



Tecnológico de Monterrey

Inteligencia artificial avanzada para la ciencia de datos II (Gpo 101)

Profesor: Félix Ricardo Botello Urrutia

Diseño de Arquitectura en la Nube

Sofía Cantú Talamantes	A01571120
Ozner Leyva	A01742377
Nallely Serna	A00833111
Fernanda Perez	A01742102

Noviembre 2024

Informe

1. Introducción

Objetivo

Este informe describe la arquitectura en la nube diseñada para DataTech, con el fin de migrar sus aplicaciones y servicios a una infraestructura en la nube, mejorando la escalabilidad, disponibilidad y seguridad.

Proveedor de servicios en la nube

Azure.

Principales componentes

Máquinas virtuales, bases de datos IaaS/PaaS, almacenamiento, redes virtuales y servicios de aplicaciones.

2. Diagrama de Arquitectura

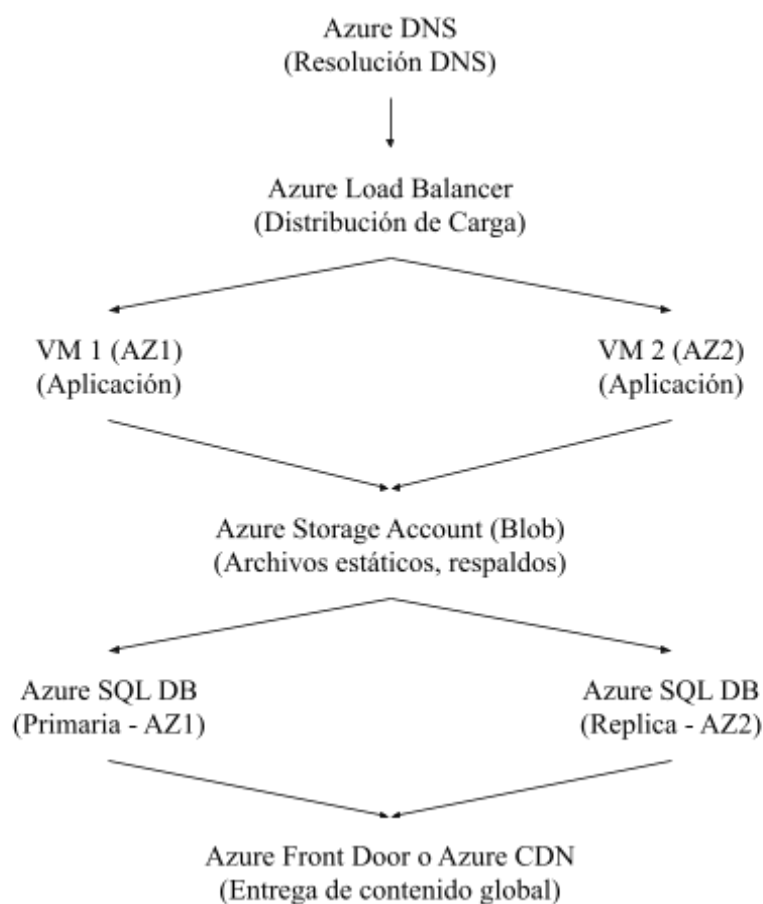


Figura 1. Diagrama de la arquitectura propuesta para el escenario.

Azure DNS

Se encarga de la resolución de nombres de dominio, dirigiendo el tráfico entrante hacia la infraestructura en la nube.

Azure Load Balancer

Distribuye la carga entre las máquinas virtuales (VMs) para garantizar alta disponibilidad y un rendimiento óptimo.

Máquinas Virtuales (VMs) en diferentes Zonas de Disponibilidad (AZ1 y AZ2)

Alojan las aplicaciones principales de DataTech. Al estar en diferentes zonas, se garantiza redundancia y resistencia a fallos.

Azure Storage Account (Blob)

Proporciona almacenamiento para archivos estáticos y copias de seguridad. Facilita la escalabilidad y el acceso seguro a datos no estructurados.

Azure SQL Database (Primaria y Réplica en distintas zonas)

- **Base de datos principal (AZ1):** Maneja las operaciones de lectura/escritura.
- **Réplicas en AZ2:** Proporciona redundancia y puede utilizarse para operaciones de solo lectura o recuperación ante desastres.

Azure Front Door o Azure CDN

Optimiza la entrega de contenido estático y dinámico a nivel global, mejorando la latencia y proporcionando mayor seguridad.

3. Descripción de Componentes y Decisiones de Diseño

3.1. Máquinas Virtuales (VMs)

Decisión

Se utilizarán dos VMs en diferentes Zonas de Disponibilidad (AZ1 y AZ2) para garantizar alta disponibilidad.

Tipo de VM

- General Purpose (D2s_v3): Para aplicaciones estándar.
- Escalabilidad: Implementación de un Auto Scaling Group para ajustar automáticamente el número de VMs según la demanda.

Alta disponibilidad

- Configuración con Azure Load Balancer para distribuir la carga de manera uniforme.

Justificación

Mejora el rendimiento y evita un solo punto de falla.

3.2. Bases de Datos (IaaS y PaaS)

Azure SQL Database (PaaS)

- Primaria: Ubicada en AZ1.
- Réplica: En AZ2, para garantizar redundancia y recuperación ante desastres.
- Seguridad: Implementación de Transparent Data Encryption (TDE) y acceso restringido con Azure Private Link.

