L3 💪Análisis de caso _ Modelos de implementación en la nube.docx.pdf

Alumno: Rodrigo Péndola
Modulo: 3

Situación inicial:

Una empresa del sector financiero está experimentando un rápido crecimiento y necesita mejorar la seguridad, escalabilidad y eficiencia de su infraestructura tecnológica. Actualmente, la empresa utiliza servidores físicos en sus oficinas para manejar transacciones, almacenamiento de datos y servicios internos. Sin embargo, los costos de mantenimiento y la falta de redundancia ante fallos han generado preocupaciones. La gerencia está considerando migrar su infraestructura a la nube, pero no está segura de qué modelo de implementación (pública, privada o híbrida) es el más adecuado. Requieren un análisis detallado para tomar una decisión informada.

Descripción del Caso:

En este caso, asumirás el rol de arquitecto de soluciones en la nube. Tu misión es evaluar la situación de la empresa y recomendar el modelo de implementación más adecuado según sus necesidades. Debes analizar los siguientes aspectos:
● Requerimientos de seguridad y cumplimiento normativo.
● Costo de operación y mantenimiento.
● Escalabilidad y capacidad de adaptación a cambios en la demanda.
● Gestión de datos y redundancia ante fallos.
● Disponibilidad y rendimiento de los servicios.
● Consideraciones estratégicas a largo plazo.

Instrucciones
Para resolver este caso, sigue los siguientes pasos:
1. Evaluación de la infraestructura actual: Identifica los principales problemas de la infraestructura on-premise.

La empresa enfrenta los siguientes desafíos con su infraestructura on-premise:

- **Altos costos** de mantenimiento y actualización de hardware.
- **Falta de redundancia**, lo que aumenta el riesgo de pérdida de datos ante fallos.
- **Escalabilidad limitada**, dificultando el crecimiento sostenido.
- **Desafíos en seguridad**, con mayores riesgos de ataques internos o fallos físicos.

2. Análisis de modelos de implementación: Explica las diferencias entre nube pública, privada e híbrida.

- **Nube pública:** Servicios ofrecidos por proveedores externos (AWS, Azure, Google Cloud). Ventajas: bajo costo inicial, escalabilidad y mantenimiento simplificado. Desventajas: menor control y dependencia del proveedor. **Nube privada:** Infraestructura dedicada exclusivamente a la empresa. Ventajas: mayor seguridad, cumplimiento normativo y control. Desventajas: costos elevados y menor flexibilidad.
- **Nube híbrida:** Combina nube pública y privada. Ventajas: equilibrio entre costos y seguridad, flexibilidad. Desventajas: complejidad en integración y administración.

3. Recomendación del modelo adecuado

Para una empresa financiera en crecimiento, **la nube híbrida** suele ser la mejor opción, ya que:

- Permite **seguridad reforzada** para datos sensibles en la nube privada.
- Ofrece **escalabilidad** con servicios en la nube pública cuando la demanda aumenta.
- Reduce costos en comparación con mantener toda la infraestructura on-premise.

4. Plan de migración

Pasos clave:

1. **Evaluación de datos y cargas de trabajo** para determinar qué mover a cada tipo de nube.
2. **Seleccionar proveedores de servicios** según costos, compatibilidad y cumplimiento normativo.
3. **Implementación de mecanismos de seguridad** como cifrado de datos y accesos controlados.
4. **Pruebas y validación** antes de la migración completa para evitar interrupciones.
5. **Capacitación del equipo** para gestionar la nueva infraestructura.

Medidas de Seguridad y Mitigación de Riesgos para la Migración a la Nube

Para garantizar una transición segura y proteger los datos y aplicaciones de tu empresa emergente, es clave implementar estrategias de seguridad *proactivas*. Aquí te detallo las **medidas esenciales** basadas en mejores prácticas de AWS/Azure y estándares internacionales:

1. Principales Riesgos en la Nube

Riesgo	**Impacto Potencial**
Accesos no autorizados	Robo de datos o sabotaje interno/externo.
Ataques DDoS	Inundación de tráfico que satura servicios.
Fugas de datos	Exposición accidental de información crítica.
Configuraciones erróneas	Servicios expuestos por errores humanos.

Cumplimiento legal	Sanciones por incumplir regulaciones (GDPR, LGPD).

