

Azure AZ-900

Parte 1 - Conceptos básicos de Azure

Azure es una plataforma de informática en la nube → Desde hosting básico hasta soluciones de software personalizadas (IaaS/ PaaS/ SaaS).

- Almacenamiento remoto
- Hospedaje de bases de datos
- Administración centralizada de cuentas
- IA + IoT

Nube

Es la entrega de servicios informáticos a través de Internet (servidores, almacenamiento, bases de datos, redes, software, análisis e inteligencia.).

Es mas barato porque te permite:

- Reducir los costos operativos.
- Ejecutar la infraestructura de forma más eficaz.
- Escalar a medida que cambien las necesidades empresariales.

Ventajas

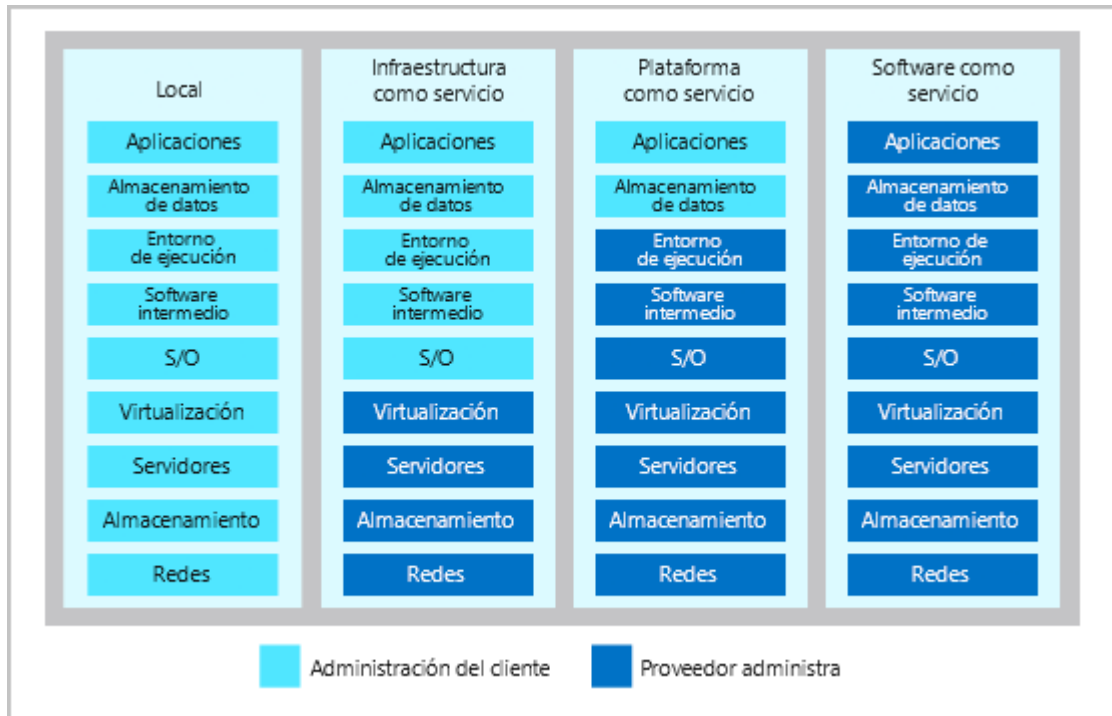
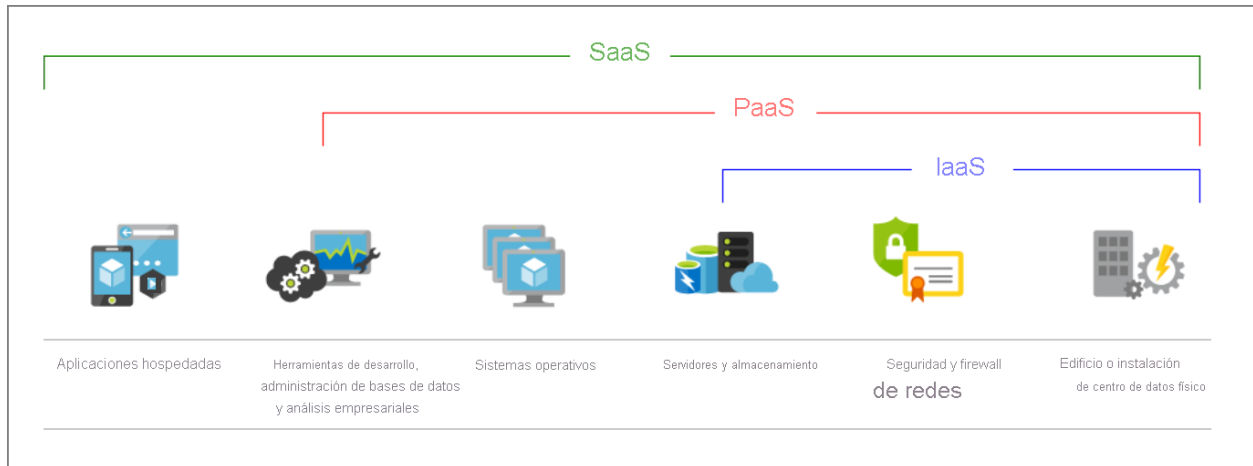
Confiabilidad, Escalabilidad (vertical y horizontalmente), Elasticidad, Agilidad, Distribución geográfica, recuperación ante desastres.

Modelos de servicio

- **Infraestructura como servicio (IaaS)** - Un proveedor de servicios en la nube mantiene actualizado el hardware, pero el mantenimiento del sistema operativo y la configuración de red es responsabilidad del inquilino de nube.
- **Plataforma como servicio (PaaS)** - El proveedor de servicios en la nube administra las máquinas virtuales y los recursos de red, y el inquilino de nube implementa sus

aplicaciones en el entorno de hospedaje administrado (Azure App Services).

- **Software como servicio (SaaS)** - el proveedor de servicios en la nube administra todos los aspectos del entorno de la aplicación, como las máquinas virtuales, los recursos de red, el almacenamiento de datos y las aplicaciones (Office 365)



Serverless

En las aplicaciones sin servidor, el proveedor de servicios en la nube aprovisiona, escala y administra automáticamente la infraestructura necesaria para ejecutar el código.

Tipos de nube

- Nube pública - disponibles para cualquiera que quiera comprarlos.
- Nube privada - uso exclusivo de los usuarios de una empresa u organización.
- Nube híbrida - combina una nube pública y una nube privada (Azure).

Azure portal

Es una consola unificada basada en web que proporciona una alternativa a las herramientas de línea de comandos.

Azure marketplace: proveedores de software independientes y nuevas empresas que ofrecen sus soluciones y servicios, optimizados para ejecutarse en Azure.