Justificación

Proporciona alta disponibilidad, mantenimiento automático, y reducción de costos operativos en comparación con IaaS

3.3. Azure Storage Account (Blob)

Uso

Almacenamiento de archivos estáticos, backups y datos no estructurados.

Tipo

Blob Storage.

Seguridad:

- Habilitación de cifrado en reposo y en tránsito.
- Implementación de Azure Private Endpoints.

Justificación

Alta escalabilidad y capacidad de recuperación ante desastres.

3.4. Redes Virtuales (VNets)

Configuración

- Dos VNets, una para aplicaciones y otra para bases de datos.
- Subredes: División lógica para aislar recursos.
- Conectividad: VNet Peering para permitir la comunicación segura entre VNets.

Seguridad

- Network Security Groups (NSGs): Controlan el tráfico entrante/saliente.
- Firewall: Implementación de un firewall perimetral.

Justificación

Proporciona aislamiento de recursos, facilita la segmentación y garantiza la seguridad del tráfico.

3.5. Azure App Service

Plan

Standard (S1) o Premium (P1v2), según la carga esperada.

Configuraciones adicionales

- Auto Scaling: Configurado según la demanda.
- Certificados SSL: Implementados para seguridad en las comunicaciones.
- Despliegues Blue-Green: Reducción del downtime en actualizaciones.

Justificación

Permite el despliegue rápido de aplicaciones web con escalabilidad y alta disponibilidad.

4. Sugerencias de Seguridad

Principio de mínimo privilegio (Least Privilege)

Asignar permisos específicos a cada recurso, limitando el acceso a los roles esenciales.

Modelo Zero Trust

Verificar continuamente la identidad y permisos de usuarios y dispositivos.

Segmentación de redes

Utilizar subredes y NSGs para aislar recursos críticos.

Encriptación

- 1. Datos en reposo: Habilitar en Azure Storage y SQL Database.
- 2. Datos en tránsito: Usar TLS/SSL.

Monitoreo y auditoría

Implementar Azure Monitor y Azure Security Center para supervisar la infraestructura en tiempo real.

5. Estimación de Costos Mensuales

Recurso	Cantidad	Costo Mensual Estimado (USD)
Azure VM (D2s_v3)	2	\$180
Azure Load Balancer	1	\$20
Azure SQL Database (Standard)	1 (Primary)	\$300
Azure SQL Replica	1	\$200
Azure Storage (Blob)	1 TB	\$50
Azure App Service (S1)	1	\$75
Total Aproximado		\$825

Tabla 1. Estimación basada en los recursos propuestos.

6. Conclusiones

Nallely

La arquitectura propuesta ofrece a DataTech una infraestructura en la nube que garantiza escalabilidad, alta disponibilidad y seguridad. Diseñada bajo las mejores prácticas de Azure, esta solución se enfoca en fortalecer la seguridad y asegurar la continuidad del negocio. Entre los beneficios clave se destaca la capacidad de escalabilidad automática para gestionar cargas variables, la alta disponibilidad lograda mediante redundancia en múltiples zonas, y una seguridad robusta, respaldada por cifrado, controles de acceso estrictos y monitoreo continuo de la infraestructura.

Sofia

La implementación de esta arquitectura en la nube no solo permitirá a DataTech optimizar sus operaciones y reducir el riesgo de interrupciones, sino que también ofrecerá un marco flexible para el crecimiento futuro. La integración de componentes avanzados como Azure Load Balancer y Azure Front Door asegura un rendimiento eficiente, mientras que las estrategias de recuperación ante desastres y el diseño de alta disponibilidad garantizan la resiliencia frente a fallos. Además, la inversión en medidas de seguridad, como el modelo Zero Trust y el cifrado de datos, protege los activos de la empresa y refuerza la confianza en sus procesos digitales. En conjunto, este diseño posiciona a DataTech como una organización preparada para enfrentar los desafíos tecnológicos actuales y futuros.

Ozner

La propuesta de arquitectura en la nube para DataTech consolida una solución integral que equilibra rendimiento, seguridad y flexibilidad operativa. Al utilizar servicios gestionados como Azure SQL Database y Azure Storage, se logra minimizar el mantenimiento manual y garantizar la continuidad del negocio. La segmentación de redes y el enfoque en medidas de seguridad como la encriptación y el principio de mínimo privilegio fortalecen la protección de datos, mientras que la escalabilidad dinámica permite adaptarse a cambios en la demanda sin comprometer el rendimiento. Este diseño no solo responde a las necesidades actuales de DataTech, sino que también establece las bases para su transformación digital continua.

Fernanda

En el diseño arquitectónico en Azure vemos una estrategia proactiva y completa que prioriza la resiliencia y la adaptabilidad de los servicios de DataTech. La redundancia entre zonas de disponibilidad, combinada con la capacidad de recuperación ante desastres, logra garantizar operaciones ininterrumpidas incluso en escenarios críticos. Además, la incorporación de servicios como Azure Front Door optimiza la experiencia del usuario ya que hace una entrega ágil y segura de contenidos. Este enfoque demuestra cómo una infraestructura moderna en la nube puede impulsar la competitividad de DataTech, habilitando un entorno tecnológico confiable y preparado para soportar el crecimiento y la innovación a largo plazo.