Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II

Grupo 101

25 de noviembre 2024

Cloud computing — Diseño de Arquitectura en la Nube

Autor:

Catherine Johanna Rojas Mendoza - A01798149

Adrian Pineda Sánchez - A00834710

Rodolfo Jesús Cruz Rebollar - A01368326

Rogelio Lizárraga Escobar - A01742161

Luis Maximiliano López Ramírez - A00833321

Profesor:

Félix Ricardo Botello Urrutia

Diseño de Arquitectura en la Nube

1. Diseño de Arquitectura en la Nube para Máquinas virtuales en DataTech

1.1. Descripción general de la arquitectura

La arquitectura se encuentra diseñada dentro de una plataforma de nube de dominio público como lo es AWS, Google Cloud, o Azure, debido a su alto grado de flexibilidad y amplio conjunto de servicios que ofrecen, por lo que los principales componentes que integran ésta arquitectura son los siguientes:

- **Máquinas virtuales:** para el almacenamiento de las aplicaciones de la empresa DataTech.

- **Grupos de disponibilidad:** Realizar una distribución de las Vms en distintas regiones de disponibilidad con el objetivo de que se tenga en general una alta disponibilidad.

- **Balanceador de carga:** Con el propósito principal de realizar una distribución eficiente del trafico entre las VMs y al mismo tiempo asegurar que ninguna de las VMs experimente una sobrecarga.

- **Grupos de escalado automatizado:** Realizar un ajuste de forma automática de la cantidad de VMs dependiendo de la demanda de la empresa en un momento dado.

- **Redes Virtuales (VNet o VPC):** para el aislamiento y control eifciente del tráfico de red.

- **Grupos de seguridad de red (NSG):** Para controlar el acceso y la seguridad a nivel de la red.

- **Almacenamiento de los datos:** bases de datos y discos persistentes para alojar aplicaciones de la empresa.

1.2. Diagrama de la arquitectura

El diagrama de la arquitectura para este escenario incluirá los siguientes elementos principales:

- Balanceador de carga frontal.

- Varias Vms distribuidas en múltiples regiones de disponibilidad (AZ1, AZ2, AZ3).

- Bases de datos distribuidas para garantizar un alto grado de disponibilidad.

- Redes de carácter virtual conformadas por subredes tanto de dominio público como privado.

- NSG y cortafuegos (firewalls) configurados con el objetivo de asegurar la seguridad de la red.

1.3. Componentes detallados

1.3.1. Máquinas virtuales

- **Elección del tipo de VM:**

  - Emplear máquinas virtuales de mediano tamaño (por ejemplo las VMs D-Series en Azure son apropiadas para aplicaciones con un nivel moderado de carga) con 4 vCPUs y 16 GB de memoria RAM.

  - **Tipos de discos:** discos premium de tipo SSD para asegurar un alto grado de rendimiento en tareas de escritura y lectura.

  - **Sistema operativo:** Ubuntu Server o Windows Server, de acuerdo a las apps que sean ejecutadas.

- **Grupos de disponibilidad:** las VMs son distribuidas en varias regiones de disponibilidad con el objetivo de asegurar la continuidad del servicio en caso de presentarse una falla de zona.

1.3.2. Escalabilidad y balanceo de carga

- **Grupo de escalado automatizado:**

  - Implementación de grupos de escalado automatizado para incrementar o decrementar el número de máquinas virtuales de acuerdo con el nivel de demanda (escalado automático tanto horizontal como vertical).

- **Balanceador de carga:**

- Un balanceador de carga en la región frontal de distribuirá el tráfico entrante entre las máquinas virtuales, balanceando de esa manera la carga y asegurando una alta disponibilidad.

- La configuración se realizará de forma que se rediriga el tráfico hacia máquinas virtuales en buen estado y en cambio, desconectar aquellas otras que no emitan respuesta.

1.3.3. Redes y configuración de seguridad

- **Redes Virtuales y Subredes:**

  - La infraestructura se encuentra organizada en subredes tanto públicas como privadas en el interior de una red virtual VNet o VPC. Las máquinas virtuales encargadas del manejo del tráfico público están localizadas en subredes públicas, mientras que las bases de datos y otros servicios internos se ubican en subredes privadas.

- **Seguridad de Red (NSG y Firewalls):**

  - Los Grupos de Seguridad de Red (NSG) se encargarán de controlar el acceso a las VMs, restringiendo el tráfico a través de normas estrictas basadas en IPs y puertos.

  - **Segmentación de la red:** será utilizada con el propósito de aislar distintas capas de la aplicación (frontend, backend, bases de datos).

- **Principio de Mínimos Privilegios (Least Privilege):**

  - Configurar roles y permisos en base al principio de mínimos privilegios, asegurando de esa manera que tanto los usuarios como servicios solamente tengan acceso a aquellos recursos que requieren para desempeñar sus funciones.

- **Zero Trust:**

  - Modelo de seguridad que se basa en la premisa de "nunca confiar y siempre verificar". Además se implementará autenticación de múltiples factores (MLA), además de comprobación recurrente de identidad y acceso para todas las conexiones tanto en el interior como en el exterior de la red.

1.3.4. Almacenamiento y bases de datos

- **Almacenamiento en discos:** discos SSD de alto rendimiento para el alojamiento de las máquinas virtuales (VMs).

- **Base de datos:** servicios administrados de bases de datos relacionales como Azure SQL Database o Amazon RDS, con réplicas en numerosas regiones de disponibilidad para asegurar la oportuna recuperación frente a desastres en la zona.

1.4. Seguridad

La arquitectura para el presente escenario sigue las mejores prácticas de seguridad, mismas que se mencionan a continuación:

- **Principio de Mínimos Privilegios:** se asignan permisos mínimos necesarios a los usuarios y servicios.

