



# Tecnológico de Monterrey

*Instituto Tecnológico y de Estudios Superiores de Monterrey*

## Cloud Computing. Diseño de Arquitectura en la Nube

### **TC3007C.501 Inteligencia Artificial Avanzada para la Ciencia de Datos II**

Profesores:

*Iván Mauricio Amaya Contreras*

*Blanca Rosa Ruiz Hernández*

*Félix Ricardo Botello Urrutia*

*Edgar Covantes Osuna*

*Felipe Castillo Rendón*

*Hugo Terashima Marín*

### Equipo 2

Integrantes:

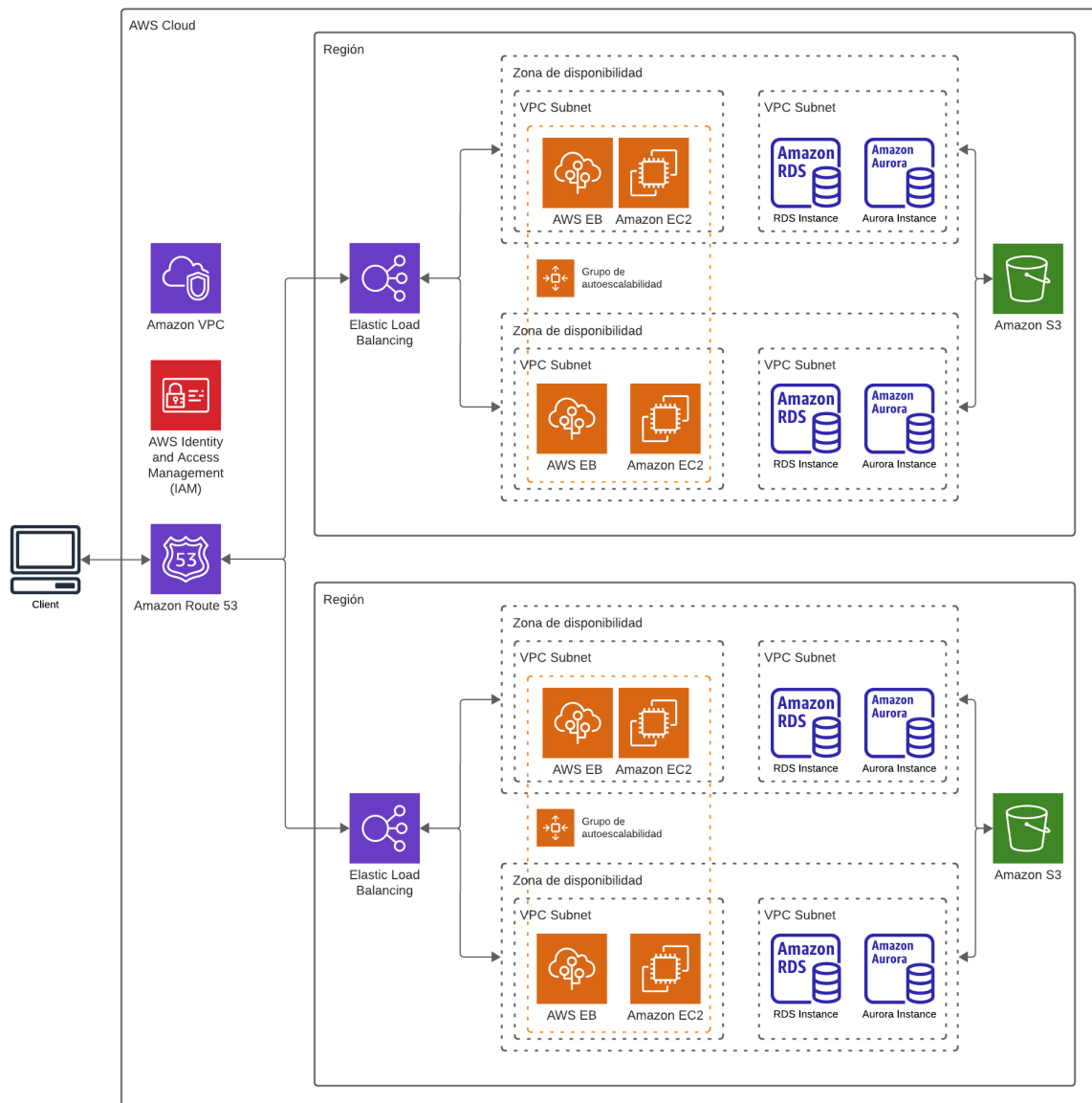
*Luis Ángel Guzmán Iribe – A01741757*

*Julian Lawrence Gil Soares – A00832272*

*Alberto H Orozco Ramos – A00831719*

20 de Noviembre de 2023

## Diagrama de arquitectura



- **Máquinas virtuales:**

- *DataTech necesita alojar sus aplicaciones en máquinas virtuales en la nube. Debes diseñar una infraestructura de máquinas virtuales que cumpla con los requisitos de rendimiento, escalabilidad y alta disponibilidad de la empresa. Considera aspectos como la selección del tamaño y tipo de las máquinas virtuales, la distribución de carga, la implementación de grupos de disponibilidad y el equilibrio de carga para garantizar la continuidad del negocio y la eficiencia operativa.*

Servicio recomendado: **AWS EC2 / Auto Scaling / Identity and Access Manager**

1. **Auto Scaling Groups (ASG):** Configura ASG para ajustar automáticamente el número de instancias de EC2 según la carga. Define políticas de escala basadas en métricas como la CPU o la utilización de red.

2. *Zonas de Disponibilidad (AZ)*: Distribuye instancias en diferentes AZ para garantizar alta disponibilidad. Si una AZ falla, las instancias en otras AZ seguirán operativas.
3. *Tipos de instancias*: Selecciona tipos de instancias apropiadas según los requisitos de rendimiento de las aplicaciones. Puedes usar instancias de propósito general, optimizadas para la memoria, o con su capacidad de cómputo optimizada, según lo necesario.
4. *Configuración de privilegios de usuario*: Se utiliza el Identity Access Manager (IAM) para generar perfiles con diferentes niveles de acceso a los sistemas existentes dentro de la arquitectura del sistema, ya sea lectura a la base de datos, acceso a instancias de cómputo, acceso a redes privadas, etc..

**Costos mensuales:**

Instancia EC2: \$150

- **Bases de datos IaaS y PaaS:**