Servicios de Azure



Servicios de infraestructura

1. **Procesos** (compute services) - máquinas virtuales, contenedores y Kubernetes, Azure functions (serverless y microservicios).
2. **Redes** (Networking) - vpn, load balancer, dns, traffic manager, app gateways, express route, DDoS Protection.
3. **Almacenamiento** (cloud storage) - Archivos (servidor de archivos), discos, Table (almacenamiento NoSQL para datos no estructurados), Queue storage (colas para mensaje entre apps), blob (objetos grandes como videos).



Servicio de plataforma

1. **Movil** (app hosting) - servicios de back-end móviles para aplicaciones iOS, Android y Windows

2. **Bases de datos** (app hosting) - bases de datos relacionales como Postgres, MySQL, SQL Server, Maria DB, etc.
3. **Web** (app hosting) - compilar y hospedar aplicaciones web y servicios web basados en HTTP.
4. **IoT** (Internet of things) - supervisión y la administración de los recursos de IoT a escala (Hubs, dashboards, apps).
5. **Macrodatos** (Big Data) - Synapse Analytics (almacenamiento y consulta), HDInsight (procesamiento Hadoop) y Databricks (análisis colaborativo Apache Spark).
6. **IA** (Artificial Intelligence) - Machine Learning Service (desarrollar y entrenar modelos), ML Studio (área visual con algoritmos predefinidos) y Cognitive Services (API precompiladas de vision, vpz, pln, Bing search y asignación de conocimiento).
7. **Devops** (Integration) - automatización de la entrega de software (pruebas, integración continua, etc)
8. **Seguridad** (Security) - Security center, active directory, key vault, multifactor authentication.

Todos estos incluyen durabilidad, seguridad, escalabilidad, administración y accesibilidad.

Componentes principales de la arquitectura de Azure

La estructura organizativa de los recursos de Azure consta de cuatro niveles:

- **Grupos de administración** - administrar el acceso, las directivas y el cumplimiento de varias suscripciones.
- **Suscripciones** - agrupa las cuentas de usuario y los recursos que han creado esas cuentas de usuario.
- **Grupos de recursos** - contenedor lógico en el que se implementan y administran recursos (flexible).
- **Recursos** - instancias de servicios.

Suscripciones

Una suscripción de Azure es una unidad lógica de servicios de Azure que está vinculada a una cuenta de Azure, que es una identidad en Azure Active Directory y definir límites en torno a los productos, servicios y recursos de Azure.

- Límite de facturación
- Límite de control de acceso

Se pueden crear distintas suscripciones para separar entornos, estructuras organizativas y facturación.

Grupos de administración

Los grupos de administración de Azure ofrecen un nivel de ámbito que está por encima de las suscripciones. Las suscripciones se organizan en contenedores llamados grupos de administración y las condiciones de gobernanza se aplican a 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.
- Cada grupo de administración puede tener muchos elementos secundarios.
- Todas las suscripciones y grupos de administración están dentro de una única jerarquía en cada directorio.

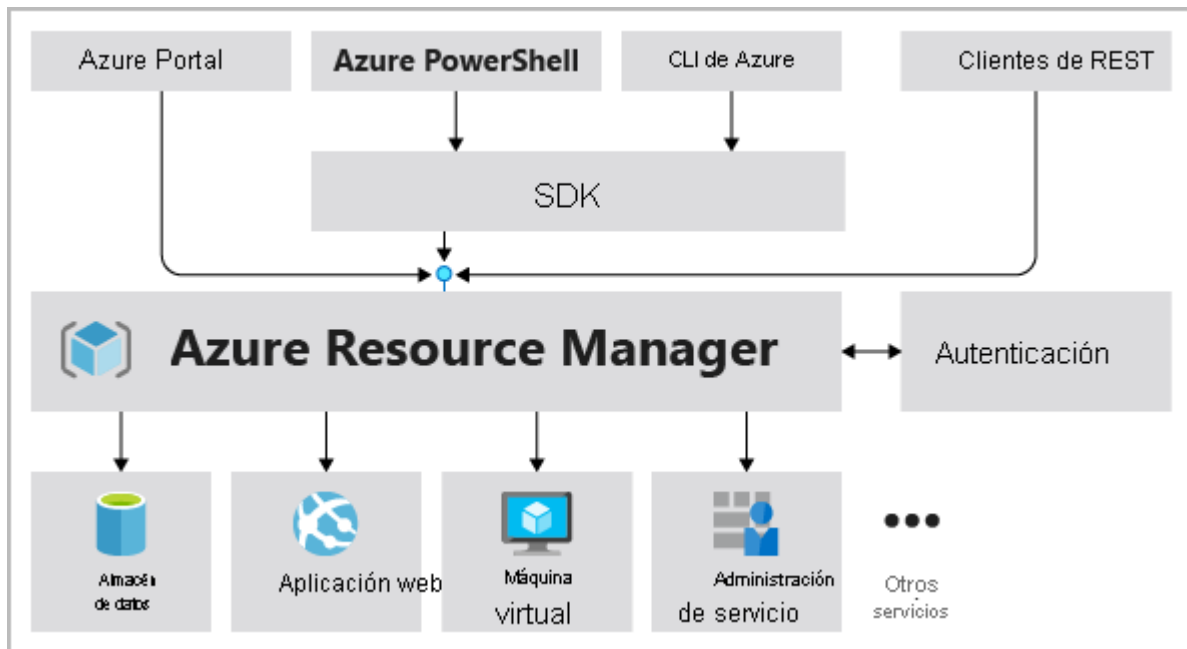
Grupo de recursos

Los grupos de recursos existen para ayudar a administrar y organizar los recursos de Azure. Al colocar recursos de uso, tipo o ubicación similar en un grupo de recursos, puede proporcionar orden y organización a los recursos que cree en Azure.

- **Ciclo de vida** - Si elimina un grupo de recursos, también se eliminarán todos los recursos que contenga.
- **Autorización** - se pueden aplicar permisos de control de acceso basado en roles (RBAC).

Azure Resource Manager

Proporciona una capa de administración que le permite crear, actualizar y eliminar recursos de la cuenta de Azure.



Todas las funcionalidades que están disponibles en Azure Portal también lo están a través de PowerShell, la CLI de Azure, las API REST y los SDK de cliente.

Regiones y zonas

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

- **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).

Pares de regiones: Cada región de Azure se empareja siempre 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.

Conceptos de Azure

App Service es un servicio basado en HTTP que permite crear y hospedar muchos tipos de soluciones basadas en la Web sin necesidad de administrar la infraestructura.

Azure Marketplace es una tienda en línea que hospeda aplicaciones certificadas y optimizadas para ejecutarse en Azure.

Parte 2 - Servicios básicos de Azure

2.1 Análisis y bases de datos

Azure Cosmos DB - es un servicio de base de datos de varios modelos distribuido globalmente compatible con datos sin esquema. Los datos se abstraen y se proyectan como una API, que se especifica al crear la base de datos. Entre las opciones se incluyen SQL, MongoDB, Cassandra, Tables y Gremlin .