- **Esquema Zero Trust:** cada acceso es debidamente validado con autenticación multifactor (MLA) y encriptación de datos tanto en tránsito como en reposo.

- **NSG:** Utilización de grupos de seguridad de red con el objetivo de restringir el acceso a las subredes y máquinas virtuales.

- **Cifrado:** los datos son cifrados estando tanto en reposo como en tránsito, empleando técnicas de cifrado como TLS y SSL. Además, las bases de datos y los discos se encuentran encriptados mediante el uso de claves administradas.

- **Monitoreo y logs:** Se realiza la configuración de herramientas de supervisión/monitoreo y auditoría, tales como Azure Monitor o CloudWatch con el propósito de rastrear sucesos y realizar auditorías en materia de seguridad.

1.5. Estimación de Costos

A continuación se plantea una estimación de aproximada de los costos por mes para los recursos propuestos, tomando en cuenta una plataforma como Azure:

Recurso	Descripción	Costo mensual (USD)
Máquinas Virtuales (D4_v3)	4 VMs D4_v3 (4 vCPUs, 16 GB RAM)	$640.00 ($160.00/mes por VM)
Discos Premium SSD	4 Discos premium SSD	$120.00 ($30.00/mes por disco)
Balanceador de Carga	1 Azure Load Balancer	$20.00
Base de Datos	1 Azure SQL Database (S3)	$300.00
Tráfico de Red	Estimación de transferencia de datos	$50.00
Total Estimado Mensual		**$1,130.00**

Cuadro 1: Estimación de costos mensuales para la infraestructura en la nube.

Nota: los costos mostrados en la tabla anterior son aproximados y puedan variar de acuerdo al proveedor de nube que se seleccione y la zona de implementación.

2. Diseño de Arquitectura en la Nube para Bases de Datos en DataTech

El objetivo de esta parte del diseño es proporcionar a DataTech una solución híbrida de bases de datos en la nube, utilizando tanto servicios de bases de datos gestionados (PaaS) como infraestructuras personalizables (IaaS). La arquitectura propuesta considera requisitos de confiabilidad, escalabilidad, seguridad, y recuperación ante desastres, asegurando un rendimiento óptimo para las aplicaciones de la empresa.

2.1. Bases de Datos PaaS: Azure SQL Database

Azure SQL Database es un servicio de base de datos gestionado, altamente escalable, que ofrece funcionalidades como respaldo automatizado, alta disponibilidad, y capacidades integradas de seguridad.

- **Escalabilidad:** Escala automáticamente según la carga de trabajo, lo que permite manejar picos de demanda. SQL Database ofrece un rendimiento predecible con varios tipos de recursos, niveles de servicio y tamaños de proceso. Proporciona escalabilidad dinámica sin tiempo de inactividad, optimización inteligente integrada, escalabilidad y disponibilidad globales y opciones de seguridad avanzadas. Estas funcionalidades le permiten centrarse en el desarrollo rápido de aplicaciones y en reducir el plazo de acceso al mercado, y olvidarse de la administración de máquinas virtuales e infraestructuras. SQL Database se encuentra actualmente en 38 centros de datos de todo el mundo, por lo que la base de datos se puede ejecutar en el que se encuentre más cerca. [1]
- **Mantenimiento Reducido:** Microsoft se encarga de las actualizaciones, parches y copias de seguridad, liberando al equipo de TI de tareas operativas y permitiendo enfocarse en actividades estratégicas. [1]

- **Alto Desempeño:** Optimización integrada para cargas de trabajo relacionales. Azure SQL Database se basa en la versión estable más reciente del motor de base de datos de Microsoft SQL Server. Puede usar características avanzadas de procesamiento de consultas, como las tecnologías en memoria de alto rendimiento y el procesamiento de consultas inteligente. Azure SQL Database se basa en la versión estable más reciente del motor de base de datos de Microsoft SQL Server. Puede usar características avanzadas de procesamiento de consultas, como las tecnologías en memoria de alto rendimiento y el procesamiento de consultas inteligente. [1]

- **Funcionalidades Adicionales:** Análisis avanzado de datos mediante integración nativa con servicios como Azure Synapse. [2]

2.2. Bases de Datos IaaS: Máquinas Virtuales (VM) con Software de Base de Datos

Implementar bases de datos en máquinas virtuales (VM) bajo un modelo de Infraestructura como Servicio (IaaS) ofrece a DataTech un control y flexibilidad significativos en bases de datos relacionales y no relacionales (como PostgreSQL y MongoDB) en máquinas virtuales.

- **Control Total:** Ideal para aplicaciones que requieren configuraciones personalizadas o soporte para tecnologías no disponibles en PaaS. Al gestionar directamente el sistema operativo y el software de la base de datos, el equipo de TI puede realizar configuraciones específicas y optimizaciones adaptadas a las necesidades particulares de las aplicaciones. [3]

- **Flexibilidad:** La capacidad de instalar versiones específicas de sistemas de gestión de bases de datos (SGBD) y aplicar integraciones personalizadas permite a DataTech adaptar el entorno a requisitos únicos, facilitando la compatibilidad con aplicaciones heredadas o especializadas. [3]

- **Seguridad Extendida:** La administración directa de la VM permite implementar políticas de seguridad personalizadas, incluyendo controles de acceso detallados y cifrado de datos según los estándares internos de la empresa. [3]

2.2.1. Consideraciones:

- **Responsabilidad de mantenimiento:** El equipo de TI es responsable de las actualizaciones, parches y copias de seguridad, lo que puede aumentar la carga operativa y requerir una planificación cuidadosa para garantizar la continuidad del servicio.