- *DataTech requiere bases de datos confiables y escalables para almacenar y gestionar sus datos. Debes diseñar una combinación de bases de datos IaaS y PaaS que se ajuste a las necesidades de la empresa. Considera opciones como Azure SQL Database para bases de datos PaaS y máquinas virtuales con software de base de datos instalado para bases de datos IaaS. Asegúrate de tener en cuenta aspectos de rendimiento, seguridad, escalabilidad y opciones de respaldo y recuperación.*

Servicio recomendado: **AWS RDS / AWS Aurora**

1. *Replicación Multi-Zona*: Configura la replicación en diferentes zonas de disponibilidad para garantizar la disponibilidad continua y la recuperación ante desastres.
2. *Políticas de Respaldo y Recuperación*: Establece políticas de respaldo automáticas y frecuentes para proteger los datos. Práctica la restauración de backups para garantizar la eficacia del proceso de recuperación.
3. *Grupos de Parámetros*: Ajusta los parámetros de configuración según las necesidades específicas de las aplicaciones de DataTech para optimizar el rendimiento.

**Costos mensuales:**

Servidor AWS: \$1,497.08

- **Storage Account - Fileshare:**

- *DataTech necesita un almacenamiento en la nube seguro y escalable para sus archivos y datos no estructurados. Debes diseñar y configurar una o varias cuentas de almacenamiento que cumplan con los requisitos de capacidad y rendimiento de la empresa. Considera el uso de Azure Storage*

*Accounts con opciones como File Share para compartir archivos entre aplicaciones y equipos.*

1. *Bucket de S3:* Configura buckets para organizar y almacenar datos. Establece políticas de acceso para controlar quién puede acceder y modificar los datos.
2. *Transferencia de Datos Acelerada:* Mejora la velocidad de transferencia de datos utilizando la transferencia de datos acelerada de S3, especialmente útil para garantizar la seguridad de los datos almacenados en S3
3. *Encriptación:* Utiliza opciones de encriptación para garantizar la seguridad de los datos almacenados en S3.

Servicio recomendado: **AWS S3**

#### **Costos mensuales:**

Amazon S3:

- Primeros 50 TB/mes - 0.023 USD por GB
- Sigüientes 450 TB/mes - 0.022 USD por GB
- Más de 500 TB/mes - 0,021 USD por GB

Dichos precios corresponden a la versión estándar de S3, los precios pueden variar dependiendo del tipo de almacenamiento que se desee implementar. En este [enlace](#) es posible encontrar más información acerca de este servicio.

