fácilmente. O bien podría rediseñar las bases de datos relacionales y no relacionales a una solución de base de datos totalmente administrada. Puede rediseñar en Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL y Azure Cosmos DB.
- **Recompilación:** esta estrategia va más lejos, ya que vuelve a compilar una aplicación desde cero mediante tecnologías de la nube de Azure. Puede compilar aplicaciones con tecnologías nativas de nube, como Azure Functions, Azure AI, Azure SQL Managed Instance y Azure Cosmos DB.
- **Sustitución:** Implemente soluciones con la mejor tecnología y enfoque disponible en este momento. A veces, las aplicaciones de software como servicio (SaaS) pueden proporcionar todas las funciones necesarias para las aplicaciones hospedadas. A continuación, se puede programar una carga de trabajo para reemplazarla, quitándola del ámbito de migración.

<b>Rehospedaje</b>	<b>Refactorización</b>	<b>Rediseño</b>	<b>Recompilación</b>	<b>Replace</b>
<i>Mover cargas de trabajo rápidamente a la nube</i>	<i>Aplicar prácticas innovadoras de DevOps que proporciona Azure</i>	<i>Las aplicaciones necesitan revisiones importantes para incorporar nuevas capacidades</i>	<i>Desarrollo rápido</i>	<i>Estandarizar en función de los procedimientos recomendados del sector</i>
<i>Mover una carga de trabajo sin modificarla</i>	<i>Implementar una estrategia de contenedor de DevOps para cargas de trabajo</i>	<i>Las aplicaciones necesitan revisiones importantes para funcionar de forma eficaz en una base de código existente y las aptitudes de desarrollo disponibles</i>	<i>Compatibilidad con aplicaciones existentes con función y duración limitadas</i>	<i>Acelerar la adopción de enfoques basados en procesos de negocio</i>
<i>Para las aplicaciones diseñadas a fin de aprovechar la escalabilidad de IaaS de Azure después de la migración</i>	<i>Compatibilidad con la portabilidad de la base de código existente y las aptitudes de desarrollo disponibles</i>	<i>Cumplir con los requisitos de escalabilidad</i>	<i>Recompilación con nuevas tecnologías nativas de la nube, como Azure Blockchain</i>	<i>Inversiones de desarrollo reasignadas que crean diferenciación o ventajas competitivas</i>
<i>Cuando las aplicaciones son importantes para su negocio, pero no es necesario realizar cambios inmediatamente en las capacidades de la aplicación</i>	<i>Aplicar prácticas innovadoras de DevOps</i>	<i>Minimizar el uso de máquinas virtuales</i>	<i>Recompilar aplicaciones heredadas como "aplicaciones sin código" o "aplicaciones con poco código" en la nube</i>	<i>Reemplazar las soluciones existentes en favor de las ofertas de SaaS</i>

Después de completar la evaluación, puede comenzar **el proceso de migración de las aplicaciones de destino y sus servicios y datos relacionados**. La fase de migración normalmente consta de los siguientes trabajos:

- **Implementar destinos de infraestructura de la nube.** Para poder migrar las cargas de trabajo de Tailwind Traders, deberá crear los destinos de infraestructura en la nube necesarios. En función de las herramientas que use para realizar la migración, es posible que tenga que crear los recursos de Azure necesarios antes de comenzar la migración. Algunas herramientas, como Azure Migrate y Azure Database Migration Service, pueden crear los recursos de Azure de destino.
- **Migrar las cargas de trabajo.** Es una buena idea pilotar la migración de la carga de trabajo y elegir una aplicación no crítica para el piloto. Este enfoque le permite conocer bien las herramientas, obtener experiencia con procesos y procedimientos, así como reducir el riesgo al migrar cargas de trabajo grandes o complejas.
- **Retirar la infraestructura local.** Una vez que esté satisfecho de que las aplicaciones y bases de datos de origen se han migrado correctamente, debe retirar las cargas de trabajo de origen. Considere la posibilidad de conservar las copias de seguridad de la carga de trabajo de origen y los datos archivados. Estos datos pueden resultar útiles, ya que proporcionan un archivo histórico. Puede almacenar estas copias de seguridad y archivos en Azure Blob Storage.

Para la **fase de optimización**, hay tres trabajos principales en los que centrarse a la hora de la planificación:

- Analizar los costos de migración de las cargas de trabajo
- Revisar las recomendaciones para reducir los costos
- Identificar las opciones para mejorar el rendimiento de la carga de trabajo

Puede usar Azure Monitor para capturar información de estado y rendimiento de las máquinas virtuales de Azure. Instale el agente de registros de Azure Monitor (anteriormente conocido como Log Analytics) en las máquinas virtuales de destino y, después, configure alertas e informes.

Herramienta o servicio	Fases	Descripción
Service Map	Evaluar	La característica Service Map de Azure Monitor asigna la comunicación entre los componentes de la aplicación en Windows o Linux. Use esta característica para identificar las dependencias al determinar qué datos se van a migrar. Service Map requiere que se instale otro agente en las máquinas virtuales del entorno de origen.
Calculadora de TCO de Azure	Evaluar	La calculadora del costo total de propiedad (TCO) calcula el ahorro de costos que puede obtener al migrar las cargas de trabajo a Azure.
Azure Migrate	Evaluar y Migrar	Azure Migrate realiza la evaluación y la migración a Azure de máquinas virtuales (Hyper-V y VMware), máquinas virtuales basadas en la nube, servidores físicos, bases de datos, datos, infraestructura de escritorio virtual y aplicaciones web.
Data Migration Assistant (DMA)	Evaluar y Migrar	Data Migration Assistant de SQL Server le permite actualizar a una plataforma de datos moderna. Detecta problemas de compatibilidad que pueden afectar a la función de la base de datos en nuevas versiones de SQL Server o Azure SQL Database.
Database Migration Service	Evaluar y Migrar	Azure Database Migration Service realiza la evaluación y la migración de varias bases de datos diferentes, no solo las de Azure SQL Database.
Herramienta de migración de datos.	Migrar	La herramienta de migración de datos de Azure Cosmos DB migra las bases de datos existentes a Azure Cosmos DB.
Microsoft Cost Management	Optimize (Optimizar)	Microsoft Cost Management (anteriormente conocido como Azure Cost Management and Billing) le permite supervisar, optimizar y controlar los costos continuos de Azure.
Advisor	Supervisión	Azure Advisor ayuda a optimizar los recursos de Azure para garantizar la fiabilidad, el rendimiento, el costo, la seguridad y la excelencia operativa.
Supervisión	Supervisión	Azure Monitor recopila telemetría de supervisión de recursos locales y de Azure que le ayudan a analizar datos, configurar alertas e identificar problemas.
Microsoft Sentinel	Supervisión	Microsoft Sentinel proporciona análisis de seguridad inteligentes para las aplicaciones que le permiten recopilar, detectar e investigar incidentes, así como responder a estos.

La **característica Service Map** de Azure Monitor permite detectar automáticamente las aplicaciones y sus componentes en el entorno local. Use la característica para obtener información valiosa sobre la estructura de la aplicación a fin de planificar y realizar la migración de forma eficaz. Service Map admite la detección en plataformas Windows y Linux. Service Map muestra los detalles del entorno en varios formatos:

- Conexiones entre servidores
- Procesos de servidor
- Latencia de conexión entrante y saliente
- Puertos TCP o UDP en cualquier arquitectura conectada

La característica Service Map de Azure Monitor admite varias funciones de evaluación críticas:

- **Detección:** cree una referencia común de las dependencias de los servidores y sus procesos. Revise la información detectada como un mapa gráfico intuitivo. Identifique las conexiones de red con errores.
- **Administración de incidentes:** elimine las dudas en torno al aislamiento de problemas. Identifique los componentes y sistemas mal configurados.
- **Control de la migración:** planifique, acelere y valide las migraciones de Azure. Asegúrese de que no se olvida nada y de que no se producen interrupciones inesperadas.
- **Continuidad empresarial:** identifique cómo los sistemas se basan entre sí, lo que ayuda a garantizar que el plan de recuperación sea fiable. Identifique qué sistemas de front-end debe recuperar después de restaurar un servidor y estar disponible una vez más.
- **Administración de revisiones:** identifique qué otros equipos y servidores dependen de un servicio al que se va a aplicar la revisión. Notifique a los equipos de antemano antes de desactivar los sistemas para la aplicación de revisiones.

Para usar Azure Service Map, necesita la configuración siguiente:

- Un área de trabajo de Log Analytics en Azure Portal.
- El agente de Azure Monitor instalado en los equipos Windows o Linux. Este agente recopila eventos y datos de rendimiento del equipo y los entrega al área de trabajo de Log Analytics.
- Dependency Agent instalado en los equipos Windows o Linux. Este agente recopila datos detectados sobre los procesos que se ejecutan en el equipo y las dependencias de procesos externos. Dependency Agent requiere que el agente de Azure Monitor se instale en la misma máquina.

**La calculadora de TCO de Azure** le permite calcular y optimizar los costos esperados de Azure después de la migración. La calculadora le guía por tres pasos para preparar las estimaciones:

1. Definir las cargas de trabajo
2. Ajustar las suposiciones
3. Visualizar el informe de estimaciones

**Azure Migrate** le permite realizar una detección de entorno sin agente, o bien usar agentes para realizar un análisis de dependencias. Puede acceder a las características de Azure Migrate en Azure Portal para ayudar a evaluar las cargas de trabajo locales actuales. Azure Migrate realiza recomendaciones para el tamaño de la máquina virtual que debe aprovisionar a fin de evaluar la preparación para el traslado a Azure. Puede identificar los costos estimados de los recursos que consumirán esas máquinas, de modo que el equipo de administración pueda fijar los presupuestos.

**Azure Migrate** incluye varias herramientas de evaluación a fin de ayudarle a prepararse para la migración. Para realizar una detección sin agente, use la herramienta de evaluación de servidores de Azure Migrate.