- **Gestión de recursos:** Es esencial dimensionar adecuadamente la VM para evitar problemas de rendimiento, ya que una configuración insuficiente puede afectar negativamente la eficiencia de la base de datos.

- **Costos operativos:** Aunque las VMs ofrecen flexibilidad, los costos asociados al licenciamiento del software de base de datos y al mantenimiento de la infraestructura pueden ser superiores en comparación con soluciones PaaS.

2.3. Arquitectura

División de Responsabilidades

El diseño contempla una arquitectura híbrida que utiliza bases de datos PaaS y IaaS, asignando las cargas de trabajo según las características de las aplicaciones y sus necesidades específicas:

Azure SQL Database (PaaS):

- Aplicaciones modernas con requerimientos transaccionales estándar.
- Sistemas que no requieren configuraciones personalizadas de la base de datos.
- Cargas de trabajo que necesitan alta disponibilidad, respaldo automatizado y escalabilidad dinámica.
- Base de datos principal para sistemas de análisis y reportes en tiempo real.

Máquinas Virtuales con Bases de Datos Personalizadas (IaaS):

- Aplicaciones heredadas o sistemas con dependencias específicas que no pueden migrarse fácilmente a PaaS.
- Sistemas que necesitan configuraciones avanzadas, como cambios en los parámetros de rendimiento, *tuning* específico del motor de base de datos, o integración con tecnologías no soportadas en Azure SQL Database.
- Uso de bases de datos no relacionales o híbridas (como MongoDB o Elasticsearch).
- Casos en los que se requieren versiones específicas de bases de datos no disponibles en PaaS.

Componentes del Diseño

La arquitectura incluye los siguientes elementos principales:

A. Bases de Datos PaaS: Azure SQL Database

1. **Configuración:**
   - Crear bases de datos en un grupo elástico (*elastic pool*) para gestionar múltiples bases con cargas de trabajo variables.
   - Configurar niveles de servicio escalables: por ejemplo, *General Purpose* o *Business Critical* según las necesidades de IOPS y latencia.
2. **Seguridad:**
   - Habilitar conexión con Azure Active Directory (AAD) para autenticación centralizada.
   - Aplicar cifrado en reposo con Transparent Data Encryption (TDE) habilitado por defecto.

- Habilitar reglas de firewall en nivel de servidor para restringir accesos no autorizados.

3. **Respaldo y Recuperación:**
   - Retención de copias automáticas con políticas personalizadas (7 a 35 días).
   - Configurar *long-term retention* (LTR) si se requieren copias de seguridad a largo plazo.

B. Máquinas Virtuales con Bases de Datos Personalizadas (IaaS)

1. **Configuración:**
   - Máquinas virtuales en Azure, ejecutando bases de datos como:
     - **SQL Server** para sistemas relacionales heredados.
     - **PostgreSQL** para aplicaciones modernas con soporte a datos geoespaciales.
     - **MongoDB** para bases de datos no relacionales.
   - Las VM estarán configuradas en una subred dedicada dentro de una Virtual Network (VNet).
   - Configuración de discos de almacenamiento SSD Premium para optimizar la IOPS.

2. **Seguridad:**
   - Implementar reglas en *Network Security Groups* (NSG) para restringir el tráfico a la VM.
   - Aplicar Azure Disk Encryption para cifrar los discos de datos.
   - Usar claves gestionadas por el cliente en Azure Key Vault para mayor seguridad.
   - Deshabilitar accesos directos como RDP y SSH desde internet; habilitar el acceso solo a través de Azure Bastion.

3. **Respaldo y Recuperación:**
   - Automatizar respaldos incrementales diarios con Azure Backup.
   - Implementar *snapshots* de disco como parte del plan de recuperación ante desastres (DRP).

Red y Comunicaciones

1. **Virtual Network (VNet):**
   - Crear una VNet con subredes dedicadas:
     - Subred para Azure SQL Database.
     - Subred para máquinas virtuales con bases de datos.
   - Configurar *peering* entre subredes para permitir comunicación segura.

2. **Gateway y Firewall:**
    - Implementar Azure Firewall para filtrar tráfico hacia las bases de datos desde ubicaciones externas.
    - Configurar Application Gateway para gestionar el acceso de las aplicaciones a las bases de datos.
3. **Conexión Segura:**
    - Habilitar TLS 1.2 para cifrar conexiones entre las bases de datos y las aplicaciones.
    - Aplicar rutas definidas para limitar el acceso a las bases de datos únicamente desde direcciones IP específicas.

2.4. Diagrama de Arquitectura

Elementos Clave:

- **Bases de Datos PaaS (Azure SQL Database):**
    - Grupo elástico para múltiples bases.
    - Conexiones seguras mediante Azure Private Link.
- **Bases de Datos IaaS (Máquinas Virtuales):**
    - VM configuradas en subred dedicada dentro de la VNet.
    - Backups automatizados con Azure Backup.
- **Red y Seguridad:**
    - Azure Firewall para filtrar tráfico.
    - *Network Security Groups* en las subredes.
    - TLS habilitado en conexiones.

2.5. Beneficios de la Arquitectura

- **Escalabilidad:**
    - Azure SQL Database escala automáticamente según demanda.
    - Las máquinas virtuales pueden ajustarse con mayor capacidad (CPU, RAM, almacenamiento) según sea necesario.
- **Disponibilidad:**
    - Alta disponibilidad nativa en Azure SQL Database.
    - Máquinas virtuales integradas con zonas de disponibilidad.
- **Seguridad:**
    - Cifrado en reposo y en tránsito.
    - Autenticación centralizada con Azure AD.
    - Aplicación del principio de *least privilege* en accesos.

2.6. Consideraciones de Seguridad Detalladas

Principio de Least Privilege

El principio de *Least Privilege* implica otorgar a los usuarios y aplicaciones solo los permisos necesarios para realizar sus funciones, reduciendo el riesgo de accesos no autorizados y errores operativos.