Sirve cuando quieres migrar distintas bases de datos en tecnologías y estructuras diferentes (NoSQL).

Azure SQL Database - base de datos relacional basada en la última versión estable del motor de base de datos de Microsoft SQL Server totalmente administrada (PaaS). Controla las actualizaciones, las aplicaciones de revisiones, las copias de seguridad y la supervisión, sin intervención del usuario.



Sirven cuando se quieren migrar servidores locales que ejecutan SQL Server con Azure Database Migration Service.

Azure SQL Managed Instance - servicio de datos en la nube escalable que proporciona la mayor compatibilidad con el motor de base de datos de SQL Server con todas las ventajas de una plataforma como servicio totalmente administrada.

Flujo del proceso de migración

Guía paso a paso



Es básicamente lo mismo que **Azure SQL Database** pero con mas funciones.

Azure Database for MySQL - servicio de bases de datos relacionales en la nube, y se basa en el motor de base de datos de MySQL Community Edition.

Azure Database for PostgreSQL - El software de servidor se basa en la versión de la comunidad del motor de base de datos de PostgreSQL de código abierto. Está disponible en dos opciones de implementación: Servidor único e Hiperescala (Citus).

Exploración de análisis y macrodatos - Azure Synapse Analytics (big data Warehouse), Azure HDInsight (spark, hadoop, Kafka, HBase), Azure Databricks (IA, TensorFlow, PyTorch y Scikit-learn) y Azure Data Lake Analytics (análisis a petición).

2.2 Servicios de Azure Compute

Azure Compute es un servicio de informática a petición para ejecutar aplicaciones basadas en la nube. El servicio es compatible con Linux, Windows Server, SQL Server, Oracle, IBM y SAP.

Azure Virtual Machines (IaaS) - Incluyen un procesador virtual, memoria, almacenamiento y recursos de red y se manejan mediante un cliente de escritorio remoto. También existen los conjuntos de escalado de máquinas virtuales idénticas.

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

Los conjuntos de escalado le permiten administrar, configurar y actualizar de forma centralizada un gran número de máquinas virtuales en cuestión de minutos para proporcionar aplicaciones altamente disponibles de carga equilibrada.

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 necesite un control total sobre el entorno y el sistema operativo, las máquinas virtuales son la opción idónea

Azure Container Instances y Kubernetes - implementar contenedores (entornos de aplicación ligeros y virtualizados) y administrarlos. Los contenedores son una excelente opción si quiere ejecutar varias instancias de una aplicación en un solo equipo host.

Las máquinas virtuales virtualizan el hardware mientras que los contenedores virtualizan el sistema operativo. Son instancias más ligeras y fáciles de escalar y pueden funcionar en cluster.

- Azure Container Instances - Es una oferta de plataforma como servicio (PaaS) que permite cargar los contenedores, que se ejecutan automáticamente.
- Azure Kubernetes Service (AKS) - La tarea de automatizar y administrar una gran cantidad de contenedores (y de interactuar con ellos) se conoce como orquestación.

- Microservicio - Servicio web individual que consiste en una implementación de un conjunto de los mismos para albergar diferentes funcionalidades de un negocio (ej. front, back, bases de datos). Son mejor opción cuando se tiene una aplicación compleja que requiera de una alta velocidad de release.



Ejecutar varias instancias de una aplicación en contenedores en un único equipo host. Los contenedores se usan normalmente para crear soluciones mediante una arquitectura de microservicios.

Azure App Service (PaaS) - compilar, implementar y escalar de forma rápida aplicaciones de nivel empresarial en una plataforma totalmente administrada. El plan de App Service determina la cantidad de hardware dedicado al host. Puede hospedar:

- Aplicaciones web
- Aplicaciones de API
- Trabajos web
- Aplicaciones móviles

WebJobs - Los trabajos web suelen usarse para ejecutar tareas en segundo plano como parte de la lógica de aplicación.

- Almacenar los datos de aplicaciones móviles en una base de datos SQL basada en la nube.
- Autenticar a clientes con proveedores sociales comunes, como MSA, Google, Twitter y Facebook.
- Enviar notificaciones de inserción.
- Ejecutar lógica de back-end personalizada en C# o Node.js.

Azure Functions (*serverless*) - Se usan normalmente cuando se debe realizar un trabajo en respuesta a un evento (a menudo a través de una solicitud REST), un temporizador o un mensaje de otro servicio de Azure.

La informática sin servidor es la abstracción de los servidores, la infraestructura y los sistemas operativos. Incluye la abstracción de servidores, un escalado controlado por eventos y la microfacturación.

- Temporizadores, por ejemplo, si una función tiene que ejecutarse todos los días a las 10:00 UTC.
 - HTTP, por ejemplo, escenarios de API y webhook.
 - Colas, por ejemplo, con procesamiento de pedidos.
 - Y mucho más.
-
- **Azure Functions:** las funciones pueden ejecutar código en prácticamente cualquier lenguaje moderno.
 - **Azure Logic Apps:** las aplicaciones lógicas están diseñadas en web y pueden ejecutar lógica desencadenada mediante servicios de Azure sin escribir código



Es una opción ideal si le preocupa solo el código que ejecuta el servicio y no la infraestructura o la plataforma subyacente.

Windows Virtual Desktop - es un servicio de virtualización de escritorio y de aplicaciones que se ejecuta en la nube.

2.3 Azure Storage

Servicio que puede usar para almacenar archivos, mensajes, tablas y otros tipos de información.

Disk storage (IaaS) - proporciona discos para Azure Virtual Machines. Disk Storage permite que los datos se almacenen de forma persistente y que se acceda a ellos desde un disco duro virtual conectado. Estos pueden ser de diferentes capacidades o SSD/HDD.

Azure Blob storage - Puede almacenar grandes cantidades de datos, es no estructurado, lo que significa que no hay ninguna restricción en cuanto a los tipos de datos que puede contener.

- 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.
- Almacenamiento de hasta 8 TB de datos para máquinas virtuales.



Una ventaja del almacenamiento en blobs con respecto al almacenamiento en disco es que no requiere que los desarrolladores piensen en discos o los administren; los datos se cargan como blobs y Azure se encarga de las necesidades de almacenamiento físico. Es como un bucket.

Niveles de acceso, ayuda a almacenar datos de objetos de la manera más rentable: acceso frecuente, acceso esporádico, acceso de archivo.

Azure Files - ofrece recursos compartidos de archivos totalmente administrados en la nube.



Sirven especialmente para tener archivos compartidos en la nube, como datos de aplicaciones, datos de diagnóstico, archivos de configuración, etc. Es como un Drive.

2.4 Servicios de Red de Azure

Azure Virtual Network - 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.