Una vez completada la recopilación de datos, estos se insertan en el proyecto de Azure Migrate. En Azure Portal, puede ver los sistemas detectados y descargar un informe. El proceso completo para evaluar un servidor se puede visualizar de la siguiente manera:

1. Descargar y configurar el dispositivo
2. Iniciar detección
3. Crear una evaluación
4. Revisar la evaluación

**Azure Migrate incluye los componentes siguientes para admitir el proceso de migración:**

- **Plataforma de migración unificada:** Azure Migrate proporciona un único portal en el que se puede llevar a cabo la migración a Azure y realizar un seguimiento del estado de esta.
- **Herramientas de evaluación y migración:** Azure Migrate proporciona varias herramientas de evaluación y migración, como la evaluación de servidores, la migración de servidores y otras herramientas de fabricantes de software independientes (ISV).
- **Características de evaluación y migración para diferentes cargas de trabajo:** el centro de Azure Migrate Hub admite varias cargas de trabajo diferentes para la migración:
  - Servidores: los servidores locales se evalúan y se migran a máquinas virtuales de Azure.
  - Bases de datos: las bases de datos locales se evalúan y se migran a Azure SQL Database o a una instancia de Azure SQL Managed Instance.
  - Aplicaciones web: las aplicaciones web locales se evalúan y se migran a Azure App Service mediante Azure App Service Migration Assistant.
  - Escritorios virtuales: la Infraestructura de escritorio virtual (VDI) local se evalúa y se migra a Azure Virtual Desktop.
  - Datos: los volúmenes elevados de datos se migran a Azure mediante productos de Azure Data Box.
- **Herramientas del centro de Azure Migrate:** el centro de Azure Migrate proporciona acceso a muchas herramientas de migración.

Herramienta	Uso
Azure Migrate: Detección y evaluación: Evaluación del servidor	Descubrimiento y evaluación de servidores, incluidos SQL y aplicaciones web
Azure Migrate: Server Migration	Migrar servidores
Data Migration Assistant (DMA) de SQL Server	Evaluar bases de datos de SQL Server para la migración a Azure SQL Database, Azure SQL Managed Instance o máquinas virtuales de Azure que ejecutan SQL Server
Azure Database Migration Service	Migrar bases de datos locales a máquinas virtuales de Azure en las que se ejecutan SQL Server, Azure SQL Database o SQL Managed Instance.
Migration Assistant para aplicaciones web	Evaluación de aplicaciones web locales y migración de dichas aplicaciones a Azure
Azure Data Box	Migración de datos sin conexión

Azure Migrate puede ayudarle a completar seis escenarios de migración principales:

- Cargas de trabajo de Windows Server
- Cargas de trabajo de SQL Server
- Cargas de trabajo de Linux
- Aplicaciones Windows, Java y PHP
- SAP HANA
- Proceso especializado

Azure Migrate usa **Azure App Service Migration Assistant** para evaluar y migrar las aplicaciones web. App Service Migration Assistant permite evaluar y migrar las aplicaciones web locales de Windows ASP.NET a Azure. Use App Service Migration Assistant para realizar estas tareas:

- Determinar si la aplicación es una candidata adecuada para la migración.
- Ejecutar comprobaciones de preparación para realizar una evaluación general de los valores de configuración de la aplicación.
- Migrar una aplicación a Azure App Service.

**App Service Migration Assistant** usa un agente que se instala localmente y, después, lo usa para realizar un análisis detallado de las aplicaciones. Debe usar la herramienta para migrar esas aplicaciones a Azure. Una vez completada la evaluación inicial de las aplicaciones, se le guiará por el proceso de migración mediante una interfaz gráfica controlada por el asistente.

Hay cuatro pasos de implementación técnica principales implicados en la migración real de una carga de trabajo de servidor a una carga de trabajo de máquina virtual de Azure mediante Azure Migrate.

1. Preparación de Azure para la herramienta Azure Migrate: Server Migration.
2. Preparar las máquinas virtuales locales para la migración.
3. Replicar las máquinas virtuales locales.
4. Migrar las máquinas virtuales.

**Azure Resource Mover** es una herramienta que ayuda a mover los recursos de Azure entre suscripciones, grupos de recursos y regiones. Azure Resource Mover proporciona las ventajas siguientes:

- Una única ubicación para mover recursos.
- Simplicidad y velocidad en el traslado de recursos.
- Una interfaz y un procedimiento coherentes para mover distintos tipos de recursos de Azure.
- Una manera de identificar las dependencias entre los recursos que desea mover.
- Limpieza automática de recursos en la región de origen.
- La capacidad de probar una operación de movimiento antes de confirmarla.

Puede usar Azure Resource Mover de dos maneras:

- **Antes de la migración**, para organizar los recursos.
- **Después de la migración**, para optimizar la organización de recursos.

Se trata de Azure Migrate y Azure Database Migration Service. Puede usar Database Migration Service para migrar las bases de datos locales, incluido lo siguiente:

- Máquinas virtuales de Azure que ejecutan SQL Server
- Azure SQL Database (Database Migration Assistant)
- Instancia administrada de Azure SQL
- Azure Cosmos DB
- Azure Database for MySQL
- Azure Database for PostgreSQL

**Azure Database Migration Service** es un servicio totalmente administrado. El servicio proporciona dos maneras de migrar datos estructurados en bases de datos de SQL Server:

- **Migración en línea:** una migración en línea usa una sincronización continua de los datos activos, lo que permite transicionar a la base de datos de réplica de Azure en cualquier momento. La migración en línea minimiza el tiempo de inactividad.
- **Migración sin conexión:** una migración sin conexión requiere apagar el servidor al iniciar la migración, lo que provoca un tiempo de inactividad del servicio.

Al comenzar una migración de datos estructurados con Database Migration Service, Data Migration Assistant (DMA) de SQL Server le guía por el proceso. Este proceso consta de tres pasos principales:

1. **Evaluar bases de datos:** DMA le ayuda a evaluar las bases de datos que quiere migrar.
2. **Migrar el esquema:** DMA separa el esquema de las bases de datos. Después, se vuelve a crear el esquema en las instancias de Azure SQL Database de destino.
3. **Migrar datos y verificar:** DMA copia los datos de las bases de datos en las instancias de destino y, después, comprueba las bases de datos migradas.

Para las migraciones en línea y sin conexión, debe completar las tareas de requisitos previos siguientes:

- Descarga de DMA
- Creación de una instancia de Azure Virtual Network
- Configuración de los grupos de seguridad de red (NSG)
- Configuración de Firewall de Windows de Azure
- Configuración de credenciales
- Aprovisionamiento de la base de datos de destino en Azure (establecer el tamaño adecuado de la base de datos de destino para la carga de trabajo migrada)

El primer paso consiste en evaluar el entorno local con DMA.

**La evaluación** genera un informe con recomendaciones y enfoques alternativos para la migración. Revise el informe en busca de problemas de compatibilidad entre las bases de datos de origen y destino que podrían provocar un error en la migración. Solucione los problemas y, después, genere un nuevo informe de evaluación. Repita este proceso hasta que confirme que se han solucionado todos los problemas.

Cada base de datos tiene un esquema que representa toda su estructura. El esquema define las reglas que rigen cómo se organizan los datos estructurados y las relaciones que hay entre los elementos de datos. Antes de migrar los datos de la base de datos, hay que migrar el esquema. Al migrar el esquema en primer lugar, se logran dos objetivos:

- Se crea una estructura vacía en la nueva base de datos de Azure SQL. Esta estructura coincide con la de la base de datos de origen local.
- La conectividad se valida antes de ejecutar la migración de datos completa. DMA crea y ejecuta un script para realizar las acciones necesarias.

Después de completar la evaluación y migrar el esquema, puede migrar los datos estructurados con Database Migration Service.

Cuando termine de realizar todos los pasos de migración, el esquema y los datos estructurados se habrán migrado a la instancia de Azure SQL Database. Después, puede apagar y retirar las bases de datos y servidores locales de forma segura.

**El servicio de migración** de almacenamiento de Azure en Windows Admin Center es útil cuando necesita mover servidores a máquinas virtuales o hardware más recientes. Puede usar el servicio de migración para ayudar a migrar los datos no estructurados de varias maneras, entre las que se incluyen las siguientes:

- Realizar un inventario de los servidores y sus datos
- Transferir rápidamente los archivos, los recursos compartidos de archivos y la configuración de seguridad de los servidores de origen
- Tomar el control de la identidad de los servidores de origen (o *transicionar*)
- Administrar una o varias migraciones desde la interfaz de Windows Admin Center

El servicio de migración de almacenamiento de Azure puede ayudarle a migrar datos almacenados no estructurados en servidores de archivos locales a Azure Files y máquinas virtuales hospedadas en Azure. El proceso de migración se realiza mediante capacidades que proporciona el servicio de migración, Azure File Sync y Azure Migrate.

El servicio de migración de almacenamiento de Azure implementa tres pasos para mover los datos no estructurados locales en línea:

1. **Realizar un inventario de los servidores:** el servicio de migración realiza un inventario de los servidores para recopilar información sobre sus archivos y configuración.
2. **Transferir datos:** el servicio de migración transfiere los datos del origen a los servidores de destino.
3. **Transicionar (opción):** como opción, el servicio de migración transiciona a los servidores nuevos.

**Azure File Sync** es una característica de Azure Files. Azure Files es un servicio de Azure que proporciona la funcionalidad de un recurso compartido de archivos local con las ventajas de un servicio en la nube de plataforma como servicio (PaaS).

Azure File Sync le permite centralizar los recursos compartidos de archivos de la organización en Azure Files, a la vez que mantiene la flexibilidad, el rendimiento y la compatibilidad de un servidor de archivos local. También puede usar Azure File Sync para almacenar en caché recursos compartidos de archivos de Azure en equipos con Windows Server para poder acceder rápidamente cerca del lugar por el que se accede a los datos. Puede usar cualquier protocolo disponible en Windows Server para acceder a sus datos localmente, como SMB, NFS y FTPS.

Escenario	Descripción
<i>Reemplazar o complementar servidores de archivos locales</i>	Prácticamente todas las empresas usan servidores de archivos. Azure Files puede complementar o reemplazar totalmente los servidores de archivos locales tradicionales o los dispositivos de almacenamiento conectado a la red. Con los recursos compartidos de archivos de Azure y la autenticación de Microsoft Entra Domain Services, puede migrar los datos a Azure Files y usar la alta disponibilidad y escalabilidad, a la vez que minimiza los cambios del cliente.
<i>Lift-and-shift (rehome)</i>	Azure Files facilita la migración mediante lift and shift de aplicaciones que esperan un recurso compartido de archivos para almacenar datos de la aplicación o el usuario en la nube.
<i>Copia de seguridad y recuperación ante desastres</i>	Puede usar recursos compartidos de archivos de Azure como almacenamiento para copias de seguridad o para la recuperación ante desastres con el fin de mejorar la continuidad empresarial. Puede usar recursos compartidos de archivos de Azure para realizar copias de seguridad de los datos a partir de servidores de archivos existentes, a la vez que conserva las listas de control de acceso discretionarios de Windows que se han configurado. Los datos que se almacenan en recursos compartidos de archivos de Azure no se ven afectados por desastres que podrían afectar a ubicaciones en el entorno local.
<i>Azure File Sync</i>	Con Azure File Sync, los recursos compartidos de archivos de Azure se pueden replicar en instancias de Windows Server, locales o en la nube, para obtener un almacenamiento en caché eficiente y distribuido de los datos en la ubicación en que se usan. Considere la posibilidad de usar Azure File Sync cuando desee migrar contenido de carpeta compartida a Azure. Este método es especialmente útil como medio para reemplazar Sistema de archivos distribuido en los servidores Windows de los centros de datos locales.