1. Asignación de Roles en Azure SQL Database:

- **Roles Predefinidos:**
  - `db_datareader`: Permite consultar datos pero no modificar ni administrar la base de datos.
  - `db_datawriter`: Autoriza insertar y modificar datos, pero no eliminar ni alterar configuraciones.
  - `db_owner`: Utilizado solo para administradores con permisos de configuración completa.
- **Prácticas Recomendadas:**
  - Utilizar roles predefinidos siempre que sea posible en lugar de permisos personalizados.
  - Crear usuarios específicos para tareas automatizadas con permisos restringidos.

2. Implementación en IaaS:

- Configuración granular en bases de datos personalizadas (ej. SQL Server) mediante esquemas y roles internos.
- Supervisión del acceso a través de herramientas como *Azure Monitor* o registros de auditoría SQL.

Modelo Zero Trust

El modelo *Zero Trust* aplica el principio de "Nunca confiar, siempre verificar". Cada acceso requiere autenticación y es validado explícitamente.

1. Autenticación Multifactor (MFA):

- Habilitar MFA para todos los administradores y usuarios con acceso a las bases de datos.
- Configuración mediante Azure AD Conditional Access para requerir MFA basado en el tipo de usuario o ubicación.

2. Azure Active Directory (AAD):

- Centralización de identidades mediante AAD, eliminando dependencias de contraseñas estáticas.
- Integración con Azure SQL Database para autenticación mediante identidades de AAD.
- Habilitación de políticas avanzadas como .ªcceso adaptativo"para detectar comportamientos anómalos.

Segmentación de Redes y NSG

1. Azure Virtual Network (VNet):

- Implementar una **VNet** con subredes dedicadas para bases de datos, separando servicios internos y externos.
- Uso de **Azure Private Link** para evitar que el tráfico hacia bases de datos pase por internet pública.

2. Network Security Groups (NSG):

- Configurar reglas para:
  - Permitir únicamente conexiones desde direcciones IP autorizadas o rangos específicos.
  - Bloquear accesos de entrada y salida no esenciales.
  - Priorizar reglas basadas en la importancia del tráfico (ejemplo: puertos específicos para SQL Server, como el puerto 1433).

Encriptación

1. En Tránsito:

- **TLS 1.2:**
  - Asegurar todas las conexiones entre clientes y servidores mediante cifrado TLS.
  - Verificar que los clientes usen certificados válidos para autenticación mutua.

2. En Reposo:

- **Transparent Data Encryption (TDE):**
  - Azure SQL Database habilita TDE de forma predeterminada, cifrando datos y respaldos.
  - En IaaS, usar herramientas como SQL Server TDE o PostgreSQL con claves administradas en Azure Key Vault.
- **Claves de Cliente (BYOK):**
  - Configurar *Bring Your Own Key* (BYOK) para un control completo de las claves de cifrado, almacenándolas en Azure Key Vault.

Respaldo y Recuperación

1. Azure SQL Database:

- **Políticas Automatizadas:**
  - Configuración de respaldo automático con retención de 7 a 35 días.
  - Uso de copias de seguridad geo-redundantes para recuperación en otra región en caso de fallas mayores.
- **Long-Term Retention (LTR):**
  - Configuración de copias de seguridad para almacenamiento a largo plazo (hasta 10 años).

2. Máquinas Virtuales (IaaS):

- **Azure Backup:**
  - Configurar respaldos incrementales diarios.
  - Realizar copias de seguridad completas semanales y diferenciales para reducir tiempos de recuperación.
- **Snapshots:**
  - Implementar snapshots regulares de discos para puntos de restauración rápidos.

3. Pruebas de Recuperación:

- Realizar pruebas regulares para garantizar que los respaldos sean funcionales y que los procesos de recuperación cumplan con los objetivos de tiempo de recuperación (RTO).

2.7. Estimación de costo mensual de los recursos propuestos

Componente	Descripción	Costo Mensual (USD)
Azure SQL Database (PaaS)	Nivel de servicio Business Critical (4 vCores, 32 GB)	$1,500.00
Máquinas Virtuales (IaaS)	2 x Standard_D4s_v3 (4 vCPUs, 16 GB RAM)	$400.00
Almacenamiento Adicional	2 x Discos Premium SSD (512 GB c/u)	$153.60
Azure Firewall	Protección de red avanzada	$1,000.00
Azure Backup	Respaldo para 2 VMs	$20.00
Total Estimado Mensual		**$3,073.60**

Cuadro 2: Estimación de costos mensuales de los recursos propuestos.

3. Storage Account - Fileshare (Azure Storage Accounts)

3.1. Arquitectura de Almacenamiento

El sistema estará basado en **Azure Storage Account**, aprovechando **Azure File Share** para almacenar y compartir datos no estructurados. La arquitectura propuesta incluye los siguientes elementos:

- **Cuentas de almacenamiento escalables:**
  - Tipo: *General Purpose v2*.
  - Nivel de rendimiento: Escogeremos *Estándar* para datos accedidos infrecuentemente y *Premium* para datos críticos con alta demanda.
  - Redundancia: *Geo-Redundant Storage (GRS)* para datos críticos y *Local-Redundant Storage (LRS)* para datos menos sensibles.
- **Azure File Share:**
  - Habilitará la compartición de archivos mediante el protocolo *SMB*.
  - Configuración de cuotas para evitar sobrepasos y administrar costos.