#### ● **Configuración entre VNets:**

- *DataTech requiere una arquitectura en la nube con redes virtuales (VNets) bien definidas y una configuración segura entre ellas. Debes diseñar y configurar las VNets, asignar subredes adecuadas y establecer reglas de conectividad para permitir la comunicación entre las diferentes partes de la arquitectura. Asegúrate de considerar aspectos de seguridad, aislamiento de recursos y enrutamiento adecuado.*

Servicio recomendado: **AWS VPC**

1. *División de sistema:* Dividir la arquitectura en VPCs para aislar diferentes partes del sistema.
2. *Medidas de seguridad:* Establecer subredes públicas y privadas según sea necesario para tener un mejor segmentación de la red.
3. *Protocolos de seguridad y aislamiento de recursos:* Configurar reglas de seguridad de red (grupos de seguridad) para controlar el tráfico y el acceso de los usuarios.
4. *Conexiones al sistema:* Utilizar AWS Direct Connect o VPN para conexiones seguras desde las instalaciones de DataTech.

#### **Costos mensuales:**

Sin costo adicional

- **App Service:**

- *DataTech desea implementar sus aplicaciones web utilizando servicios de App Service. Debes diseñar y configurar el entorno de App Service para permitir la implementación y escalabilidad de las aplicaciones web de la empresa. Considera aspectos como la selección del plan de App Service, la configuración de dominios personalizados, la implementación de certificados SSL, la configuración de escalabilidad automática basada en la demanda y la integración con los servicios de bases de datos.*

Servicio recomendado: **AWS Elastic Beanstalk**

1. *Implementación inicial:* Implementar aplicaciones web en Elastic Beanstalk para facilitar la implementación y la administración.
2. *Medidas de seguridad:* Configurar dominios personalizados y utilizar certificados SSL para la seguridad.
3. *Preparar sistema para ser escalable:* Establecer reglas de escalabilidad automática basada en métricas como la carga de la CPU o la demanda de red.
4. *Integración de infraestructura antigua:* Integrar Elastic Beanstalk con las bases de datos RDS / Aurora para una comunicación eficiente.

**Costos mensuales:**

Sin costo adicional

También consideramos importante resaltar los siguientes puntos debido a su relación con los servicios anteriores, y además pueden resultar de mucha utilidad e interés para la empresa:

1. *Least Privilege:* Se utiliza el servicio de Identity Access Manager (IAM) para segmentar los privilegios de diferentes usuarios e instancias de cómputo para restringir la libertad que tienen estos 'usuarios' sobre el sistema. De este modo garantizamos el acceso segregado a la información desde instancias de cómputo a bases de datos, archivos en buckets de S3, redes virtuales privadas, etc...
2. *Modelo Zero Trust:* Zero Trust es muy útil para la seguridad de red, lo que significa que no se confía automáticamente en ninguna entidad, incluso si está dentro de la red. Cada conexión se verifica y se autentica, proporcionando una capa adicional de seguridad.
3. *Segmentación de redes y NSG (Network Security Groups):* Puedes dividir la infraestructura de EC2 en segmentos de red y utiliza NSG para controlar el tráfico entre ellos. La segmentación mejora la seguridad al limitar la exposición y controlar el flujo de datos.

4. *Encriptación:* Es posible Implementar la encriptación en las instancias de EC2 para proteger datos sensibles durante el almacenamiento y la transferencia de datos. Esto puede incluir el uso de EBS encriptados y comunicaciones seguras a través de protocolos seguros (por ejemplo, SSH).

## **Conclusiones**

### **Luis:**

Al diseñar una arquitectura de Cloud es necesario tomar en cuenta la diversidad de servicios, casos de uso y productos que ofrecen los proveedores de servicio, así como las necesidades individuales del cliente con el que se trabaja. La principal ventaja que veo en cuanto a esta clase de arquitectura, es la modularidad que ofrece en los servicios y la libertad que ofrece en la customización de los mismos, permitiendo elegir los indicados para cumplir con las necesidades de negocio específicas de la empresa, además de proveer una red e infraestructura confiable que garantiza que su producto.