El servicio **Azure Import/Export** migra grandes cantidades de datos entre una ubicación local y una cuenta de almacenamiento de Azure. Con el servicio Import/Export, puede enviar y recibir discos físicos que contienen los datos entre la ubicación local y un centro de datos de Azure. Se envían los datos que se almacenan en sus propias unidades de disco. Estas unidades de disco pueden ser unidades de disco duro (HDD) de Serial ATA (SATA) o unidades de estado sólido (SSD).

Para usar el servicio Azure Import/Export, debe crear un trabajo que especifique los datos que quiere importar o exportar. A continuación, prepara los discos que se van a usar para transferir los datos. Para un trabajo de importación, escribe los datos en estos discos y envíelos a un centro de datos de Azure. Microsoft carga los datos automáticamente. Para un trabajo de exportación, prepare un conjunto de discos en blanco y envíelos a un centro de datos de Azure. Microsoft copia los datos a estos discos y los envía de vuelta.

Estos son algunos puntos más sobre cómo trabajar con el servicio Import/Export:

- Puede usar el servicio Azure Import/Export para exportar datos únicamente de Azure Blob Storage.
- No se pueden exportar los datos contenidos en Azure Files.
- Para usar el servicio Import/Export, BitLocker debe estar habilitado en el sistema Windows.
- Necesita una cuenta activa con un transportista de envío, como FedEx o DHL, para enviar unidades a un centro de datos de Azure.
- Para la exportación, necesita un conjunto de discos que puede enviar a un centro de datos de Azure. El centro de datos usa estos discos para copiar los datos de Azure Storage.

**El servicio Azure Import/Export** es ideal para cargar y descargar grandes cantidades de datos cuando la red troncal no tiene suficiente capacidad o fiabilidad a fin de admitir transferencias a gran escala. El servicio Import/Export puede ser útil en otros escenarios, entre los que se incluyen los siguientes:

Escenario	Descripción
Migración	Use el servicio Import/Export para migrar grandes cantidades de datos desde el entorno local a Azure, como una tarea única.
Backup	Puede realizar copias de seguridad de los datos locales en Azure Storage con el servicio Import/Export.
Recuperación	Con el servicio Import/Export, puede recuperar grandes cantidades de datos almacenados anteriormente en Azure Storage.
Distribución	El servicio Import/Export le permite distribuir datos de Azure Storage a sitios de clientes.

**Azure Data Box** proporciona un método rápido, confiable y económico para mover grandes volúmenes de datos a Azure. Mediante Data Box, puede enviar terabytes de datos dentro y fuera de Azure. La solución se basa en un dispositivo de almacenamiento seguro que se envía a su organización. Data Box puede incluir varios dispositivos, como discos, chasis de servidores resistentes o discos móviles.

Azure ofrece varios productos para adaptarse a diferentes escenarios: Data Box, Data Box Disk y Data Box Heavy. El proceso de configuración es básicamente el mismo en todos los productos.

Azure Data Box incluye los componentes siguientes:

- **Dispositivo Data Box:** un dispositivo físico que proporciona almacenamiento principal, administra la comunicación con el almacenamiento en la nube y ayuda a garantizar la seguridad y confidencialidad de todos los datos almacenados en el dispositivo. El dispositivo Data Box tiene una capacidad de almacenamiento utilizable de 80 TB.
- **Servicio Data Box:** una extensión de Azure Portal que permite administrar un dispositivo Data Box mediante una interfaz web a la que puede acceder desde diferentes ubicaciones geográficas. Use el servicio Data Box para realizar la administración diaria del dispositivo Data Box. Las tareas de servicio incluyen cómo crear y administrar pedidos, ver y administrar alertas y administrar recursos compartidos.
- **Interfaz de usuario basada en web local de Data Box:** una interfaz de usuario basada en web que se usa para configurar el dispositivo, de modo que pueda conectarse a la red local y, después, registrar el dispositivo con el servicio Data Box. También puede usar la interfaz de usuario web local para apagar y reiniciar el dispositivo Data Box, ver registros de copia y ponerse en contacto con el Soporte técnico de Microsoft a fin de enviar una solicitud de servicio.

**Data Box** es ideal para transferir tamaños de datos mayores de 40 TB. El servicio es especialmente útil en escenarios con conectividad a Internet limitada. Puede considerar la posibilidad de usar Data Box en las situaciones siguientes.

Escenario	Descripción
<i>Migración única</i>	Use Azure Data Box para migrar una gran cantidad de datos locales a Azure. Traslade una biblioteca multimedia desde cintas sin conexión a Azure para crear una biblioteca multimedia en línea. Migre la granja de máquinas virtuales, el servidor SQL Server y las aplicaciones a Azure. Traslade los datos históricos a Azure para un análisis exhaustivo y la generación de informes con Azure HDInsight.
<i>Transferencia masiva inicial</i>	Puede realizar una transferencia masiva inicial con Azure Data Box y seguir con las transferencias incrementales a través de la red. Mueva grandes volúmenes de copias de seguridad históricas a Azure. Despues de agregar estos datos, puede seguir manteniendo el archivo con transferencias incrementales de datos mediante la red a Azure Storage.
<i>Cargas periódicas</i>	Use Azure Data Box para mover grandes volúmenes de datos que se generan periódicamente a Azure. Mueva los datos que generan sensores de dispositivos IoT conectados por el cliente.

Comparación	Azure Import/Export	Azure Data Box
Factor de forma	Unidades de disco duro o SSD SATA internas	Dispositivo de hardware individual seguro y a prueba de alteraciones
Microsoft administra la logística de envío	No	Sí
Se integra con productos de asociados	No	Sí
Dispositivo personalizado	No	Sí

# Marco de buena arquitectura de Microsoft Azure: optimización de costos

Azure Well-Architected Framework es un marco de diseño que puede mejorar la calidad de una carga de trabajo al ayudar a:

- Ser resistente, disponible y recuperable.
- Ser tan seguro como lo necesite.
- **Ofrecer una rentabilidad de la inversión suficiente.**
- Apoyar el desarrollo y las operaciones responsables.
- Lograr su propósito en períodos de tiempo aceptables.

El diseño de la arquitectura siempre se basa en los objetivos empresariales y debe tener en cuenta la rentabilidad de la inversión (ROI) y las restricciones financieras. Entre las preguntas habituales que se deben tener en cuenta se incluyen:

- ¿Los presupuestos asignados le permiten cumplir sus objetivos?
- ¿Cuál es el patrón de gasto para la aplicación y sus operaciones? ¿Cuáles son las áreas prioritarias?
- ¿Cómo maximizará la inversión en recursos, mediante un mejor uso o reducción?

Los conceptos descritos en este módulo no lo incluyen todo sobre la optimización de costos en una carga de trabajo, pero representan los principios básicos y algunos de sus enfoques clave a la hora de diseñar una carga de trabajo. Para obtener una perspectiva completa en todos los pilares de Well-Architected Framework, visite Azure Well-Architected Framework a medida que empiece a planear y diseñar la arquitectura.

**Un modelo de costos** ayuda a segmentar los gastos y calcular y prever el costo total de propiedad, incluida la infraestructura, el soporte técnico y la implementación. Permite identificar los impulsores de costos al principio y predecir cómo el crecimiento o la reducción del uso afectarán a los ingresos generales y al gasto en el modelo de negocio proyectado para la carga de trabajo. El modelo de costos de la carga de trabajo debe incluir un factor de uso para ayudar a predecir el cambio en el TCO.

**Un presupuesto** es el límite financiero final que impulsa las decisiones de diseño e implementación.

**La implementación de un enfoque** equilibrado que tenga en cuenta la rentabilidad de la inversión evita el exceso de ingeniería, que podría aumentar los costos.

La aplicación a través de directivas de gobernanza o de patrones de diseño de aplicaciones incorporados puede evitar cargos accidentales o no aprobados.

**El impacto en la rentabilidad** de la inversión es uno de los factores que debe tener en cuenta a la hora de medir los costos totales de su carga de trabajo.

Mediante el uso de **precios basados en el consumo**, solo se paga por lo que se usa exactamente. Esta opción es una buena opción cuando no se espera que el proceso de carga de trabajo se use a tiempo completo.

Si el diseño usa modelos **activos-pasivos**, es posible que tenga recursos inactivos que, de lo contrario, se podrían usar. La conversión a activo-activo puede permitirle cumplir los requisitos de expansión de escalado y expansión de carga sin sobrecargar. Si puede cumplir los objetivos de recuperación con un modelo de solo activo, los costos de esos recursos se pueden quitar completamente.

**La consolidación de la infraestructura** le ayudará a optimizar los costos de la nube. A medida que aumenta la densidad, la cantidad de recursos que necesita para ejecutar una carga de trabajo disminuye. Esto reduce el costo por unidad y el costo de la administración.

Microsoft ofrece tasas reducidas para un compromiso predecible y a largo plazo con recursos y categorías de recursos específicos. Los recursos cuestan menos durante el período de uso y se pueden amortizar durante el período.

Al mantener al equipo de licencias al tanto de la inversión actual y predicha por recurso, puede ayudarles a cumplir los compromisos de tamaño correcto cuando su organización firma el contrato. En algunos casos, estas proyecciones y compromisos podrían influir en la hoja de precios de la organización, lo que beneficia el costo de la carga de trabajo y también otros equipos que usan la misma tecnología.

Cuando el uso es alto y predecible, el modelo de precio fijo suele costar menos y a menudo admite más características. Su uso podría aumentar el ROI.

Las revisiones periódicas de métricas, datos de rendimiento, informes de facturación y uso de características pueden dar lugar a un ajuste preciso que puede reducir los costos.

El marco de buena arquitectura de Azure es un marco de diseño que puede mejorar la calidad de una carga de trabajo al ayudar a:

- Ser resistente, disponible y recuperable.
- Ser tan seguro como lo necesite.
- Ofrecer una rentabilidad de la inversión suficiente.
- Apoyar el desarrollo y las operaciones responsables.
- Lograr su propósito en períodos de tiempo aceptables.