3.2. Seguridad y Acceso

- **Cifrado:**
  - *Datos en reposo*: Activaremos el cifrado gestionado por Azure.
  - *Datos en tránsito*: Configuración de conexiones SMB cifradas y el uso de HTTPS.
- **Control de acceso:**
  - Autenticación mediante *Azure Active Directory (Azure AD)*.
  - Implementación de roles basados en identidad ($RBAC$) para restringir el acceso según necesidades.
- **Políticas de red:**
  - Configuración de *firewalls* de red y restricciones IP.
  - Uso de *Azure Private Endpoints* para evitar accesos externos no autorizados.

3.3. Escalabilidad y Disponibilidad

- Escalaremos la capacidad de almacenamiento automáticamente según la demanda.
- Configuraremos *Azure Monitor* para rastrear el uso de recursos y generar alertas para eventos críticos.
- Redundancia geográfica para garantizar disponibilidad en caso de fallas regionales.

3.4. Integración con Sistemas y Aplicaciones

- **Mapeo en sistemas locales:**
  - Los equipos podrán montar *Azure File Share* como una unidad de red utilizando el protocolo SMB.
- **Acceso desde aplicaciones:**
  - Configuración de claves de acceso o integración con *Azure AD* para que las aplicaciones se conecten al almacenamiento de forma segura.

3.5. Flujo de Implementación

1. **Fase 1: Configuración Inicial:**
   - Crear Storage Accounts con opciones de redundancia y rendimiento adecuadas.
   - Configurar Azure File Share con cuotas y permisos iniciales.
2. **Fase 2: Seguridad y Red:**
   - Habilitar cifrado y configurar *Azure AD* para autenticación.
   - Implementar *firewalls* y *endpoints* privados.
3. **Fase 3: Integración y Pruebas:**
   - Mapear unidades de red en sistemas locales.
   - Probar la integración con aplicaciones existentes y medir tiempos de respuesta.
4. **Fase 4: Monitoreo y Optimización:**
   - Configurar *Azure Monitor* para supervisión.
   - Realizar ajustes de rendimiento y costos.

Recurso	Descripción	Costo Mensual (USD)
Cuenta de Almacenamiento	Cuenta de almacenamiento de uso general v2 con redundancia geográfica (GRS) para alta disponibilidad.	$20.00
Azure File Share	Recurso compartido de archivos con 1 TiB de almacenamiento en nivel estándar.	$23.00
Azure Monitor	Servicio de monitoreo para supervisar el rendimiento y el uso de recursos.	$5.00
Azure Active Directory	Gestión de identidades y control de acceso basado en roles (RBAC).	Incluido en la suscripción
Endpoint Privado	Configuración de endpoints privados para asegurar el tráfico de red.	$6.00
Transferencia de Datos Salientes	100 GB de datos salientes hacia Internet.	$8.00
Transacciones de Almacenamiento	1 millón de operaciones de lectura/escritura.	$0.05
Total Estimado		**$62.05**

Cuadro 3: Recursos necesarios, descripción y costo mensual estimado en USD

4. Diseño de Redes Virtuales (VNets)

- **Creación de VNets:**
  - Se implementarán redes virtuales separadas para diferentes capas de la arquitectura:
    - VNet para la capa de aplicaciones (App Service y máquinas virtuales).
    - VNet para la capa de bases de datos (Azure SQL Database y máquinas virtuales con bases de datos).
    - VNet para la capa de almacenamiento (Azure Storage Account con File Share).
  - Cada VNet estará configurada con un rango de direcciones IP único y subredes específicas.
- **Asignación de Subredes:**
  - Dividir cada VNet en subredes dedicadas:
    - Subred para servicios internos.
    - Subred para comunicación con internet, si es necesario.
  - Aislamiento mediante reglas de seguridad aplicadas a cada subred.

4.1. Conectividad entre VNets

- **VNet Peering:**
  - Configurar *peering* entre VNets para permitir la comunicación directa sin pasar por internet pública.
  - Garantizar baja latencia y alta velocidad en la comunicación entre redes virtuales.
- **Configuración de Rutas:**
  - Implementar rutas definidas para dirigir el tráfico entre subredes y VNets.
  - Asegurar que el tráfico fluya únicamente a través de canales seguros.

4.2. Seguridad y Aislamiento

- **Network Security Groups (NSGs):**
  - Configurar reglas de entrada y salida para controlar el acceso al tráfico en cada subred.
  - Permitir únicamente conexiones desde rangos de IP autorizados.
- **Azure Firewall:**
  - Implementar un firewall para filtrar el tráfico entre VNets y hacia recursos externos.
  - Configurar políticas de acceso basadas en aplicaciones.
- **Azure Private Link:**
  - Usar *Private Link* para evitar que el tráfico hacia los servicios gestionados (como bases de datos y almacenamiento) pase por internet pública.

4.3. Enrutamiento y Administración de Conexiones

- **Gateway de Red Virtual:**
  - Configurar un gateway para facilitar la conectividad con redes externas o conexiones híbridas (por ejemplo, entre la nube y el centro de datos local de DataTech).
- **Supervisión y Logs:**
  - Habilitar *Azure Monitor* y *Network Watcher* para supervisar el tráfico y detectar anomalías.
  - Configurar logs en los NSGs y el firewall para realizar auditorías de acceso.

4.4. Estimación de Costos para Configuración entre VNets

La configuración entre VNets incluye los costos asociados a herramientas de conectividad y seguridad como VNet Peering, Azure Firewall y Network Security Groups (NSGs). A continuación, se presenta un desglose detallado:

Componente	Descripción	Costo Mensual (USD)
VNet Peering	Conexión entre redes virtuales para comunicación segura	$30.00
Azure Firewall	Protección de tráfico entre redes y hacia recursos externos	$1,000.00
Network Security Groups	Reglas para controlar tráfico en subredes (10 NSGs)	$20.00
Monitorización de Redes	Uso de Azure Monitor y Network Watcher	$50.00
Total Estimado Mensual		**$1,100.00**

Cuadro 4: Estimación de costos mensuales para la configuración entre VNets.