- Aislamiento y segmentación (dividir espacios de direcciones IP en subredes)
- Comunicación con Internet (manejar una IP pública)
- Comunicación entre recursos de Azure (redes virtuales y puntos de conexión de servicio)
- Comunicación con los recursos locales
- Enrutamiento del tráfico de red (tablas de ruta y protocolo de puerta de enlace de borde)
- Filtrado del tráfico de red (grupos de seguridad de red y aplicaciones virtuales de red)
- Conexión de redes virtuales

Para configurar una Azure Virtual Network básica se define el nombre de la red, espacio de direcciones (no se deben superponer), suscripción, grupo de recursos, ubicación, subred, DDoS, Puntos de conexión de servicio.

Azure VPN Gateway - Es un túnel cifrado que sirve para conectar varias VPNs a través de internet, cifrando el tráfico mientras viaja para evitar ataques de interceptación. Se implementan en instancias de Azure Virtual Network y habilitan 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*.

Redes privadas basadas en directivas son de enrutamiento estáticas para casos específicos como compatibilidad de dispositivos y las basadas en rutas son dinámicas se modelan como una interfaz de red, el enrutamiento decide cuál de estas interfaces de túnel se va a usar al enviar cada paquete.

Para implementarlas es necesario contar con los siguientes recursos de Azure: Red virtual, Gateway subnet, Dirección IP pública, Puerta de enlace de red local y virtual, conexión.

Hay varias opciones para escenarios de alta disponibilidad como configuraciones de 2 instancias de VPN Gateways activas o en espera y de conmutación por error de ExpressRoute o puertas de enlace con redundancia de zona.

Azure ExpressRoute - permite ampliar las redes locales a la nube con servicios como Microsoft Azure y Microsoft 365 mediante una conexión privada con la ayuda de un proveedor de conectividad (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.

Ventajas:

- Conectividad de nivel 3 entre su red local y Microsoft Cloud a través de un proveedor de conectividad.
- Redundancia integrada.
- Conectividad con los Servicios en la nube de Microsoft
- Conectividad local con Global Reach de ExpressRoute
- Enrutamiento dinámico

ExpressRoute admite tres 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

3. Soluciones y Herramientas de Administración de Azure

3.1 Servicios de IA

El objetivo de la IA es crear un sistema de software que pueda adaptarse o aprender algo por sí mismo sin estar programado explícitamente para hacerlo.

- Aprendizaje profundo (deep learning) - modela en la red neuronal de la mente humana, lo que le permite descubrir, aprender y crecer a través de la experiencia.
- Aprendizaje automático (machine learning) - usa los datos existentes para entrenar un modelo, probarlo y aplicarlo a nuevos datos para pronosticar comportamientos, resultados y tendencias futuros.

Azure Machine Learning - Permite crear modelos para realizar predicciones, puede implementarlo y usarlo en tiempo real a través de un punto de conexión de API web.



Cuando los científicos de datos necesiten un control completo sobre el diseño y el entrenamiento de un algoritmo con sus propios datos. Uso de datos propios.

Azure Cognitive Services - proporciona modelos de aprendizaje automático creados previamente que permiten integrar visión, voz, lenguaje y decisión. Personalizar de Azure Cognitive Services te permite predecir el comportamiento del usuario o proporcionar recomendaciones personalizadas a los usuarios.



Sirve para la solución de problemas generales con acceso a través de API sin conocimiento sobre aprendizaje automático.

Azure Bot Service - son plataformas para crear agentes virtuales que comprenden y responden a preguntas como un ser humano. Existen soluciones precompiladas sin

código que abarquen los escenarios habituales como QnA Maker o Power Virtual Agents o interacciones más complejas con Microsoft Bot Framework.

3.2 Herramientas para crear soluciones (desarrollo de software)

Elegir los servicios y herramientas para los procesos de desarrollo de software que adapten mejor un escenario empresarial determinado.

DevOps es un nuevo enfoque que ayuda a alinear los equipos técnicos que trabajan para conseguir un objetivo común. Su objetivo consiste en agilizar el lanzamiento de los cambios de software, garantizar la implementación continua del sistema y asegurar que todos los cambios cumplen un nivel alto de calidad.

Azure DevOps Services (SaaS) - es un conjunto de servicios que aborda cada fase del ciclo de vida de desarrollo de software.

- Azure Repos
- Azure Boards
- Azure Pipelines (CI/CD)
- Azure Artifacts (artefactos como código fuente compilado)
- Azure Test Plans (pruebas automatizadas)



Entorno empresarial y más nivel de permisos y reportes.

GitHub y Acciones de GitHub - herramienta de administración de código fuente descentralizada. Acciones de GitHub permite la automatización del flujo de trabajo con desencadenadores para muchos eventos del ciclo de vida.



Código abierto y comunidad.

Azure DevTest Labs - medio automatizado para administrar el proceso de compilación, configuración y anulación de máquinas virtuales que contienen las compilaciones de los proyectos de software.



Control de calidad.

3.3 Visibilidad, información y mitigación de interrupciones

Elegir los servicios de supervisión en la nube que mejor aborden los desafíos empresariales a los que se enfrenta su organización. investigar problemas intermitentes, optimizar el uso y mantener una actitud proactiva en el control de los tiempos de inactividad planeados.

Azure Advisor - evalúa los recursos de Azure y hace recomendaciones que contribuyen a mejorar la confiabilidad, la seguridad y el rendimiento, lograr la excelencia operativa y reducir los costos. Recomendaciones para suscripciones, grupos de recursos o servicios específicos.

- Confiabilidad
- Seguridad
- Rendimiento
- Costos
- Excelencia Operativa

Azure Monitor - permite recopilar, analizar y mostrar datos, así como llevar a cabo acciones en función de las métricas y los datos registrados en todo el entorno local y de Azure. Cuenta con alertas para situaciones específicas.

Azure Service Health - vista personalizada del estado de los servicios, regiones y recursos de Azure en los que se basa su infraestructura. Proporciona informes de incidentes oficiales, llamados análisis de la causa principal (RCA) para los siguientes tipos de eventos:

- Problemas de servicio.
- Mantenimiento planeado.
- Avisos de estado.

3.4 Herramientas para admin y config Azure

Mediante las herramientas de administración de Azure, los administradores y desarrolladores pueden interactuar con el entorno de nube para realizar tareas como:

- Implementar decenas o cientos de recursos a la vez.
- Configurar servicios individuales mediante programación.
- Ver informes enriquecidos relativos al uso, el mantenimiento, los costos y mucho más.

Herramientas visuales.

El Portal de Azure - dispone de una UI gráfica sencilla en la que se pueden ver todos los servicios que se están usando, crear servicios nuevos, configurar los servicios y ver informes.

Azure Mobile App - permite acceder a los recursos de Azure desde iOS y Android para supervisar recursos, consultar alertas o ejecutar comandos desde la CLI.