2. Medidas de Mitigación por Capa

A. Identidad y Acceso (IAM)

- **Mínimos privilegios:** Asignar permisos solo a lo necesario (ej: solo-lectura para analistas).
- **Autenticación MFA:** Obligar doble factor (ej: Google Authenticator o tokens físicos).
- **Roles temporales:** Usar credenciales de corta duración para terceros.
- **Herramientas:**
  - AWS IAM / Azure Active Directory.

B. Protección de Datos

- **Cifrado:**
  - **En tránsito:** TLS 1.3 para conexiones (HTTPS, SFTP).
  - **En reposo:** AES-256 en discos (ej: AWS EBS, S3).
- **Gestión de claves:** Usar servicios gestionados (AWS KMS, Azure Key Vault).
- **Backups automatizados:**
  - Retención de 7 días (RPO < 1 hora).
  - Almacenados en otra región (ej: AWS S3 Cross-Region Replication).

C. Seguridad de Red

- **Segmentación:**
  - Redes privadas (VPC en AWS, VNet en Azure).
  - Subnets para frontend/backend/base de datos.
- **Firewalls y NACLs:**
  - Reglas que bloquean tráfico no esencial (ej: solo puerto 443 desde internet).
- **Protección DDoS:**
  - AWS Shield Standard (gratis) o Advanced (+$3,000 USD/mes).
  - Azure DDoS Protection.

D. Monitoreo y Detección

- **Logs centralizados:**
    - AWS CloudTrail (registro de actividades) + GuardDuty (detección de amenazas).
    - Azure Sentinel.
- **Alertas en tiempo real:**
    - Notificaciones por SMS/email ante intentos de acceso sospechosos.

E. Cumplimiento Normativo

- **Certificaciones:**
    - AWS: ISO 27001, SOC 2, GDPR.
    - Azure: HIPAA, FedRAMP.
- **Documentación:**

Políticas de retención de datos y procedimientos de respuesta a incidentes.

5. Evaluación de costos

Comparación de costos entre modelos:

Modelo	**Costo Inicial**	**Mantenimiento**	**Escalabilidad**	**Seguridad**
Nube Pública	Bajo	Bajo	Alta	Media
Nube Privada	Alto	Alto	Media	Alta
Nube Híbrida	Medio	Medio	Alta	Alta

6. Estrategias de seguridad y cumplimiento

- Implementar **cifrado de datos** para proteger información sensible.
- Garantizar **autenticación multifactor** para accesos seguros.
- Asegurar el **cumplimiento normativo** con auditorías y controles periódicos.

Seguridad:

Cómo mitigar el Downtime en la Nube

1. **Redundancia:** Usar múltiples servidores en zonas geográficas distintas (ej: AWS Availability Zones).
2. **Balanceo de carga:** Distribuir tráfico para evitar sobrecargas.
3. **Monitoreo en tiempo real:** Herramientas como CloudWatch (AWS) o Azure Monitor.
4. **Backups automatizados:** Permitir recuperación rápida ante fallos.
5. **SLA (Acuerdo de Nivel de Servicio):** Elegir proveedores con garantías de uptime (ej: 99.9%).

7. Caso de éxito

Un ejemplo destacado es el **Banco Santander**, que ha migrado a un modelo de nube híbrida para mejorar seguridad, escalabilidad y eficiencia operativa. Esto les ha permitido optimizar costos y garantizar un servicio confiable.

Si necesitas más detalles o ayuda con la redacción del informe, dime cómo te gustaría estructurarlo. ¡Vamos a hacerlo sólido! 🚀

3. Recomendación del modelo adecuado: Justifica tu elección con base en los requerimientos de la empresa.

Para una empresa financiera en crecimiento, **la nube híbrida** suele ser la mejor opción, ya que:

- Permite **seguridad reforzada** para datos sensibles en la nube privada.
- Ofrece **escalabilidad** con servicios en la nube pública cuando la demanda aumenta.
- Reduce costos en comparación con mantener toda la infraestructura on-premise.

4. Plan de migración: Define los pasos clave para la transición a la nube.
5. Evaluación de costos: Presenta una comparación de costos entre los diferentes modelos de implementación.
6. Estrategias de seguridad y cumplimiento: Explica cómo se pueden mitigar riesgos y cumplir normativas del sector financiero.