4.5. Consideraciones Adicionales

- Los costos de VNet Peering pueden aumentar si se añaden más redes virtuales o si el tráfico entre redes es alto.
- La monitorización puede optimizarse configurando alertas específicas para reducir el volumen de datos analizados.
- Los NSGs no tienen costos adicionales directos por uso, pero pueden requerir supervisión y mantenimiento para ajustar reglas según cambios en la arquitectura.

5. App Service

Propuesta de diseño para la implementación del entorno de **App Service** en la nube para la empresa **DataTech**, con el objetivo de garantizar la escalabilidad, alta disponibilidad y seguridad de las aplicaciones web. Esta propuesta se fundamenta en los principios de diseño arquitectónico en la nube establecidos y considera un enfoque práctico utilizando **Microsoft Azure** como plataforma. Además, se incluye una estimación de costos basada en los servicios seleccionados.

5.1. Requerimientos del Diseño

Los requisitos de DataTech para el entorno de App Service son los siguientes:

1. Implementación de aplicaciones web escalables.
2. Configuración de dominios personalizados para aplicaciones corporativas.

3. Uso de certificados SSL para garantizar la seguridad en las conexiones.
4. Escalabilidad automática según la demanda.
5. Integración segura con bases de datos como *Azure SQL Database*.
6. Monitoreo y diagnóstico para garantizar un rendimiento óptimo.

5.1.1. Propuesta de Diseño

Selección del Plan de App Service

- **Plan sugerido:** Azure App Service *Premium v3*.
  - Soporta instancias dedicadas con mejor rendimiento y alta disponibilidad.
  - Escalabilidad hasta 30 instancias, permitiendo manejar cargas de tráfico altas.
  - Incluye soporte para conexiones privadas y certificados SSL.

Configuración de Escalabilidad Automática

- Configuración de reglas de autoescalado basadas en las siguientes métricas:
  - **CPU:** Escalar al 80 % de uso.
  - **Memoria:** Escalar al 70 % de uso.
  - **Solicitudes por segundo:** Escalar cuando superen 1000 solicitudes simultáneas.
- Se establecerá un rango de 2 a 10 instancias como umbral mínimo y máximo para garantizar un equilibrio entre costo y rendimiento.

Seguridad y Certificados SSL

- Implementación de **TLS 1.2** en todas las conexiones.
- Configuración de certificados SSL gratuitos proporcionados por Azure. Para aplicaciones críticas, se integrarán certificados *premium* de terceros como DigiCert o GlobalSign.

Integración con Dominios Personalizados

- Configuración de dominios corporativos usando el *DNS de Azure*.
- Configuración de reglas de *firewall* para restringir el tráfico desde direcciones IP no autorizadas.

Monitoreo y Diagnóstico

- Uso de **Azure Monitor** y **Application Insights** para:
  - Supervisar la latencia, tiempo de respuesta y errores.
  - Detectar problemas de disponibilidad en tiempo real.
  - Configurar alertas personalizadas para métricas clave.

Integración con Bases de Datos

- Integración directa con *Azure SQL Database* utilizando:
  - **Azure Private Link** para garantizar que el tráfico no pase por la internet pública.
  - Configuración de cadenas de conexión seguras en el App Service mediante variables de entorno.

5.1.2. Presupuesto Estimado

A continuación, se presenta una estimación de costos mensuales considerando la configuración propuesta:

Componente	**Descripción**	**Costo Mensual (USD)**
App Service Plan (P3v3)	2 instancias básicas escalables a 10 instancias	450.00
Certificados SSL	Certificados estándar incluidos	0.00
Dominios personalizados	Gestión de 2 dominios	12.00
Application Insights	Supervisión y logs	50.00
Azure SQL Database	Plan Business Critical (4 vCores, 32 GB)	1,500.00
Azure Private Link	Conexión privada a base de datos	50.00
Transferencia de datos	Uso estimado de transferencia	100.00
Total Estimado Mensual		**2,162.00**

Cuadro 5: Estimación de costos mensuales para el entorno de App Service.

[9] [10] [11] [12] [13] [14]

5.1.3. Beneficios de la Propuesta

1. **Escalabilidad Dinámica:** La configuración de autoescalado asegura que los recursos se ajusten según la demanda, optimizando costos y rendimiento.
2. **Alta Disponibilidad:** El uso de instancias premium y conexiones privadas garantiza un tiempo de actividad del 99.95 %.
3. **Seguridad Mejorada:** Los certificados SSL, la integración con Azure AD y el cifrado TLS protegen tanto los datos como las conexiones.
4. **Eficiencia Operativa:** La supervisión en tiempo real permite identificar problemas antes de que afecten a los usuarios finales.

5.1.4. Conclusión

El diseño propuesto cumple con los requerimientos establecidos para DataTech, proporcionando una arquitectura robusta, segura y escalable para su entorno web. Los costos estimados reflejan una inversión óptima para garantizar un servicio de calidad acorde con

las necesidades de la empresa. Este diseño puede ser ajustado según las necesidades específicas y el presupuesto final disponible.

6. Presupuesto Total

La siguiente tabla muestra un desglose detallado del presupuesto mensual necesario para implementar la solución completa en la nube para DataTech. Esta solución incluye la configuración de máquinas virtuales para alojar las aplicaciones, bases de datos confiables y escalables bajo esquemas de IaaS y PaaS, el Storage Account - Fileshare con Azure Monitor y Azure Active Directory, optimizando almacenamiento, supervisión y gestión de identidades con un enfoque en seguridad y rendimiento, la configuración segura entre redes virtuales (VNets) para el aislamiento del tráfico, y el uso de servicios de App Service para soportar las aplicaciones web con alta disponibilidad y seguridad. El presupuesto considera costos estimados para infraestructura, seguridad, almacenamiento y monitoreo.