Herramientas basadas en código - Infraestructura como código, el código imperativo detalla cada uno de los pasos que debe realizarse para lograr un resultado deseado. Por el contrario, el código declarativo solo detalla un resultado deseado, y es el intérprete quien debe decidir cuál es la mejor forma de lograr dicho resultado.

Azure PowerShell (imperativo)- ejecutar comandos denominados cmdlets o command-lets. Pueden ejecutarse de forma independiente o combinarse en un archivo de script y

ejecutarse en conjunto para organizar:

- La configuración de rutinas, la anulación y el mantenimiento de un único recurso o de varios recursos conectados.
- La implementación de una infraestructura completa, que puede contener decenas o cientos de recursos, de código imperativo.

CLI de Azure (interfaz de línea de comandos) (imperativo)- es un programa ejecutable que permite ejecutar comandos en Bash.

Plantillas de ARM (Azure Resource Manager) (declarativo)- puede describir los recursos que quiere usar en un formato JSON declarativo.

Las plantillas de Resource Manager expresan los requisitos de infraestructura de la aplicación para una implementación que se pueda repetir. Un paso de validación garantiza que se puedan crear todos los recursos, de modo que los recursos se creen en el orden adecuado en función de las dependencias, en paralelo, y sean idempotentes.

3.5 Tecnología sin servidor de Azure (serverless)

Se usa para describir un entorno de ejecución que se configura y administra de manera automática y puede hacer un escalado instantáneo para satisfacer la demanda.

La informática sin servidor suele utilizarse para controlar los escenarios de back-end. En otras palabras, la informática sin servidor es responsable de enviar mensajes de un sistema a otro o de procesar mensajes enviados desde otros sistemas. No se usa para sistemas orientados al usuario, sino que funciona en segundo plano.

Azure Functions - puede hospedar un único método o función mediante un lenguaje de programación popular en la nube que se ejecuta en respuesta a un evento. Un ejemplo de un evento podría ser una solicitud HTTP, un mensaje nuevo en una cola o un mensaje en un temporizador.



La solución Azure Functions es ideal si le preocupa solo el código que ejecuta el servicio y no la infraestructura o la plataforma subyacente.

Azure Logic Apps (orquestración)- plataforma de desarrollo de poco código o sin código hospedada como un servicio en la nube. Ayuda a automatizar y organizar tareas, procesos empresariales y flujos de trabajo cuando tiene que integrar aplicaciones, datos, sistemas y servicios en empresas u organizaciones.

Para crear soluciones de integración empresarial con Azure Logic Apps, se puede elegir entre una galería creciente de más de 200 conectores. La galería incluye servicios como Salesforce, SAP, Oracle DB y recursos compartidos de archivos.

3.6 Servicio de Azure IoT

Permite a los dispositivos recopilar y luego retransmitir información para el análisis de datos.

Azure IoT Hub - un servicio administrado hospedado en la nube que actúa como centro de mensajes centralizado para la comunicación bidireccional entre la aplicación de IoT y los dispositivos que administra.

Azure IoT Central (GUI) - se basa en IoT Hub y agrega un panel que le permite conectar, supervisar y administrar sus dispositivos de IoT. La interfaz de usuario (UI) visual facilita la conexión rápida de nuevos dispositivos y la inspección a medida que comienzan a enviar mensajes de telemetría o de error.

Puede usar la interfaz de usuario para controlar los dispositivos de forma remota. Esta característica permite enviar una actualización de software o modificar una propiedad del dispositivo. Las plantillas de dispositivo permiten conectar un dispositivo sin ningún código de servicio.

Azure Sphere - crea una solución de IoT de un extremo a otro de alta seguridad para los clientes que lo abarca todo, desde el hardware y el sistema operativo del dispositivo hasta el método seguro para enviar mensajes desde el dispositivo al centro de mensajes. Integra:

- Microcontrolador
- Sistema Operativo
- Seguridad y autenticación (AS3)

4. Seguridad general y de Seguridad de red

4.1 Seguridad General

Azure Security Center - servicio de supervisión que proporciona visibilidad del nivel de seguridad en todos los servicios, tanto en Azure como en el entorno local.

- Supervisar la configuración de seguridad
- Aplicar automáticamente la configuración de seguridad necesaria a los nuevos recursos
- Proporcionar recomendaciones de seguridad
- Supervisar de forma continua los recursos y realizar valoraciones de seguridad automáticas
- Usar el aprendizaje automático para detectar y bloquear la instalación de malware en las máquinas virtuales (VM)
- Detectar y analizar posibles ataques entrantes e investigar amenazas
- Proporcionar control de acceso Just-in-Time a los puertos de red.

La puntuación de seguridad es una medida del nivel de seguridad de una organización basada en controles de seguridad, o en grupos de recomendaciones de seguridad relacionadas. Incluye funciones avanzadas de defensa en la nube para máquinas virtuales, seguridad de red e integridad de archivos. Se puede conectar con App Logic para generar alertas o automatizaciones del flujo de trabajo.



Servicio de seguridad integral para los recursos de Azure.

Azure Sentinel - sistema de administración de eventos e información de seguridad (SIEM) dedicado para administrar a escala. Usa análisis de seguridad inteligente y análisis de amenazas.

- Recopilar datos en la nube a gran escala
- Detectar amenazas no detectadas anteriormente
- Investigar amenazas con inteligencia artificial
- Responder a incidentes rápidamente

Azure Sentinel admite una serie de orígenes de datos que puede analizar en busca de eventos de seguridad. Estas conexiones las administran conectores integrados o API y formatos de registro estándar del sector.

- Conexión de soluciones de Microsoft
- Conexión con otros servicios y soluciones
- Conexión con orígenes de datos estándar del sector (CEF, Syslog y API)



Sirve mas para recopilar datos de distintas herramientas, no solo de Azure.

Azure Key Vault - s un servicio en la nube centralizado para almacenar los secretos de la aplicación en una única ubicación central.

- Administración de secretos (tokens, contraseñas, certificados, claves API, etc)
- Administrar claves de cifrado
- Administrar certificados SSL/TLS
- Almacenar secretos respaldados por módulos de seguridad de hardware (HSM)

Sus ventajas son la centralización de secretos, almacenarlos de manera segura, supervisión y control de acceso, admin simplificada e integración con otros servicios de Azure.

Azure Dedicated Host - proporciona servidores físicos dedicados para hospedar las máquinas virtuales de Azure para Windows y Linux.

- Ofrece visibilidad y control sobre la infraestructura de servidor que ejecuta las máquinas virtuales de Azure.

- Ayuda a satisfacer requisitos de cumplimiento mediante la implementación de las cargas de trabajo en un servidor aislado.
- Permite elegir el número de procesadores, capacidades de servidor, series de máquinas virtuales y tamaños de máquina virtual dentro del mismo host.