Elegimos AWS como proveedor de Cloud para esta actividad por nuestra experiencia empleándolo para la solución del reto, pero esta actividad sirvió para familiarizarnos con los beneficios que otorgan algunos de los servicios que no entran dentro del alcance de nuestro proyecto, como aquellos relacionados con escalabilidad (ELB), bases de datos (RDS / Aurora), redes virtuales privadas (VPC), y estos son solamente un puñado de los más de 200 servicios que ofrece AWS, lo cual sirve para poner en perspectiva la capacidad que tiene la infraestructura en la nube para ofrecer servicios de cómputo bajo demanda y de manera flexible a la medida de cada empresa.

### **Julian:**

El migrar una infraestructura a la nube puede implicar una inversión de muchos recursos y tiempo así que es importante tener un entendimiento de lo que se quiere obtener y un plan para su ejecución. A pesar de los costos puede ser un gran beneficio debido a varias características de las infraestructuras en la nube como lo son: la escalabilidad, la seguridad de los datos y la facilidad de gestión y administración. AWS cuenta con muy buenos servicios para empresas que están pensando en migrar sus infraestructuras a la nube. Tiene buenas herramientas para escalar y para tener generadas medidas de seguridad para los datos gracias a la facilidad de establecer reglas de seguridad y tener una gestión sobre los permisos de los usuarios. Adicionalmente, el uso de los buckets s3 para el almacenamiento de archivos agrega una capa de seguridad extra a la infraestructura.

### **Alberto:**

La migración de los servicios de DataTech a la nube a través de AWS se ha diseñado de manera integral, abordando múltiples aspectos para garantizar un despliegue seguro, eficiente y altamente disponible. Al considerar las distintas capas

de la infraestructura, desde máquinas virtuales hasta servicios de aplicaciones, se ha buscado cumplir con los siguientes objetivos clave:

- Seguridad: La implementación del principio de Least Privilege garantiza que los recursos tengan solo los permisos necesarios para ejecutar sus funciones, reduciendo la exposición a amenazas potenciales.
- Alta disponibilidad y escalabilidad: El uso de autoscaling groups y la distribución en zonas de disponibilidad garantiza que las Máquinas Virtuales (EC2) sean altamente disponibles y escalables para adaptarse a las demandas cambiantes de las aplicaciones.
- Gestión eficiente de datos: La combinación de bases de datos IaaS y PaaS permite a Data Tech gestionar sus datos de manera confiable y escalable, con opciones flexibles de respaldo y recuperación.
- Conectividad y Redes: La configuración de redes virtuales con una estructura bien definida, subredes y reglas de seguridad garantiza una conectividad segura y eficiente entre los diferentes componentes de la arquitectura.
- Gestión Financiera: Se consideró la selección cuidadosa de tipos de instancias, regiones y servicios específicos para cumplir con los requisitos de rendimiento sin exceder los recursos necesarios.

En resumen, la migración planificada a la nube utilizando los servicios de AWS proporciona a DataTech una infraestructura sólida y segura, con la flexibilidad necesaria para adaptarse a las cambiantes necesidades del negocio.

## **Bibliografía consultada:**

Amazon Web Services. (s.f.). *Amazon Route 53*. Recuperado de:  
<https://aws.amazon.com/es/route53/>

Amazon Web Services. (s.f.). *Elastic Load Balancing*. Recuperado de:  
<https://aws.amazon.com/es/elasticloadbalancing/>

Amazon Web Services. (s.f.). *Auto Scaling*. Recuperado de:  
<https://aws.amazon.com/es/autoscaling/>

Amazon Web Services. (s.f.). *Amazon Elastic Compute Cloud (EC2)*. Recuperado de:  
<https://aws.amazon.com/es/ec2/>

Amazon Web Services. (s.f.). *Amazon Virtual Private Cloud (VPC)*. Recuperado de:  
<https://aws.amazon.com/es/vpc/>

Amazon Web Services. (s.f.). *AWS Identity and Access Management (IAM)*. Recuperado de:  
<https://aws.amazon.com/es/iam/>

Amazon Web Services. (s.f.). *AWS Elastic Beanstalk*. Recuperado de:  
<https://aws.amazon.com/es/elasticbeanstalk/>

Amazon Web Services. (s.f.). *Amazon Relational Database Service (RDS)*. Recuperado de:  
<https://aws.amazon.com/es/rds/>

Amazon Web Services. (s.f.). *Amazon Aurora*. Recuperado de:  
<https://aws.amazon.com/es/rds/aurora/>