Etapa	Componente y Descripción	Costo Mensual (USD)
Máquinas Virtuales	4 VMs D4.v3 (4 vCPUs, 16 GB RAM)	640.00
	4 Discos Premium SSD (30 USD por disco)	120.00
	1 Azure Load Balancer	20.00
	Estimación de transferencia de datos	50.00
Bases de Datos (IaaS y PaaS)	Azure SQL Database (Nivel Business Critical, 4 vCores, 32 GB)	1,500.00
	2 x Standard D4s v3 (4 vCPUs, 16 GB RAM)	400.00
	1 Azure SQL Database (S3)	300.00
	2 Discos Premium SSD (512 GB c/u)	153.60
	Azure Backup (respaldo para 2 VMs)	20.00
Storage Account - Fileshare	Cuenta Almacenamiento (Uso general v2)	20.00
	Azure File Share (1 TiB de almacenamiento)	23.00
	Azure Monitor (Monitreo de supervisiones del uso)	5.00
	Transferencias salientes (100 GB datos salientes)	8.00
	Endpoint Privado (Endpoint para tráfico de red)	6.00
Configuración entre VNets	VNet Peering (comunicación segura entre redes virtuales)	30.00
	Azure Firewall (protección de tráfico)	1,000.00
	Network Security Groups (10 NSGs para tráfico en subredes)	20.00
	Monitorización de Redes (Azure Monitor y Network Watcher)	50.00
App Service	App Service Plan (P3v3, 2 instancias escalables)	450.00
	Certificados SSL (estándar incluidos)	0.00
	Gestión de 2 dominios personalizados	12.00
	Application Insights (supervisión y logs)	50.00
	Transferencia de datos (uso estimado)	100.00
Total General		**4,787.60**

Cuadro 6: Presupuesto consolidado por etapas de implementación en la nube con componentes adicionales incluidos.

Este presupuesto refleja los costos necesarios para mantener una solución escalable, segura y con alta disponibilidad, cumpliendo los requerimientos técnicos y operativos de DataTech. Se recomienda revisar periódicamente los costos con el proveedor de servicios en la nube para asegurar que sigan siendo competitivos y adecuados a las necesidades de la empresa.

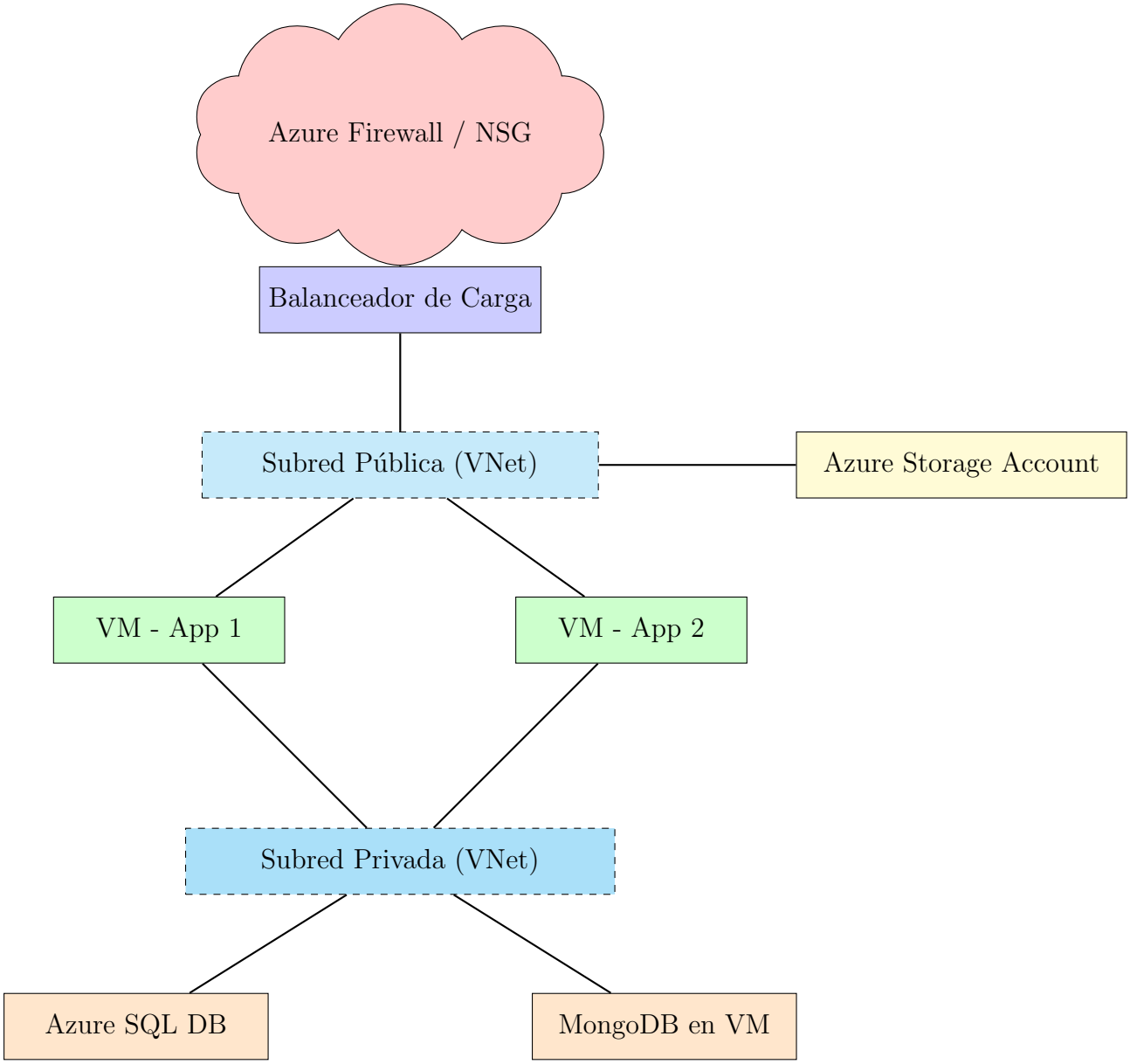

Figura 1: Diagrama detallado de la arquitectura propuesta.