4.2 Seguridad en redes

El objetivo de la defensa en profundidad es proteger la información y evitar que personas no autorizadas a acceder a ella puedan sustraerla. Azure proporciona herramientas y características de seguridad en todas las capas del concepto de defensa en profundidad.

- Seguridad física
- Identidad y acceso (control de la infraestructura)
- Perímetro (protección contra DDoS y Firewalls)
- Network (red y conexiones seguras entre los recursos)
- Proceso (acceso a máquinas virtuales)
- Aplicación (mitigar vulnerabilidades y seguridad en el diseño de apps)
- Datos (bases, discos, SaaS, archivos, etc)

Los principios comunes usados para definir un nivel de seguridad son lo que se conoce colectivamente como CIA por sus siglas en inglés.:

- La confidencialidad (restringir el acceso a la información únicamente a los usuarios a las que se concede acceso de forma explícita).
- La integridad evitar cambios no autorizados en la información cuando se almacenan o transfieren.
- La disponibilidad, Asegúrese de que los servicios funcionan y que solo pueden acceder a ellos los usuarios autorizados.

Azure Firewall - es un servicio de seguridad de red administrado y basado en la nube que supervisa el tráfico de red entrante y saliente y decide si se permite o bloquea un

tráfico específico en función de un conjunto definido de reglas de seguridad.

Un firewall con estado analiza el contexto completo de una conexión de red, no solo un paquete individual de tráfico de red.

- Alta disponibilidad integrada
- Escalabilidad en la nube sin restricciones.
- Reglas de filtrado entrante y saliente.
- Compatibilidad con la traducción de direcciones de red de destino (DNAT).
- El registro de Azure Monitor.

Azure DDoS Protection - ayuda a proteger sus recursos de Azure frente a ataques DDoS. El servicio DDoS Protection ayuda a proteger las aplicaciones de Azure al analizar y descartar el tráfico de DDoS en la red perimetral de Azure antes de que afecte a la disponibilidad del servicio. DDoS Protection Estándar ayuda a garantizar que la carga de red que se procesa refleja el uso del cliente y no se cobre de más.

Niveles de protección:

- Basic, El nivel de servicio básico está habilitado de forma automática sin coste como parte de la suscripción de Azure.
- Estándar, funcionalidades adicionales de mitigación adaptadas específicamente a los recursos de Azure Virtual Network.

Grupos de seguridad de red (NSG) - permite filtrar el tráfico de red desde y hacia los recursos de Azure en una red virtual de Azure. Es como un Firewall interno. Un NSG puede contener varias reglas de seguridad entrantes y salientes que permiten filtrar el tráfico con los recursos por dirección IP de origen y destino, puerto y protocolo.

Cuando se crea un grupo de seguridad de red, Azure crea una serie de reglas predeterminadas para proporcionar un nivel de línea de base de seguridad.

5. Características de identidad, gobernanza, privacidad y cumplimiento

5.1 Servicios de identidad de Azure

La identidad se ha convertido en el nuevo límite de seguridad principal. Para mantener el control de los datos, es fundamental que el usuario demuestre con exactitud que es un usuario válido del sistema y que cuenta con un nivel de acceso adecuado.

- Autenticación (AuthN) - es el proceso de establecimiento de la identidad de una persona o servicio que quiere acceder a un recurso. Implica el acto de solicitar a un usuario credenciales legítimas y proporciona la base para la creación de una entidad de seguridad para el control de identidad y de acceso.
- Autorización (AuthZ) - es el proceso de establecer el nivel de acceso que tiene una persona o un servicio autenticados. Especifica a qué datos puede acceder y qué puede hacer con ellos.

Azure Active Directory (Azure AD) - es un servicio de administración de acceso e identidades basado en la nube de Microsoft. Con Azure AD, usted controla las cuentas de identidad, pero Microsoft garantiza que el servicio esté disponible globalmente. Proporciona:

- Autenticación
- Inicio de sesión único (SSO) (usar la misma cuenta para otros servicios)
- Administración de aplicaciones
- Administración de dispositivos

Azure AD ayuda a los usuarios a acceder a recursos tanto internos (red corporativa, intranet, apps en la nube) como externos (office 365, Azure Portal, etc).



Azure AD Connect sincroniza las identidades de usuario entre la instalación local de Active Directory y Azure AD.

Azure AD Multi-Factor Authentication - es un servicio de Microsoft que proporciona funcionalidades de autenticación multifactor. Azure Active Directory Premium (licencias P1 o P2) permite una configuración exhaustiva y detallada de Azure AD Multi-Factor Authentication a través de directivas de acceso condicional.

Acceso condicional: Estas señales incluyen quién es el usuario, dónde se encuentra y desde qué dispositivo solicita el acceso.

5.2 Estrategia de gobernanza en la nube Azure





Cloud Adoption Framework para Azure - guía consolidada para ayudar en el recorrido para la adopción de la nube.

1. Definir la estrategia (qué queremos obtener con la migración a la nube) - definir motivaciones, documentar los resultados empresariales, dar argumentos empresariales, elegir el proyecto adecuado.
2. Crear un plan (correspondencia entre los objetivos y acciones) - inventario de bienes digitales, alineación inicial de la organización, plan de preparación de aptitudes, plan de adopción de la nube.
3. Preparar la organización (un entorno en la nube donde empezar a hospedar nuestras cargas de trabajo) - instalación de Azure, zona de aterrizaje de Azure (suscripciones), expansión, procedimientos recomendado.
4. Adoptar la nube (migrar nuestras aplicaciones a la nube) - migrar la primer carga, escenarios de migración, procedimientos recomendados, mejoras del proceso, innovar.
5. Controlar y administrar los entornos de nube (estrategias de administración y gobernanza) - metodologías, banco de pruebas, base de gobernanza inicial, mejorar la base de gob.

Estrategia de gobernanza de suscripciones - se debe identificar una estructura de la organización en la nube que cubra las necesidades empresariales (equipo de habilitación de la nube).

- Facturación (requisitos internos) - una posible solución es organizar las suscripciones por departamento o por proyecto.
- Control de acceso (basado en roles) - entornos de desarrollo y producción con suscripciones independientes, es posible controlar el acceso a cada una de ellas por separado y aislar los recursos entre sí.
- Límites de suscripción - se tienen algunas limitaciones de recursos. Si alcanzamos un límite máximo estricto, no hay flexibilidad para aumentarlo.

Control de acceso basado en roles de Azure (RBAC de Azure) - un recurso o un conjunto de recursos en los que este acceso se permite

Ámbito	Rol					
	Lector	Específico del recurso	Personalizado	Colaborador	Propietario	
	 Grupo de administración	Observadores	Usuarios que administran recursos			Administradores
	 Suscripción					
	 Grupo de recursos					
 Recurso	Procesos automatizados					

Si se otorga acceso a un ámbito primario, esos permisos se heredan en todos los ámbitos secundarios. RBAC de Azure se puede aplicar a una persona individual o a un grupo.