**DevOps** es una comunidad de prácticas en la que la diversidad de perspectivas y aptitudes impulsa una misión. Los equipos deben fomentar un entorno colaborativo de conocimiento compartido en lugar de un aprendizaje aislado. Use funciones compartidas para esforzarse por superar las restricciones de recursos. DevOps optimiza las tareas operativas para que sean eficaces pero no pesadas. Para aprovechar todas las ventajas de DevOps, la referencia cultural debe optimizar los procesos a través de la tecnología y contar con procesos para que las personas de la organización promuevan una comunicación transparente.

**La adopción de una metodología** conocida establece el ritmo del proyecto. Elimina las ambigüedades del proceso al proporcionar a los miembros del equipo expectativas y responsabilidades claras.

Mediante el seguimiento de una lista común, las tareas se pueden refinar y priorizar con prácticas estándar. El proyecto tendrá más posibilidades de entregarse a tiempo.

Las metodologías estándar ayudan con la administración de riesgos. Con las revisiones de hitos pormenorizadas, los desarrolladores pueden abordar posibles problemas antes de convertirse en programadores.

Con **las visualizaciones**, puede analizar tendencias, realizar un seguimiento de los objetivos empresariales y administrar incidentes.

Los paneles que se adaptan al interés del cliente hacen que la interpretación sea relevante y acelere el tiempo de detección y acción.

**Las tecnologías de IaC (Infraestructura como Código)** declarativa están diseñadas teniendo en cuenta la automatización y la reutilización. Puede descargar implementaciones de infraestructura de usuarios en herramientas y lograr una calidad coherente.

Desde una perspectiva de la infraestructura, tener menos opciones tecnológicas elimina la varianza en las herramientas y facilita la detección del desfase de configuración. El mantenimiento también será más fácil. Si alinea opciones con el conjunto de aptitudes existente del equipo, el equipo puede adoptarlas fácilmente.

**Los objetivos de rendimiento** se centran en la experiencia del usuario que se basa en lo que es factible, los procedimientos recomendados del sector y las tendencias actuales del mercado.

**Una prueba de concepto** es fundamental para validar el diseño para determinar si el sistema puede cumplir los objetivos de rendimiento y si esos objetivos son realistas. En función de la carga prevista, puede validar si la capacidad prevista puede cumplir los objetivos de rendimiento.

Estos puntos de **control garantizan** que cada fase de implementación cumpla los estándares de rendimiento necesarios antes de continuar con el siguiente proceso. Los puntos de control ayudan a evitar la regresión de rendimiento no deseada. Por ejemplo, si el rendimiento es significativamente inferior a las expectativas, puede bloquear una versión hasta que se realicen mejoras.

**Azure Well-Architected Framework** es un marco de diseño que puede mejorar la calidad de una carga de trabajo al ayudar a:

- **Ser resistente, disponible y recuperable.**
- Ofrecer una rentabilidad de la inversión suficiente.
- Apoyar el desarrollo y las operaciones responsables.
- Lograr su propósito en períodos de tiempo aceptables.

Las interrupciones y los errores de funcionamiento son preocupaciones graves en todas las cargas de trabajo. Una carga de trabajo confiable debe sobrevivir a esos eventos y **seguir proporcionando su funcionalidad prevista de forma coherente**. Debe ser **resistente** para que pueda detectar, resistir y recuperarse de los errores dentro de un período de tiempo aceptable. También debe estar **disponible** para que los usuarios puedan acceder a la carga de trabajo durante el período de tiempo prometido en el nivel de calidad prometido.

Las arquitecturas de las cargas de trabajo deben tener **garantías de confiabilidad en el código de la aplicación, la infraestructura y las operaciones**. Las opciones de diseño no deben cambiar la intención especificada por los requisitos empresariales. Estos cambios se deben considerar inconvenientes importantes.

**Los estándares proporcionan** coherencia y minimizan los errores humanos. Enfoques como las convenciones de nomenclatura estándar y las guías de estilo de código pueden ayudarle a mantener la calidad y facilitar la identificación de los recursos durante la solución de problemas.

# Aceleración de la adopción de la nube en Microsoft Cloud Adoption Framework para Azure

**Cloud Adoption Framework** abarca todo el ciclo de vida de la adopción de la nube. A lo largo de ese ciclo de vida, puede usar diferentes metodologías diseñadas para ayudar a que un rol concreto proporcione una función definida.

- **Establecimiento de equipos:** en función de la estrategia de adopción y el modelo operativo, es posible que tenga que crear algunos equipos. Estas guías le ayudan a dar los primeros pasos con esos equipos nuevos, o bien a redistribuir las tareas si no se necesita un equipo dedicado.
- **Mejora de los controles:** a medida que crece la adopción de la nube, se necesita un modelo operativo sólido para garantizar decisiones acertadas y un cambio adecuado en la organización. Prepare al personal y mejore las operaciones para desarrollar su modelo operativo en la nube.
- **Agilización de la adopción:** la adopción de la nube exige cambios técnicos, pero para la transformación digital con la nube, se necesita algo más que simplemente TI. Use estas guías para empezar a alinear varios equipos para agilizar los trabajos de migración e innovación.
- **Alineación de las bases:** la nube de la empresa se basa en un conjunto de decisiones fundamentales que pueden afectar a todos los resultados basados en la nube. Esta guía y la información conceptual pueden ayudarle a tomar decisiones fundamentales y a documentarlas.

Los tipos de roles que van a intervenir en el establecimiento de la visión estratégica y el área de interés más común de cada rol:

- **Liderazgo financiero:** aumentar la rentabilidad al tiempo que se impulsa el cumplimiento
- **Marketing:** lograr y conservar clientes y crear una reputación
- **Ventas:** acelerar las ventas y mejorar el valor de vigencia de los clientes
- **Recursos humanos:** conservar, contratar y capacitar a los empleados
- **Liderazgo ejecutivo y junta directiva:** cumplir los requisitos de crecimiento del mercado y las métricas de sostenibilidad medioambiental

<b>Eventos empresariales críticos</b>	<b>Migración</b>	<b>Innovación</b>
Salida del centro de datos	Ahorro de costes	Preparación de nuevas funcionalidades técnicas
Fusión, adquisición o desinversión	Reducción de la complejidad técnica o de proveedores	Creación de nuevas funcionalidades técnicas
Reducción de gastos de capital	Optimización de las operaciones internas	Escalado para satisfacer las demandas del mercado
Finalización del soporte técnico para tecnologías críticas	Aumento de la agilidad empresarial	Escalado para satisfacer las demandas geográficas
Respuesta a los cambios de cumplimiento normativo	Preparación de nuevas funcionalidades técnicas	Experiencias e involucración mejoradas de los clientes
Nuevos requisitos de soberanía de datos	Escalado para satisfacer las demandas del mercado	Transformación de productos o servicios
Reducción de interrupciones y mejora de la estabilidad de TI	Escalado para satisfacer las demandas geográficas	Perturbación del mercado con nuevos productos o servicios
Reducción de la huella de carbono	Integración de una cartera de TI compleja	Democratización o entornos de autoservicio

Las motivaciones para la adopción de la nube probablemente se incluyan en varias categorías. A medida que crea la lista de motivaciones, es probable que vea tendencias emergentes. Las motivaciones tienden a asociarse más con una clasificación (evento de negocio crítico, migración, innovación) que con otras. Use la clasificación predominante para ayudar a guiar el desarrollo de la estrategia de adopción de la nube.

Cuando la prioridad más alta es dar respuesta a **eventos empresariales críticos**, es importante empezar con la migración pronto, a menudo en paralelo con los esfuerzos de estrategia y planificación. Este enfoque exige una mentalidad de crecimiento y una disposición a mejorar de forma repetida los procesos en función de las lecciones directas aprendidas.

Si la **migración** es la prioridad más alta, la estrategia y la planificación desempeñan un papel fundamental en una fase temprana del proceso. Se recomienda implementar la primera carga de trabajo en paralelo con los esfuerzos de planeación. Esta experiencia ayuda al equipo a comprender y prever las curvas de aprendizaje asociadas a la adopción de la nube.

Cuando la **innovación** es la prioridad más alta, la estrategia y el planeamiento requieren más inversiones al principio del proceso. Este enfoque garantiza el equilibrio en la cartera y la alineación sensata de la inversión realizada durante la adopción de la nube. Para obtener más información e instrucciones, vea Descripción del recorrido de innovación.

Las motivaciones de migración que se muestran cerca de la parte superior de la tabla de motivaciones son las razones más comunes para adoptar la nube, pero no necesariamente las más significativas. El logro de estos resultados es importante, pero se usan de forma más eficaz para realizar la transición a otros conceptos más útiles. Este importante primer paso para la adopción de la nube a menudo se denomina **migración a la nube**. En el marco se usa el término migración para hacer referencia a la estrategia de ejecución de una migración a la nube.

Algunas motivaciones se alinean bien con una estrategia de migración. Las motivaciones de la parte superior de esta lista probablemente tengan un impacto empresarial menor que las de la parte inferior. Entre las principales motivaciones de las migraciones se incluyen las siguientes:

- Ahorro en costos operativos
- Reducción de la complejidad técnica o de proveedores
- Optimización de las operaciones internas
- Aumento de la agilidad comercial
- Preparación para nuevas funcionalidades técnicas
- Escalado para satisfacer demandas del mercado
- Escalado para satisfacer demandas geográficas

Los datos son la nueva mercancía. Las aplicaciones modernas son la cadena de suministro que impulsa los datos en varias experiencias. En el mercado empresarial de hoy en día, es difícil encontrar un producto o servicio transformador que no se base en los datos, la información y las experiencias de los clientes. Las motivaciones que aparecen en la parte inferior de la lista de innovaciones se alinean con una estrategia tecnológica que, en este marco, se denomina metodología de innovación.

**La estratificación** es un principio sólido de la macroeconomía. Pero con las limitaciones presupuestarias de la mayoría de los proyectos de administración de cambios basados en la tecnología, un enfoque estratificado conduce a señales confusas y molestas dentro del programa. En concreto, varias inversiones simultáneas en estrategias contrapuestas provocan una alineación incorrecta de los individuos, procesos y proyectos necesarios para el éxito general de los programas. Para que la transformación digital tenga éxito, las organizaciones deben priorizar las motivaciones en función de las expectativas de los plazos, la alineación organizativa y la capacidad de inversión.