7. Conclusiones individuales

Catherine

La arquitectura en la nube propuesta para DataTech aprovecha plataformas públicas como Azure, utilizando componentes como máquinas virtuales, balanceadores de carga, y redes virtuales configuradas para alta disponibilidad y escalabilidad. Estas características aseguran una operación continua incluso frente a fallas en zonas específicas, optimizando el rendimiento según la demanda y garantizando la eficiencia en la distribución de recursos.

Adrián

El almacenamiento propuesto mediante Azure Storage Accounts y Azure File Share ofrece una solución eficiente para gestionar datos no estructurados, con capacidades como redundancia geográfica y cifrado nativo. Su integración con sistemas locales a través del protocolo SMB garantiza compatibilidad, mientras que las políticas de acceso controladas aseguran que solo usuarios autorizados puedan manipular los recursos.

Rodolfo

En la presente actividad se realizaron diseños correspondientes a diferentes escenarios posibles en los que se puede implementar una arquitectura en la nube, para lo cual, fue necesario tomar en cuenta recursos como máquinas virtuales, cortafuegos (firewalls), entre otros elementos que garantizan el que una empresa cumpla con los estrictos estándares de seguridad establecidos a escala internacional, además de que la actividad realizada también nos resultó útil para tomar conciencia de todos los costos que implica el migrar los servicios de una empresa a la nube, motivo por el cual, resultó sumamente relevante el analizar detalladamente cada escenario planteado para determinar cuál es el modelo adecuado para la infraestructura en la nube que mejor se adapte a cada caso.

Además, también es importante mencionar que para determinar el modelo de infraestructura que mejor satisfaga las necesidades en cada escenario, fue necesario considerar un adecuado equilibrio entre los costos de implementación de los componentes de las arquitecturas y el rendimiento de los mismos, ésto con el objetivo de que para cada caso, se eligiera aquel tipo de infraestructura cuyos componentes fueran de preferencia de bajo costo, pero que a su vez tuvieran un alto rendimiento para soportar adecuadamente todo el flujo de datos entrantes y salientes de la empresa y procesarlos de forma eficiente.

Rogelio

La actividad nos permitió realizar un diseño de arquitectura en la nube, enfocándonos en garantizar seguridad, escalabilidad y eficiencia en la conectividad. Por ello, configuraciones como *VNet Peering*, *NSGs* y Azure Firewall fueron esenciales para segmentar y proteger los flujos de datos, asegurando un cumplimiento estricto de los principios de seguridad.

De igual manera, fue necesario encontrar un buen balance entre costo y rendimiento, donde se busca optimizar recursos sin comprometer la funcionalidad. Visualizar la interacción entre componentes a través del diagrama permitió validar el diseño y entender su lógica.

Luis

La implementación de prácticas de seguridad avanzadas, como el principio de mínimos privilegios y el modelo Zero Trust, junto con tecnologías de cifrado en reposo y en tránsito, fortalece la protección de datos sensibles. Además, herramientas como Azure Monitor permiten supervisar eventos críticos, detectar anomalías y mantener un alto estándar de cumplimiento en la gestión de la infraestructura.

Referencias

[1] Microsoft (n.d.). Azure SQL Database: A fully managed SQL database service. https://learn.microsoft.com/es-es/azure/azure-sql/database/sql-database-paas-overview?view=azuresql.

[2] Microsoft (n.d.). Azure SQL: Cloud database service. https://azure.microsoft.com/es-es/products/azure-sql/.

[3] Ontrack (n.d.). Las ventajas y desventajas de la virtualización de SQL y otras bases de datos: Parte 1. https://www.ontrack.com/es-es/blog/las-ventajas-y-desventajas-de-la-virtualizacion-de-sql-y-otras-bases-de-datos-par

[4] Microsoft (n.d.). Elastic pool overview: Optimize costs for multiple databases. https://learn.microsoft.com/es-es/azure/azure-sql/database/elastic-pool-overview?view=azuresql.

[5] Microsoft (n.d.). Virtual network peering: Overview. https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview.

[6] Microsoft (n.d.). Azure Firewall: Overview. https://learn.microsoft.com/en-us/azure/firewall/overview.

[7] Microsoft (n.d.). Network security groups: Overview. https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview.

[8] Microsoft (n.d.). Network monitoring with Azure Monitor. https://learn.microsoft.com/en-us/azure/network-watcher/monitoring-overview.

[9] Microsoft (n.d.). App Service Pricing. https://azure.microsoft.com/en-us/pricing/details/app-service/.

[10] Microsoft (n.d.). App Service Certificates. https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-certificate.

[11] Microsoft (n.d.). Domain Services Pricing. https://azure.microsoft.com/en-us/pricing/details/app-service/.

[12] Microsoft (n.d.). Azure Monitor Pricing. https://azure.microsoft.com/en-us/pricing/details/monitor/.

[13] Microsoft (n.d.). Azure SQL Database Pricing. https://azure.microsoft.com/en-us/pricing/details/sql-database/.

[14] Microsoft (n.d.). Azure Private Link. https://learn.microsoft.com/en-us/azure/private-link/private-link-overview.