Bloqueo de recursos - impiden que se eliminen o modifiquen recursos por error. Podemos aplicar bloqueos a una suscripción, a un grupo de recursos o a un recurso individual.

- CanNotDelete
- ReadOnly

Azure Blueprints nos permite definir el conjunto recursos estándar de Azure que la organización necesita (puede reemplazar automáticamente el bloqueo de recursos si dicho bloqueo se quita.).

Etiquetas para organizar los recursos de Azure - Las etiquetas proporcionan información extra, o metadatos, sobre los recursos. Azure Policy se puede usar también para aplicar reglas y convenciones de etiquetado. Así, podemos requerir que se agreguen determinadas etiquetas a los nuevos recursos a medida que se aprovisionan.

- Administración de recursos
- Optimización y administración de costes
- Administración de operaciones
- Seguridad
- Gobernanza y cumplimiento normativo
- Automatización y optimización de las cargas de trabajo

Azure Policy - es un servicio de Azure que permite crear, asignar y administrar directivas que controlan o auditan recursos. Aplican distintas reglas y efectos a las configuraciones de los recursos con el propósito de que estas configuraciones sigan cumpliendo con los estándares corporativos.

Azure Policy evalúa los recursos y resalta los que no cumplen las directivas que hemos creado. Azure Policy también puede impedir que se creen recursos no conformes. en categorías como Almacenamiento, Redes, Proceso, Centro de seguridad y Supervisión.

Azure Policy se integra con Azure DevOps aplicando directivas de integración continua y canalización de entrega que competen a las fases de implementación anterior y posterior de las aplicaciones. Todos los recursos secundarios dentro de ese ámbito heredarán las asignaciones de directivas. Si una directiva se aplica a un grupo de recursos, se aplicará también a todos los recursos dentro de ese grupo.

Pasos para implementar una directiva:

1. Crear una definición de directiva

2. Asignar la definición a los recursos
3. Revisar los resultados de evaluación

Una iniciativa de Azure Policy es una forma de agrupar las directivas relacionadas en un mismo conjunto.

Azure Blueprints (estándares organizativos)- En lugar de tener que configurar características como Azure Policy en cada nueva suscripción, con Azure Blueprints puede definir un conjunto repetible de herramientas de gobernanza y recursos de Azure estándar que la organización necesita.

- Asignaciones de roles
- Asignaciones de directivas (Azure Policy)
- Plantillas de Azure Resource Manager
- Grupos de recursos

Los planos técnicos también tienen versiones. El control de versiones nos permite llevar un control de los cambios que se producen en el plano técnico y comentarlos. Cada componente de la definición de un plano técnico se denomina *artefacto*.

5.3 Privacidad, cumplimiento y protección de datos

En general, cumplimiento significa cumplir una ley, un estándar o un conjunto de directrices. El cumplimiento normativo hace referencia a la disciplina y al proceso de garantizar que una empresa sigue las leyes que establecen los organismos competentes.

Piense en un control como un estándar conocido con el que puede comparar su solución para garantizar la seguridad.

Global	<input checked="" type="checkbox"/> ISO 27001:2013	<input checked="" type="checkbox"/> ISO 22301:2012	<input checked="" type="checkbox"/> SOC 1 Type 2	<input checked="" type="checkbox"/> CSA STAR Certification
	<input checked="" type="checkbox"/> ISO 27017:2015	<input checked="" type="checkbox"/> ISO 9001:2015	<input checked="" type="checkbox"/> SOC 2 Type 2	<input checked="" type="checkbox"/> CSA STAR Attestation
	<input checked="" type="checkbox"/> ISO 27018:2014	<input checked="" type="checkbox"/> ISO 20000-1:2011	<input checked="" type="checkbox"/> SOC 3	<input checked="" type="checkbox"/> CSA STAR Self-Assessment
				<input checked="" type="checkbox"/> WCAG 2.0 (ISO 40500:2012)
US Gov	<input checked="" type="checkbox"/> FedRAMP High	<input checked="" type="checkbox"/> DFARS	<input checked="" type="checkbox"/> DoE 10 CFR Part 810	<input checked="" type="checkbox"/> FIPS 140-2
	<input checked="" type="checkbox"/> FedRAMP Moderate	<input checked="" type="checkbox"/> DoD DISA SRG Level 5	<input checked="" type="checkbox"/> NIST SP 800-171	<input checked="" type="checkbox"/> ITAR
	<input checked="" type="checkbox"/> EAR	<input checked="" type="checkbox"/> DoD DISA SRG Level 4	<input checked="" type="checkbox"/> NIST CSF	<input checked="" type="checkbox"/> CJIS
		<input checked="" type="checkbox"/> DoD DISA SRG Level 2	<input checked="" type="checkbox"/> Section 508 VPATs	<input checked="" type="checkbox"/> IRS 1075
Industry	<input checked="" type="checkbox"/> PCI DSS Level 1	<input checked="" type="checkbox"/> FCA (UK)	<input checked="" type="checkbox"/> 21 CFR Part 11 (GxP)	<input checked="" type="checkbox"/> CDSA
	<input checked="" type="checkbox"/> GLBA	<input checked="" type="checkbox"/> MAS + ABS (Singapore)	<input checked="" type="checkbox"/> MARS-E	<input checked="" type="checkbox"/> MPAA
	<input checked="" type="checkbox"/> FFIEC	<input checked="" type="checkbox"/> 23 NYCRR 500	<input checked="" type="checkbox"/> NHS IG Toolkit (UK)	<input checked="" type="checkbox"/> DPP (UK)
	<input checked="" type="checkbox"/> Shared Assessments	<input checked="" type="checkbox"/> HIPAA BAA	<input checked="" type="checkbox"/> NEN 7510:2011 (Netherlands)	<input checked="" type="checkbox"/> FACT (UK)
Regional	<input checked="" type="checkbox"/> FISC (Japan)	<input checked="" type="checkbox"/> HITRUST	<input checked="" type="checkbox"/> FERPA	<input checked="" type="checkbox"/> SOX
	<input checked="" type="checkbox"/> APRA (Australia)			
	<input checked="" type="checkbox"/> Argentina PDPA	<input checked="" type="checkbox"/> China TRUCS / CCCPPF	<input checked="" type="checkbox"/> Germany IT-Grundschutz	<input checked="" type="checkbox"/> Singapore MTCS Level 3
	<input checked="" type="checkbox"/> Australia IRAP Unclassified	<input checked="" type="checkbox"/> EN 301 549	<input checked="" type="checkbox"/> India MeitY	<input checked="" type="checkbox"/> Spain ENS
	<input checked="" type="checkbox"/> Australia IRAP PROTECTED	<input checked="" type="checkbox"/> EU ENISA IAF	<input checked="" type="checkbox"/> Japan CS Mark Gold	<input checked="" type="checkbox"/> Spain DPA
	<input checked="" type="checkbox"/> Canada Privacy Laws	<input checked="" type="checkbox"/> EU Model Clauses	<input checked="" type="checkbox"/> Japan My Number Act	<input checked="" type="checkbox"/> UK Cyber Essentials Plus
	<input checked="" type="checkbox"/> China GB 18030:2005	<input checked="" type="checkbox"/> EU – US Privacy Shield	<input checked="" type="checkbox"/> Netherlands BIR 2012	<input checked="" type="checkbox"/> UK G-Cloud
	<input checked="" type="checkbox"/> China DJCP (MLPS) Level 3	<input checked="" type="checkbox"/> Germany CS	<input checked="" type="checkbox"/> New Zealand Gov CC	<input checked="" type="checkbox"/> UK PASF