<b>Horizonte</b>	<b>Objetivo</b>	<b>Período de tiempo</b>	<b>Consideraciones</b>
1. Migración y modernización	Clasifique por orden de prioridad la salida del centro de datos con un enfoque en soluciones de plataforma como servicio (PaaS) modernas por medio de una migración mediante lift-and-shift básica.	Meses 0-18	La migración como prioridad debe minimizar los conflictos con los compromisos de innovación existentes.
2. Modernización de las operaciones	Clasifique por orden de prioridad las mejoras operativas basadas en la gobernanza nativa de nube, la administración de operaciones, la seguridad y las funcionalidades de cumplimiento.	Meses 6-18	Este esfuerzo complementa y respalda el esfuerzo de migración principal.
3. Modernización avanzada	Con las mejoras posteriores a la migración y las operaciones, el equipo tiene suficientes conocimientos en la nube y datos para realizar una modernización más profunda de arquitecturas complejas.	Meses 18-24	
4. Innovación y crecimiento	Redirija la reducción del capital de las salidas del centro de datos y las nuevas aptitudes en el área de TI central para centrarse en acelerar la innovación continua.	A partir del mes 24	Todos los horizontes anteriores dan lugar a una extensa lista de nuevas innovaciones a medida que el equipo de innovaciones comerciales y de TI central crean colaboraciones más estrechas y recursos de automatización.

Las operaciones modernas necesitan maneras modernas de medir los resultados empresariales, y la tecnología de la nube puede ayudar a aumentar la velocidad de una empresa. La plataforma de medición de una organización debe respaldar los resultados y el plan de crecimiento de una empresa mediante las acciones siguientes:

- Proporcionar información a los grupos y miembros del equipo.
- Respaldar la dinamización rápida del personal cuando los resultados no se alinean con la estrategia y las expectativas.
- Ofrecer a los equipos un formato estructurado, plantillas, secuencias y herramientas para ayudarlos a planear y visualizar un aumento de la velocidad.

Se ha demostrado que los OKR impulsan la alineación en entornos de trabajo complejos, fomentan la innovación y ayudan a los usuarios a centrarse en lo que importa. Muchas organizaciones han empezado a usar OKR. Los OKR se basan en dos componentes: un objetivo y los resultados clave para ese objetivo. Un objetivo es la declaración de intenciones: ¿Qué intenta conseguir el equipo y por qué es importante? Los resultados clave son resultados específicos que realizan el seguimiento del impacto del objetivo:

**Objetivo:** claridad e intención.

**Resultados clave:** medidas del éxito durante un trimestre

Los principios clave de los OKR son los siguientes:

- **Aspiraciones e inspiraciones:** los equipos establecen los mejores resultados posibles de un trimestre determinado, centran los esfuerzos en obtener resultados excelentes y usan retrospectivas para el aprendizaje y la iteración.
- **Enfoque en el resultado:** los resultados clave trimestrales proporcionan claridad sobre dónde se genera el valor. Ser consciente de dónde se crea el valor ayuda a los equipos y a la organización a impulsar el impacto empresarial con mayor rapidez.
- **Enfoque global y local:** los equipos localizan los OKR en sus nombres, verbos y números, que enriquecen los OKR con la experiencia y las conclusiones del equipo.
- **Transparencia:** los OKR, la alineación y el progreso son visibles para todos mediante software de OKR, lo que simplifica la colaboración y permite tomar decisiones correctas con mayor rapidez.

Cinco pasos pueden ayudar a la organización a adoptar los OKR:

- **Paso 1: Aprendizaje.** Comience a explorar lo que los OKR pueden hacer para la empresa. Contacte con compañeros y líderes del sector para descubrir cómo han beneficiado los OKR a sus organizaciones.
- **Paso 2: Planificación.** A medida que empiece a elaborar el borrador de los OKR, asegúrese de que los patrocinadores participen y se impliquen en el proceso. Trabaje con un asesor de OKR para ajustar sus OKR.
- **Paso 3: Lanzamiento.** Cada organización lanza las iniciativas de manera diferente. Mantenga un plan de comunicación sólido, e integre el proceso de calibración y celebración de OKR en su modelo operativo.
- **Paso 4: Impulso.** Para mantener el rigor y el enfoque, asegúrese de compartir los resultados en toda la organización. Compartir los resultados ayuda a los equipos a adoptar el hábito de usar OKR.
- **Paso 5: Mejora.** Siga mejorando, vuelva a realizar consultas y vuelva a plantearse la conexión en toda la organización. Los OKR en hojas de cálculo pueden ser útiles, pero una organización puede obtener los máximos beneficios de la participación de todos para cumplir los objetivos y obtener conclusiones de los datos alineados.

Los estados financieros básicos de la organización y libera el flujo de efectivo para su reinversión:

- **Balance general:** si opera en el entorno local de su centro de datos, es posible que haya realizado inversiones por adelantado en recursos a largo plazo que limitan el efectivo y el capital necesarios para que su negocio crezca. Mientras que si está en la nube, puede dirigir los costos de las operaciones del centro de datos hacia la modernización, el desarrollo de aplicaciones en la nube y otros proyectos que impulsen el crecimiento empresarial. Este cambio puede hacer que el balance sea más ágil.
- **Extracto de flujo de efectivo:** el modelo de pago por uso y la capacidad de aplicar directivas y etiquetas a los recursos de Azure le ayudan a mejorar la predictibilidad del extracto de flujo de efectivo. Este modelo mejora el tiempo del flujo de efectivo retrasando el gasto.
- **Balance de ingresos (pérdidas y ganancias) :** Para mejorar la rentabilidad a lo largo del tiempo, puede aprovechar la flexibilidad de Azure, los bajos costos de administración, los servicios y los modelos de precios.

**Amortización:** Un gasto asociado a un recurso (normalmente, intangible) que refleja el uso *económico* de ese recurso en un período de tiempo determinado. Por ejemplo, si compra un servidor por valor de 100 USD, lo capitalizaría en el balance general. Si la amortizara durante cinco años, reconocería un gasto anual de 20 USD que afecta a su balance de ingresos.

**Balance:** un balance es un extracto financiero que informa de los activos, pasivos y el patrimonio de una empresa en una fecha determinada.

**Gastos de capital (CAPEX):** la inversión inicial en equipos. Estos equipos se capitalizan como un recurso y se incluyen en el balance.

**Extracto de flujo de efectivo:** un extracto de flujo de efectivo es un extracto financiero que resume la cantidad de efectivo y de equivalentes de efectivo entrante y saliente de una empresa durante un período determinado.

**Economía de la nube:** información sobre las ventajas y costos de la nube, así como el impacto financiero al iniciar una migración desde el entorno local a la nube.

**Depreciación:** Un gasto asociado a un recurso capitalizado que refleja el uso *económico* de ese recurso en un período de tiempo determinado. Por ejemplo, si compra un servidor por valor de 100 USD, lo capitalizaría en el balance general. Si se depreciara durante cinco años, reconocería un gasto anual de 20 USD que afecta a su balance de ingresos.

**Período de doble hipoteca:** período en el que se tienen dos conjuntos de costos al mismo tiempo. Por ejemplo, si tiene costos relacionados con el entorno local y con la nube.

### **Beneficio antes de intereses, impuestos, depreciación y amortización**

**(EBITDA):** indicador de rendimiento de la rentabilidad de una empresa. Esta métrica empieza por los *ingresos operativos*, que son los propios de las operaciones empresariales habituales (sin tener en cuenta aspectos como los impuestos o los gastos por intereses) y se suman la depreciación y la amortización. Se trata de una métrica de rendimiento útil que se usa para hacer comparaciones, aunque a menudo se utiliza con métricas combinadas, como los gastos de capital, para tener una mejor visión general de la capacidad de una empresa para generar un flujo de caja libre.

**Valor neto actual:** evaluación del valor financiero de una inversión empresarial. Esta métrica examina los flujos de caja, la distribución temporal y el tipo de interés necesario.

**Gastos operativos (OPEX):** gastos continuos de una empresa. Por ejemplo, un pago de mantenimiento o una factura periódica por los servicios de Azure.

**Beneficios y pérdidas:** extracto financiero que resume los ingresos, costos y gastos durante un período determinado, normalmente, un trimestre o un año fiscal. También se conoce como declaración de ingresos.

**Rentabilidad de la inversión (ROI):** métrica que se usa para comprender la rentabilidad de una inversión. La rentabilidad de la inversión compara lo que ha pagado por una inversión con lo que ha ganado para evaluar la eficiencia de dicha inversión

**El cálculo de la ganancia** de la inversión requiere con frecuencia una segunda fórmula, que es específica de los resultados empresariales y los cambios técnicos asociados. Calcular los beneficios es más difícil que calcular las reducciones de costos.

Para calcular los beneficios, se requieren dos variables:

- Cambios (diferencias) en los ingresos.
- Cambios en los costos.

Estas variables se describen en las secciones siguientes:

## **Ingresos diferenciales**

Los ingresos diferenciales se deben prever en colaboración con las partes interesadas de la empresa. Una vez que las partes interesadas acuerdan un impacto sobre los ingresos, el acuerdo se puede usar para mejorar la posición de los beneficios.

## **Costos diferenciales**

Los costos diferenciales son el aumento o la disminución de los costos provocado por la transformación. Los costos diferenciales pueden verse afectados por variables independientes. Los beneficios se basan en gran medida en los costos directos como la reducción de gastos de capital, la prevención de costos, las reducciones de costos operativos y las de amortización. En las secciones siguientes se describen algunos costos diferenciales que se deben tener en cuenta.

Uno de los primeros pasos habituales que hay que seguir para cambiar la reputación de la TI como centro de costos es implementar un **modelo de contabilidad de contracargo**. Este modelo es especialmente común en empresas más pequeñas o en organizaciones de TI con una elevada eficiencia. En el modelo de contracargo, los costos de TI asociados a una unidad de negocio específica se tratan como gastos operativos en el presupuesto de esa unidad de negocio. Esta práctica reduce los efectos de costos acumulados sobre la TI, lo que permite que los valores empresariales se muestren con mayor claridad.

En el entorno local, la arquitectura se aprovisiona normalmente para una capacidad máxima. La migración del entorno local a la nube le ofrece la flexibilidad de la escalabilidad, y puede escalar y reducir verticalmente según sea necesario. Es fundamental comprender las cargas de trabajo para obtener todas las ventajas de la nube.

**Capacidad inactiva:** Azure ayuda a eliminar la capacidad inactiva generada por una arquitectura sobreaprovisionada para una cobertura durante la utilización máxima. La definición correcta y eliminación de las cargas de trabajo que no necesita ayudan a reducir la capacidad inactiva al mudarse a la nube. Este ejercicio ofrece ahorros inmediatos y reducciones en el flujo de efectivo.