7. Caso de éxito: Presenta un ejemplo real de una empresa del sector financiero que haya implementado un modelo en la nube con éxito.

Entregables □ □ Los participantes deberán entregar un informe con los siguientes apartados:
● Resumen ejecutivo: Explicación breve de la propuesta.
● Análisis de la situación actual: Evaluación de problemas y necesidades de la empresa.
● Comparación de modelos de implementación: Explicación de ventajas y desventajas de cada opción.
● Recomendación y justificación: Modelo de implementación sugerido con su respectiva justificación.
● Plan de migración: Estrategia detallada para la transición a la nube.
● Evaluación de costos: Comparación de costos operativos.
● Medidas de seguridad y cumplimiento: Estrategias de mitigación de riesgos.
● Caso de éxito: Ejemplo de una empresa que haya adoptado un modelo de nube con éxito.

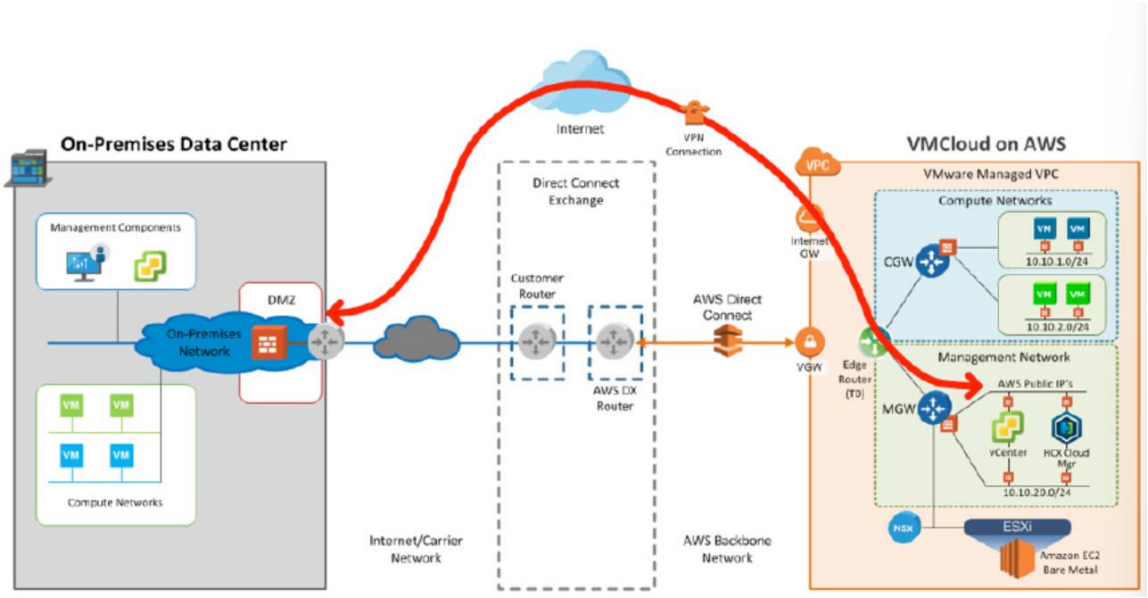
Datos que apoyan moción

¿Cuándo sí conviene mantener infraestructura local?

- **Datos ultra-sensibles:** Regulaciones estrictas (ej: gobierno).
- **Cargas de trabajo constantes:** Si la demanda no varía (ej: servidores de archivos internos).
- **Latencia crítica:** Aplicaciones que requieren respuesta en milisegundos (ej: trading algorítmico).

Para tu caso: La nube híbrida (parte en la nube, parte local) podría ser ideal si hay:

- Aplicaciones con demanda variable (nube pública).
- Datos sensibles que requieren control (nube privada o servidores locales).


On-Premises Data Center
Management Components
DMZ
On-Premises Network
VM
VM
VM
VM
Compute Networks
Internet
VPN Connection
Direct Connect Exchange
Customer Router
AWS DX Router
AWS Direct Connect
Internet/Carrier Network
AWS Backbone Network
VMCloud on AWS
VPC
VMware Managed VPC
Internet GW
VGW
Edge Router (T0)
Compute Networks
CGW
10.10.1.0/24
10.10.2.0/24
Management Network
AWS Public IP's
MGW
vCenter
HCX Cloud Mgr
10.10.20.0/24
NSX
ESXi
Amazon EC2 Bare Metal