información sobre la manera en que la declaración de privacidad de Microsoft, los Términos de los Servicios en Línea y el anexo de protección de datos explican qué datos personales recopila Microsoft

Declaración de privacidad de Microsoft - Abarca todos los servicios, sitios web, aplicaciones, software, servidores y dispositivos de Microsoft y explica qué datos personales recopila Microsoft, cómo los usa y con qué fines.

Términos de servicios en línea - son un contrato legal entre Microsoft y el cliente, detallan las obligaciones de ambas partes con respecto al procesamiento y la seguridad de los datos de los clientes y los datos personales.

Anexo de protección de datos - define también los términos de seguridad y procesamiento de datos para los servicios en línea.

- Cumplimiento de las leyes.
- Revelación de los datos procesados.
- Seguridad de los datos, lo cual incluye directivas y prácticas de seguridad, cifrado de datos, acceso a datos, responsabilidades del cliente y cumplimiento de la auditoría.
- Transferencia de datos, retención y eliminación.

Centro de confianza - presenta los principios de Microsoft para mantener la integridad de los datos en la nube y la manera en que Microsoft implementa y admite la seguridad, la privacidad, el cumplimiento y la transparencia en todos los servicios y productos de nube de Microsoft.

Documentación de cumplimiento de Azure - proporciona documentación detallada sobre el cumplimiento y los estándares legales y normativos en Azure.



Información general, planos técnicos, directrices para asegurarse que Azure cumple con estándares de pago, etc.

Azure Government - es una instancia independiente del servicio de Microsoft Azure. Aborda las necesidades de seguridad y cumplimiento de las agencias federales de EE. UU., los gobiernos locales y estatales.

Azure China 21Vianet - se trata de una instancia físicamente separada de servicios en la nube que se encuentra en China. Azure China 21Vianet es operado y administrado de forma independiente por Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet").

6. Acuerdos de nivel de servicio y la administración de costos de Azure

6.1 Planeación y administración de costo

Calculadora de TCO - calculadora de costo total de propiedad puede ayudar a comparar el costo de la ejecución en el centro de datos en lugar de en Azure.

1. Definir las cargas de trabajo - especificaciones de la infraestructura local (servidores, bases de datos, storage, redes)

2. Ajustar los supuestos - especifique el estatus de las licencias locales, la redundancia necesaria, costos de electricidad, mantenimiento, administración de TI, etc.
3. Consulte el informe - Elija un período de tiempo entre uno y cinco años. La calculadora de TCO genera un informe que se basa en la información especificada (proceso, centro de datos, redes, almacenamiento, trabajo de TI).

Comprar servicios de Azure - comprar servicios de Azure y se hará una idea de otros factores que afectan al costo.

- Tipos de suscripciones - evaluación gratuita, pago por uso, ofertas para miembros.
- Comprar servicios de Azure - contrato enterprise, directamente desde la web, a través de un Proveedor de soluciones en la nube.

Factores que afectan el costo - La forma en que usa sus recursos, el tipo de suscripción y los precios de los proveedores de terceros son factores comunes.

- Tipo de recurso - tipo, nivel de rendimiento, nivel de acceso, etc.
- Medidores de uso - tiempo de proceso, tráfico, operaciones, etc.
- Uso de recursos - cantidad de recursos utilizados y datos almacenados.
- Tipo de suscripción
- Azure Marketplace - servicios de terceros.

Distintas regiones pueden tener distintos precios asociados. Dado que las regiones geográficas pueden afectar al flujo del tráfico de red, el tráfico de red es también una influencia en el costo que se debe tener en cuenta.

Una zona es una agrupación geográfica de regiones de Azure para fines de facturación. El precio de la transferencia de datos se basa en las zonas.

Calculadora de precios varían entre productos, pero pueden incluir: región, nivel, opciones de facturación, opciones de soporte técnico, programas y ofertas, precios de desarrollo/ pruebas.

Azure Advisor - identifica los recursos no utilizados o infrautilizados, y recomienda recursos no utilizados que se pueden quitar.

Límites de gasto - Si tiene una suscripción basada en crédito y alcanza el límite de gasto configurado, Azure suspende su suscripción hasta que comience un nuevo período de facturación.

Reservas de Azure para pagar por adelantado - precios con descuento en determinados servicios de Azure.

Azure Cost Management + Billing - le ayuda a comprender su factura de Azure, administrar su cuenta y sus suscripciones, supervisar y controlar los gastos de Azure, y optimizar el uso de recursos.

Las etiquetas ayudan a administrar los costos asociados a los distintos grupos de productos y recursos de Azure. Puede aplicar etiquetas a grupos de recursos de Azure para organizar los datos de facturación.

6.2 Acuerdo de nivel de servicio y ciclo de vida

Acuerdos de nivel de servicio (SLA) - Un acuerdo de nivel de servicio es un contrato formal entre una empresa de servicios y el cliente. En Azure, este acuerdo define los estándares de rendimiento que Microsoft se compromete a proporcionar al cliente.

- El tiempo de inactividad es el período de tiempo que el servicio no está disponible.
- Un crédito de servicio es el porcentaje del precio que ha pagado que se le abonará conforme al proceso de aprobación de reclamaciones.
- Normalmente, los productos gratuitos no tienen un acuerdo de nivel de servicio.

Un acuerdo de nivel de servicio de la aplicación define los requisitos del acuerdo para una aplicación específica. Este término normalmente hace referencia a una aplicación que el cliente compila en Azure.

Para garantizar la alta disponibilidad, se puede planear que la aplicación tenga componentes duplicados en varias regiones, lo que se conoce como redundancia. Por

otro lado, para minimizar los costos durante períodos no críticos, se puede ejecutar la aplicación únicamente en una región.

Ciclo de vida de un servicio - El ciclo de vida de un servicio define la forma en que cada servicio de Azure se pone a disposición del público.