**Cargas de trabajo impredecibles:** puede escalar y reducir verticalmente los recursos de proceso en la nube a medida que cambia la demanda del negocio. Puede escalar y reducir verticalmente la capacidad y usar un modelo de costes variables en lugar de un modelo de costes fijos. Esta elasticidad de la nube hace posible el modelo de pago por uso y funciona bien para las cargas de trabajo impredecibles. Considere la posibilidad de usar conjuntos de escalado de máquinas virtuales y desasociar VM para pagar solo por los recursos que necesite cuando los necesite.

**Cargas de trabajo predecibles:** Para las cargas de trabajo predecibles, puede aprovechar las ofertas de ahorro de costos, como Azure Reservations.

**Limpieza inicial, selección del tamaño adecuado y optimización:** cuando planee la migración a Azure, revise qué cargas de trabajo ya no son necesarias. Este proceso de limpieza puede ayudarle a crear un caso de negocio más sólido y a mostrar un efecto inmediato en los presupuestos. Para las cargas de trabajo que todavía quiere usar y traer a la nube, puede usar herramientas que le ayuden a optimizarlas, como por ejemplo, Azure Migrate.

**FastTrack for Azure** ofrece asistencia directa por parte de los ingenieros de Azure, en estrecha colaboración con los asociados, para ayudar a los clientes a compilar las soluciones de Azure con rapidez y confianza. FastTrack aporta procedimientos recomendados y herramientas de experiencias reales del cliente para guiar a los clientes desde la instalación, la configuración y el desarrollo hasta la producción de soluciones de Azure, lo que incluye:

Durante una interacción típica de FastTrack for Azure, Microsoft ayuda a definir la visión empresarial para planear y desarrollar correctamente soluciones de Azure. El equipo evalúa las necesidades de diseño y proporciona instrucciones, principios de diseño, herramientas y recursos para ayudar a compilar, implementar y administrar soluciones de Azure. El equipo empareja asociados cualificados para los servicios de implementación a petición y se registran periódicamente para asegurarse de que la implementación está en buen pie y para ayudar a quitar los bloqueadores.

**Una justificación comercial** proporciona una visión de la escala de tiempo técnica y financiera de su entorno, y puede representar las oportunidades de reinversión en una mayor modernización. El desarrollo de una justificación comercial incluye la creación de un plan financiero que tenga en cuenta los aspectos técnicos y se alinee con los resultados empresariales. Ayuda a fomentar la asistencia del equipo financiero y otras áreas de la empresa, ayuda a acelerar la migración a la nube y permite una mayor agilidad empresarial.

**Ámbito del entorno, técnico y financiero:** a medida que elabora la vista de su entorno local, piense en cómo está alineado el ámbito del entorno, desde una perspectiva tanto técnica como financiera. Querrá asegurarse de que el entorno técnico que usa para el plan coincida con los datos financieros.

**Datos financieros de línea de base:** costo operativo actual. Al crear el caso de negocio, es importante extraer los datos financieros de línea de base. Las preguntas comunes que puede hacer para recopilar los datos financieros necesarios son:

- ¿Cuánto cuesta ejecutar el entorno hoy en día?
- ¿Cuánto se gasta en servidores en un año promedio?
- ¿Cuál es el gasto en las categorías de operaciones del centro de datos, por ejemplo, los costos de energía o concesión?
- ¿Cuándo es la siguiente actualización de hardware?

**Proyecciones:** Costos locales en un escenario local: Previsión de los costos locales si no migra a la nube.

**Proyecciones: Costos locales en escenarios de Azure:** Previsión de los costos locales si migra a la nube en un escenario de Azure. Se necesitan recursos y tiempo para cambiar el entorno a la nube, por lo que es importante tenerlos en cuenta en la justificación comercial. Al crear el escenario de Azure, asegúrese de tener en cuenta e incluir todas las ventajas principales que ofrece la nube.

**Proyecciones: Escala de tiempo de migración y costos de Azure (optimizados):** Proyecta cuál es la escala de tiempo de migración y los costos de Azure con un entorno determinado. Tenga en cuenta de qué manera puede optimizar y sacar el máximo partido de su inversión en Azure.

Una justificación comercial no es solo una visión en un momento dado. Es un plan para un período de tiempo. A medida que se desplace a la nube, podrá reducir el gasto a lo largo del tiempo y crear un plan de migración a la nube. Puede modelar la relación entre la caída del gasto local a lo largo del tiempo y el plan de migración a la nube.

**El modelo operativo** menos complejo es un modelo totalmente descentralizado. Este modelo está muy centrado en cargas de trabajo independientes con una dependencia mínima de operaciones centralizadas. Este modelo también se conoce como TI bimodal o descentralizada.

**Prioridad estratégica:** las organizaciones suelen usar la descentralización cuando priorizan la *innovación al control*. Este modelo es muy común entre las startups, pero también es una tendencia cada vez mayor en organizaciones de gran tamaño.

**Organización:** los equipos se organizan en torno a cargas de trabajo o procesos empresariales, lo que contrasta con los otros tres modelos operativos.

**Ámbito de la cartera:** el ámbito de la cartera también se aísla en niveles de carga de trabajo. Cuando una organización está completamente descentralizada, es improbable que invierta mucho tiempo en administrar la alineación de la cartera.

**Responsabilidad (separación de tareas):** el equipo de cargas de trabajo es totalmente responsable de las decisiones sobre operaciones, gobernanza y seguridad. En las operaciones descentralizadas no existe un modelo de responsabilidad compartida.

**Estandarización:** los procedimientos recomendados y la automatización de la implementación (las canalizaciones de integración y entrega continuas) son fundamentales para crear cualquier grado de estandarización entre las cargas de trabajo. Sin funciones centralizadas, es probable que la estandarización no dure mucho.

**Prioridad de las operaciones:** es probable que un equipo de operaciones descentralizadas priorice las operaciones exclusivas para la nube con herramientas de software como servicio (SaaS) o plataforma como servicio (PaaS) a fin de automatizarlas.

**Velocidad de desarrollo de la plataforma:** es posible que las operaciones descentralizadas comparten scripts de implementación entre cargas de trabajo, pero apenas se comparten recursos centrales entre las cargas de trabajo.

**Un modelo de operaciones centralizado** es el más común en TI. Este modelo está muy centrado en un entorno de producción controlado administrado únicamente por operaciones centralizadas. Las operaciones centralizadas se centran en un menor número de zonas de aterrizaje con utilidades fundamentales insertadas.

**Prioridad estratégica:** cuando el control y la estabilidad de la empresa son más importantes que la innovación, este modelo suele ser la tendencia más alta. Las organizaciones más grandes o estables suelen usar operaciones centralizadas. Es un modelo común cuando se adoptan decisiones para el entorno basadas en requisitos de cumplimiento de terceros.

**Organización:** los equipos primero se organizan en torno a funciones o procesos. En organizaciones más pequeñas, la central de TI es el hogar de miembros del equipo centrados en la seguridad, gobernanza, operaciones e infraestructura. A medida que las organizaciones crecen, es posible que esas funciones se diversifiquen a equipos dedicados a cada una de ellas.

**Ámbito de la cartera:** los equipos de operaciones centralizadas tienden a centrarse en una zona de aterrizaje o en un pequeño número de zonas de aterrizaje. Dentro de esas zonas de aterrizaje, la organización implementa utilidades fundamentales para admitir una combinación de cargas de trabajo en cada zona de aterrizaje. Este modelo de operaciones tiende a crear problemas de escalado cuando la organización admite bases de nube sólidas y carteras de varias nubes.

**Responsabilidad (separación de tareas):** en este modelo operativo, los equipos de operaciones centrales o de TI normalmente son responsables de todos los recursos de producción. La separación de tareas tiende a centrarse en el aislamiento del entorno, lo que evita que equipos específicos de la carga de trabajo interactúen con los recursos de producción.

**Estandarización:** es probable que la estandarización entre cargas de trabajo sea alta. Pero a medida que la cartera crece para abarcar varias zonas de aterrizaje o varias plataformas de nube, es posible que esa estandarización se divida y sea necesario realizar modificaciones significativas en el entorno.

**Prioridad de las operaciones:** las organizaciones suelen usar operaciones centralizadas cuando consideran que su modelo operativo en la nube es un modelo operativo secundario. Como las operaciones locales o en la nube privada existentes son el modelo principal, estas organizaciones tienden a conservar las herramientas de operaciones existentes y limitan el uso principal de las herramientas de operaciones modernas exclusivas para la nube.

**Velocidad de desarrollo de la plataforma:** normalmente, los equipos de operaciones centrales necesitan un enfoque de comienzo a pequeña escala para abordar utilidades comunes. Con el tiempo, los equipos se centrarán en incorporar las mejores soluciones al entorno.

**Un modelo empresarial** es adecuado para los clientes que van a migrar a la nube centros de datos completos o carteras grandes. Las operaciones empresariales se centran en un mayor número de zonas de aterrizaje con utilidades fundamentales centralizadas en una plataforma base.

**Prioridad estratégica:** el modelo empresarial se centra en la democratización de las decisiones y la delegación de responsabilidades para equilibrar la necesidad de innovación en algunas zonas de aterrizaje y un control más estricto en otras. Se trata de una prioridad estratégica para organizaciones de gran tamaño que necesitan proteger sus intereses existentes, a la vez que permite la innovación para mantener el ritmo de los cambios del mercado.

**Organización:** las operaciones empresariales posibilitan funciones de creación y operativas en cada equipo de carga de trabajo. Los equipos de carga de trabajo se alinean por función, como las de gobernanza, seguridad y operaciones. Un equipo dedicado de centro de excelencia en la nube (CCoE) une los equipos de carga de trabajo y los complementarios para coordinar las actividades y garantizar la excelencia operativa en la nube base.

**Ámbito de la cartera:** el ámbito de las operaciones empresariales se centra en la base holística en la nube para garantizar que las utilidades fundamentales estén centralizadas y disponibles para todas las zonas de aterrizaje. Despues, las zonas de aterrizaje y los entornos de carga de trabajo dedicados se pueden implementar en una capacidad de autoservicio, con todas las dependencias necesarias proporcionadas por la base en la nube.

**Responsabilidad (separación de tareas):** el equipo de CCoE es responsable del mantenimiento de los recursos centralizados necesarios y de la creación de visibilidad en toda la cartera. Las operaciones centrales o los equipos de operaciones específicas de carga de trabajo son responsables del soporte diario de las cargas de trabajo individuales.

**Estandarización:** en este modelo operativo, la estandarización es la más alta. La base en la nube centralizada garantiza la coherencia de la configuración de todas las áreas de diseño de zonas de aterrizaje. Los procedimientos recomendados sólidos favorecen la implementación automatizada en todas las cargas de trabajo. Esta automatización permite una mayor estandarización en los nivel de carga de trabajo y recurso.

**Prioridad de las operaciones:** un modelo operativo empresarial necesita un enfoque prioritario de nube para las operaciones. Las herramientas propias basadas en la nube son esenciales para mantener las operaciones centralizadas en la nube. Para que sea efectivo, este tipo de modelo debe considerar a la nube como el modelo operativo principal. La organización considera que las operaciones locales existentes son secundarias y deben incluirse en un plan de transición a largo plazo.

**Velocidad de desarrollo de la plataforma:** para fomentar la centralización de la gobernanza, la seguridad y las operaciones en una cartera de cargas de trabajo en constante crecimiento, los equipos de operaciones empresariales necesitarán que se implemente una solución empresarial antes de la adopción.

**El modelo distribuido** es la forma de operaciones más compleja. Combina los demás modelos.

**Prioridad estratégica:** las organizaciones usan este modelo cuando favorecen la integración de las unidades de negocio adquiridas, antes que la innovación o el control. Suele ser una estrategia temporal o de puente necesaria para pasar a un modelo operativo más eficaz en el futuro. Este modelo se suele conservar cuando la organización quiere mantener la autonomía y considera una estrategia de salida a corto plazo, como suele suceder en empresas de capital de inversión o sociedades gestoras.

**Organización:** en este modelo operativo, es difícil mantener una estructura centralizada de la organización. Se recomienda que las organizaciones empiecen por la formación de un equipo virtual de CCoE al principio del proceso para crear visibilidad y concienciación sobre las operaciones de la organización.

**Ámbito de la cartera:** las operaciones distribuidas se centran en una cartera compleja. Con el tiempo, se pueden centrar en niveles más granulares de la cartera.

**Responsabilidad (separación de tareas):** la responsabilidad variará entre las unidades de negocio. La separación de las tareas desde una perspectiva central es difícil de lograr.

**Estandarización:** el primer paso para la estandarización en un modelo de operaciones distribuidas consiste en obtener una visión clara de los bienes digitales de toda la cartera. Se iniciará un enfoque controlado por datos para identificar puntos comunes en la cartera orientados hacia un modelo de operaciones centralizado o empresarial.

**Prioridad de las operaciones:** la prioridad de las operaciones en este modelo se basa en los datos. La centralización de los datos mediante herramientas diseñadas para operaciones unificadas permitirá a un equipo de CCoE entrenar y asesorar a las distintas unidades de negocio durante las transiciones o los esfuerzos de madurez. Antes de forzar una prioridad de operaciones coherente, evalúe la cartera de operaciones de carga de trabajo para garantizar las herramientas y líneas de base adecuadas.

**Velocidad de desarrollo de la plataforma:** la evaluación de la cartera de operaciones de carga de trabajo debe identificar una velocidad aceptable para el desarrollo de la plataforma que se alinee con los enfoques de inicio a pequeña escala o escala empresarial. El punto de datos principal para determinar la dirección dependerá del enfoque de administración de operaciones más común en la cartera.

Área de diseño	Objetivo	Metodología pertinente
Facturación de Azure e inquilino de Active Directory	La creación y la inscripción adecuadas de los inquilinos y la configuración de la facturación son pasos iniciales importantes.	Ready
Administración de identidades y acceso	La administración de identidades y acceso es un límite de seguridad principal en la nube pública. Es la base de cualquier arquitectura segura y totalmente compatible.	Ready
Topología de red y conectividad	Las decisiones de redes y conectividad son un aspecto fundamental de cualquier arquitectura de nube.	Ready
Organización de recursos	A medida que se escala la adopción de la nube, las consideraciones para el diseño de suscripciones y la jerarquía de grupos de administración afectan a la gobernanza, la administración de operaciones y los patrones de adopción.	Control

Área de diseño	Objetivo	Metodología pertinente
Seguridad	Implemente controles y procesos para ayudar a proteger sus entornos en la nube.	Seguridad
Administración	En el caso de las operaciones estables y en curso en la nube, desarrolle una línea base de administración para proporcionar opciones de visibilidad y de cumplimiento de operaciones, así como para ayudar a proteger y recuperar las funcionalidades.	Administrar
Gobernanza	Automatizar la auditoría y el cumplimiento de las directivas de gobernanza	Control
Automatización de la plataforma y DevOps	Alinee las mejores herramientas y plantillas para implementar sus zonas de aterrizaje y recursos de soporte técnico.	Ready

**La arquitectura conceptual** de zonas de aterrizaje de Azure se aplica universalmente a cualquier proceso o implementación de zonas de aterrizaje. Como base de la arquitectura, encontramos un conjunto de principios de diseño fundamentales que sirven como brújula para las decisiones de diseño posteriores en dominios técnicos críticos.

Rampa de entrada	Descripción	Guía adicional
Iniciar	<p>Para las organizaciones que están al principio de su recorrido de adopción de la nube (también conocidas como <i>greenfield</i>) y que quieren implementar un nuevo entorno de nube basado en procedimientos recomendados y patrones arquitectónicos probados.</p> <p>Comience con la arquitectura conceptual de zonas de aterrizaje de Azure para comprender el estado final recomendado.</p> <p>A continuación, explore cada una de las áreas de diseño. Use las áreas para comprender las consideraciones y decisiones que necesita para diseñar e implementar la zona de aterrizaje que mejor se adapte a sus necesidades.</p>	<a href="#">¿Qué es una zona de aterrizaje de Azure?</a> <a href="#">Áreas de diseño de las zonas de aterrizaje de Azure</a>
Alinear	<p>Para las organizaciones que tienen un entorno existente que necesita modificarse para alinearse con la arquitectura de destino y los procedimientos recomendados de una zona de aterrizaje de Azure (también conocido como <i>brownfield</i>).</p> <p>Use la transición de la guía de brownfield para comprender los puntos de decisión y el enfoque técnico de los entornos de refactorización de forma que se alineen con la guía de la metodología de preparación.</p>	<a href="#">Refactorización de una zona de aterrizaje</a> <a href="#">Transición de entornos de Azure existentes a la arquitectura conceptual de la zona de aterrizaje de Azure</a> <a href="#">Escenario: Transición de entornos de Azure existentes a la arquitectura conceptual de la zona de aterrizaje de Azure</a>
Mejora	<p>Para entornos que ya están en línea con los procedimientos recomendados, pero la organización quiere agregar más controles o características.</p> <p>Explore artículos sobre la mejora de los procesos clave en curso para los entornos en la nube, como la administración, la gobernanza y la seguridad.</p>	<a href="#">Guía de mejora de la administración</a> <a href="#">Guía de mejora de la gobernanza</a> <a href="#">Guía de mejora de la seguridad</a>

**Las zonas de aterrizaje** de Azure proporcionan a los equipos de adopción de la nube un entorno bien administrado para sus cargas de trabajo. Cada una de las opciones siguientes aplica un conjunto predeterminado de consideraciones de diseño para zonas de aterrizaje a fin de proporcionar una implementación y una arquitectura que sirvan de guía para la configuración del entorno.

La ampliación de la zona de aterrizaje proporciona un enfoque orientado al código para incorporar los siguientes principios en la zona de aterrizaje y, a grandes rasgos, en el entorno de nube general: Azure Advisor, el Marco de buena arquitectura de Microsoft Azure y las soluciones del Centro de arquitectura de Azure comparten estos mismos principios.

Azure Migrate proporciona una plataforma de migración unificada, es decir, un único portal para iniciar, ejecutar y realizar un seguimiento de la migración a Azure. En el centro de Azure Migrate, puede evaluar y migrar lo siguiente:

- **Servidores, bases de datos y aplicaciones web:** evaluar servidores locales, incluyendo las aplicaciones web e instancias de SQL Server, y migrarlos a Azure.
- **Bases de datos:** evalúe las instancias y las bases de datos locales de SQL Server para migrarlas a un SQL Server en una máquina virtual de Azure o una Azure SQL Managed Instance o a Azure SQL Database.
- **Aplicaciones web:** evalúe las aplicaciones web locales y migrelas a Azure App Service y Azure Kubernetes Service.
- **Escritorios virtuales:** evalúe la infraestructura de escritorio virtual (VDI) local y migrela a Azure Virtual Desktop.
- **Data:** Migrar grandes cantidades de datos a Azure de manera rápida y rentable gracias a los productos de Azure Data Box.

Herramienta	Evaluación y migración	Detalles
Azure Migrate: Discovery and assessment	Descubrimiento y evaluación de servidores, incluidos SQL y aplicaciones web	Detecte y evalúe servidores locales que se ejecutan en VMware, Hyper-V y servidores físicos para preparar la migración a Azure.
Migración y modernización	Migrar servidores	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	Evalué las bases de datos de SQL Server para la migración a Azure SQL Database, Instancia administrada de Azure SQL o máquinas virtuales de Azure que ejecutan SQL Server.	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 SQL Managed Instances.	Esta herramienta permite realizar una migración completa desde varios orígenes de base de datos a plataformas de datos de Azure, con un tiempo de inactividad mínimo.
Movere	Evaluar servidores	Esta herramienta proporciona datos y conclusiones para planificar migraciones a la nube.
Migration Assistant para aplicaciones web	Evalué aplicaciones web locales y migrelas a Azure.	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	Migración de datos sin conexión	Use los productos de Azure Data Box para trasladar grandes cantidades de datos sin conexión a Azure.

Esto es lo que hace la herramienta de detección y evaluación de Azure Migrate:

- **Preparación para Azure:** Evalúa si las máquinas locales están listas para la migración a Azure.
- **Dimensionamiento de Azure:** estima el tamaño de las VM de Azure o el número de nodos de Azure VMware después de la migración.
- **Estimación de costos de Azure:** Calcule el costo de la ejecución de servidores locales en Azure.
- **Análisis de dependencias:** Identifica las dependencias entre servidores y las estrategias de optimización para mover servidores interdependientes a Azure.

La implementación de una gobernanza en la nube adecuada requiere una directiva empresarial correcta, límites de protección y personas cualificadas que adopten un enfoque coherente y disciplinado para la gobernanza.

1. **Metodología:** comprenda la metodología subyacente.
2. **Punto de referencia de la gobernanza:** evalúe su estado actual y las necesidades de estado futuras.
3. **Base de gobernanza:** establezca su base de gobernanza mediante un conjunto de herramientas de gobernanza.
4. **Materias de gobernanza consolidadas:** agregue controles de gobernanza de forma iterativa para abordar los riesgos.

La metodología de control proporciona un enfoque estructurado para consolidar la gobernanza que se requiere para adoptar con confianza la nube.

La **gobernanza** es un tema muy amplio y, quizás, abrumador la primera vez que se aborda. La gobernanza busca establecer el ámbito adecuado de las acciones corporativas mitigando riesgos tangibles mediante la directiva corporativa.

Las directivas corporativas rigen la gobernanza de la nube. Una directiva corporativa adecuada consta de tres componentes:

- **Riesgo empresarial:** identifique y comprenda los riesgos corporativos tangibles y la tolerancia ante riesgos de la organización.
- **Directiva y cumplimiento:** convierta los riesgos en instrucciones de directiva claras que admitan los requisitos de cumplimiento sin definir dependencias técnicas específicas.
- **Proceso:** establezca procesos para supervisar las infracciones y garantizar el cumplimiento de las instrucciones de directiva.

Azure incluye un conjunto de herramientas de gobernanza basadas en la plataforma Azure Resource Manager. La base de gobernanza inicial muestra cómo puede aplicar estas herramientas para demostrar la gobernanza en la nube. A medida que avance en las unidades de este módulo, descubrirá cómo aplicar estas herramientas para resolver los desafíos de gobernanza.

- **Guía de gobernanza estándar:** una guía pensada para la mayoría de las organizaciones que se basa en el modelo recomendado inicial de dos suscripciones. La guía está diseñada para implementaciones en varias regiones, pero no abarca las nubes públicas y soberanas/gubernamentales.
- **Guía de gobernanza para empresas complejas:** una guía para empresas que requieren varias capas de gobernanza. Por ejemplo, para varias unidades de negocio de TI independientes o que incluyen nubes públicas y soberanas/gubernamentales.

**La organización de recursos** se basa en lo que se considera importante para la organización. Antes de definir un grupo de administración o un diseño de suscripciones, es importante comprender cuáles de estas prioridades contrapuestas son más importantes:

- **Transparencia de los costos:** cada adopción de la nube debe alinearse con los departamentos, las unidades de negocio, los proyectos u otros mecanismos de asignación de costos para cumplir los requisitos de contabilidad aplicables a los contracargos y la visualización de costos.
- **Cumplimiento y seguridad:** cada adopción de la nube debe asignarse a requisitos de cumplimiento específicos que asigne la adopción de la nube a estructuras específicas de organización de cumplimiento, seguridad y riesgo.
- **Democratización (responsabilidad delegada):** cada adopción de la nube debe asignarse a equipos, grupos de productos o proyectos para que sea más fácil segmentar la responsabilidad por equipos.

Los tres componentes principales de la organización de recursos son:

- Los **grupos de administración**, que reflejan la seguridad, las operaciones y las jerarquías de los negocios o de la contabilidad.
- Las **suscripciones**, que agrupan recursos similares dentro de límites lógicos.
- Los **grupos de recursos**, que agrupan a su vez aplicaciones o cargas de trabajo en unidades de implementación y de operaciones.

**Nodo primario:** defina una jerarquía de grupos de administración para el entorno de TI corporativo.

**Nodos secundarios:** defina nodos secundarios para cada entorno de producción y de no producción.

**Una suscripción** es un contenedor lógico para todos los recursos implementados. Las suscripciones se usan para agrupar cargas de trabajo comunes en función de requisitos de facturación, cumplimiento, seguridad o acceso. Para maximizar la eficacia de la gobernanza, debe usar el menor número posible de suscripciones.

Para limitar de forma proactiva los costos inesperados, puede usar Azure Policy para crear límites de protección que afecten a la capacidad de cualquier rol de realizar gastos excesivos. Los dos riesgos más habituales relacionados con el costo se deben a malas decisiones:

- **Regiones de Azure:** los costos de los recursos varían de una región de Azure a otra. Siempre que sea posible, use Azure Policy para limitar la implementación de recursos en las regiones.
- **SKU de Azure:** la SKU seleccionada durante la implementación afecta directamente a los costos. Si minimiza el uso de recursos caros en las suscripciones de autoservicio o de propiedad de carga de trabajo, podrá limitar la posibilidad de salirse del presupuesto de forma inesperada.

Una línea base de administración es el conjunto mínimo de herramientas que se debe aplicar a todos los recursos del entorno. Este módulo le guía por las tres materias de una línea base de administración de la nube:

- **Inventario y visibilidad:** inventario de recursos y creación de visibilidad del estado de ejecución de cada recurso de una carga de trabajo
- **Cumplimiento operativo:** la administración de la configuración, el dimensionamiento, los costos y el rendimiento de los recursos
- **Protección y recuperación:** protección de datos y recuperación rápida para minimizar las interrupciones operativas

**La materia del cumplimiento operativo** es la piedra angular para mantener el equilibrio entre seguridad, gobernanza, rendimiento y costo. Para un cumplimiento operativo eficaz se requiere coherencia en algunos procesos críticos:

- **Coherencia de recursos:** si todos los recursos se organizan y se etiquetan de la misma manera, otras tareas de administración serán más fáciles de administrar.
- **Coherencia del entorno:** si todas las zonas de aterrizaje están organizadas de la misma manera, la administración y la solución de problemas son mucho más fáciles de administrar.
- **Coherencia en la configuración de los recursos:** como sucede con los recursos y las zonas de aterrizaje, es fundamental supervisar la configuración de los recursos. Si se cambia un valor de configuración, se puede desencadenar un trabajo de automatización para restaurar el entorno.
- **Optimización de recursos:** la supervisión periódica del rendimiento de los recursos revela tendencias en el uso de recursos y oportunidades para optimizar el costo y el rendimiento de cada recurso.
- **Coherencia de actualización:** todas las actualizaciones del entorno se deben realizar de forma programada, controlada y posiblemente automatizada. La administración de cambios controlada reduce las interrupciones y la solución de problemas innecesarias.
- **Automatización de las correcciones:** la automatización para la corrección rápida de incidentes comunes es una excelente manera de aumentar la satisfacción del cliente y minimizar las interrupciones. Sin embargo, debe corregir los problemas conocidos por sus causas principales. Pero la causa principal suele suponer un proceso largo y la automatización es una solución rápida.

La especialización de plataformas y cargas de trabajo consiste en la ejecución disciplinada de los cuatro procesos siguientes en un enfoque iterativo:

- **Mejora del diseño del sistema:** la deuda técnica y los errores arquitectónicos son la causa principal de la mayoría de las interrupciones de las cargas de trabajo. Al revisar el diseño de la plataforma o de la carga de trabajo, se puede mejorar la estabilidad. El Marco de buena arquitectura de Azure incluye recomendaciones para mejorar la calidad de la plataforma o una carga de trabajo específica.
- **Corrección automática:** algunas mejoras de diseño no son rentables, ya que la deuda técnica puede ser demasiado costosa o compleja de mejorar. En tales casos, es posible que tenga más sentido automatizar la corrección y reducir el efecto de las interrupciones.
- **Escalado de la solución:** a medida que se mejoran el diseño de sistemas y la corrección automática, los cambios se pueden escalar en el entorno mediante el catálogo de servicios. Puede publicar soluciones y plataformas optimizadas en el centro de Azure Managed Applications para reutilizarlas fácilmente en otras cargas de trabajo o clientes externos.
- **Mejora continua:** obtendrá información valiosa para la siguiente revisión del sistema mediante la recopilación de comentarios de usuarios, administradores y clientes. También es importante recopilar y visualizar los registros críticos del sistema y los datos de rendimiento. Los comentarios y los datos recopilados se usarán como base para tomar nuevas decisiones sobre futuras mejoras del sistema.

**La modularidad** es una técnica conocida para reducir la complejidad en la arquitectura de sistemas complejos. Si un sistema es una interacción compleja de muchas partes que no se pueden separar (a menudo denominada "monolítica"), las interdependencias estrechas de componentes dificultan las mejoras del sistema. Cada cambio debe validarse con el resto del sistema, por lo que el proceso de prueba es complejo.

**Las arquitecturas de microservicios** son patrones de aplicación que aprovechan la modularidad. Las aplicaciones se subdividen en componentes independientes y pequeños que se pueden desarrollar de forma independiente entre sí, incluso con lenguajes de programación diferentes. Cada componente, o microservicio, puede funcionar por sí solo. Puede escalarlo según sea necesario, solucionar sus problemas como una sola unidad y modificarlo independientemente de los otros microservicios.

**Azure App Service** es una plataforma en la que las organizaciones pueden ejecutar sus cargas de trabajo basadas en web sin tener que administrar ningún orquestador o sistema operativo subyacente. El único requisito es cargar el código de aplicación en el servicio mediante uno de los muchos métodos de implementación disponibles. Azure se ocupa del resto: escalar y reducir horizontalmente la aplicación, aplicar revisiones y mantener las máquinas virtuales subyacentes, entre otras cosas, sin necesidad de adoptar la curva de aprendizaje de Kubernetes.

Azure App Service admite cargas de trabajo basadas en contenedores, por lo que puede cargar la imagen de contenedor en lugar del código de la aplicación. También admite cargas de trabajo de Linux y Windows, así como muchos entornos de ejecución de aplicaciones diferentes.

Azure App Service admite varios modelos de precios, incluida una opción sin servidor denominada Azure Functions. En Azure Functions, solo se cobra la utilización de la aplicación. No hay costos fijos.

**El modelo sin servidor** es interesante para innovar, ya que permite implementar microservicios nuevos sin incurrir en facturas mensuales elevadas en caso de que el mercado no los acepte. Este modelo es otro ejemplo de la estrategia con respuesta rápida a errores, donde la innovación no significa necesariamente gastos elevados.

**La metodología segura** de Microsoft Cloud Adoption Framework para Azure proporciona una visión completa del estado final para guiar la mejora del programa de seguridad a lo largo del tiempo. La metodología segura proporciona un puente entre su transformación digital empresarial y su programa y estrategia de seguridad. También proporciona instrucciones estructuradas para modernizar las materias de seguridad.

Centre su programa de seguridad en la alineación empresarial en tres categorías:

- **Información sobre riesgos:** permite alinear e integrar la información sobre seguridad y sobre señales u orígenes del riesgo con las iniciativas empresariales. Asegúrese de que los procesos repetibles sirvan para educar a todos los equipos en la aplicación de esa información y que los equipos sean responsables de las mejoras.
- **Integración de seguridad:** Integre conocimientos, aptitudes e información de seguridad más profundamente en las operaciones empresariales diarias y el entorno de TI. Use procesos repetibles y desarrolle una asociación profunda en todos los niveles de la organización.
- **Resistencia empresarial:** evite tantos ataques como sea posible y limite el daño de esos ataques para fomentar la resistencia de la organización. Asegúrese de que puede continuar las operaciones durante un ataque incluso si se encuentra en un estado degradado.