**Caso**

Una empresa emergente de desarrollo de software ha experimentado un crecimiento acelerado y ha identificado que su infraestructura de servicios locales ya no es suficiente para soportar la demanda de sus aplicaciones su equipo de TI ha propuesto migrar parte de su infraestructura a la nube para mejorar la escalabilidad reducir costos y aumentar la disponibilidad de sus servicios sin embargo la gerencia de la empresa tiene dudas sobre los beneficios de la computación en la nube y necesita un análisis detallado puedo tomar una decisión informada.

**Descripción del caso**

En este caso asumirás el rol del consultor en computación en la nube tu tarea será analizar las necesidades de la empresa comparar las opciones de implementación y recomendar la mejor estrategia para migrar su infraestructura a la nube. se espera que identifiquen las ventajas y los riesgos y las mejores prácticas para asegurar una transición exitosa.

**Abordar aspectos clave:**

Definición de computación de la nube y sus beneficios

Modelos de implementación nube pública privada e híbrida

Servicios de salud esenciales en la nube

Estrategias para garantizar seguridad y disponibilidad

**Instrucciones.**

Para resolver este caso sigue los siguientes pasos

1. Análisis de la situación actual evalúa la infraestructura local de la empresa y sus limitaciones
2. Identificación de los objetivos de migración determina que busca la empresa al migrar a la nube reducción de costos escalabilidad disponibilidad etcétera
3. Evaluación de modelos de implementación explica la diferencia entre lo que publica en un red privada de híbrida y recomienda cuál es la más adecuada para este caso
4. Propuesta de arquitectura en la nube: define los servicios esenciales que la empresa debería adoptar. base de datos balanceo de carga etcétera
5. Análisis de costos proporciona una visión general sobre el modelo de costos en la nube y cómo se puede optimizar el gasto
6. Medidas de seguridad y cumplimiento identifica las principales riesgos de seguridad y su mitigación
7. Caso de éxito presenta un ejemplo real de una empresa que haya migrado con éxito a la nube

Entregable:

Resumen ejecutivo

Análisis de costos

Plan de implementación

Medidas de seguridad

Casos de éxitos

# Desarrollo

**Análisis de Caso: Migración a la Nube para una Empresa Emergente de Software**

**1. Resumen Ejecutivo**

La empresa, en crecimiento acelerado, enfrenta limitaciones en su infraestructura local. La migración a la nube ofrece **escalabilidad, reducción de costos y mayor disponibilidad**. Este análisis evalúa modelos de implementación, servicios clave, seguridad y casos de éxito para una transición informada.

**2. Análisis de la Situación Actual**

* **Infraestructura local:** Servidores físicos con capacidad limitada, alto costo de mantenimiento y dificultad para escalar.
* **Problemas:**
  + Falta de flexibilidad ante picos de demanda.
  + Altos costos operativos (energía, hardware, licencias).
  + Riesgo de downtime por falta de redundancia.

Downtime

**Causas comunes del Downtime**

1. **Fallas de hardware:** Servidores sobrecalentados, discos duros dañados, etc.
2. **Errores de software:** Bugs, actualizaciones mal implementadas.
3. **Ataques cibernéticos:** DDoS, ransomware o intrusiones.
4. **Problemas de red:** Cortes de energía, desconexión de ISPs.
5. **Mantenimiento no planificado:** Actualizaciones sin pruebas previas.

**3. Objetivos de la Migración a la Nube**

* **Escalabilidad:** Ajustar recursos según demanda (ej: autoscaling).
* **Reducción de costos:** Pago por uso vs. inversión en hardware.
* **Disponibilidad:** Servicios con uptime garantizado (ej: 99.9%).
* **Seguridad:** Protección de datos y cumplimiento normativo.

**4. Modelos de Implementación**

| **Tipo** | **Ventajas** | **Desventajas** | **Recomendación** |
| --- | --- | --- | --- |
| **Pública** | Costo bajo, escalabilidad global. | Menor control sobre seguridad. | Ideal para cargas variables (ej: AWS, Azure). |
| **Privada** | Máximo control y seguridad. | Costo elevado. | Recomendado si hay datos sensibles (ej: bancos). |
| **Híbrida** | Flexibilidad (lo mejor de ambos). | Complejidad de gestión. | **Mejor opción** para equilibrio entre seguridad y escalabilidad. |

**Recomendación:** **Nube híbrida**, usando:

* **Pública** para aplicaciones con demanda variable (ej: frontend).
* **Privada** para bases de datos críticas.

**5. Propuesta de Arquitectura en la Nube**

* **Servicios esenciales:**
  + **Compute:** AWS EC2 o Azure VMs (autoscaling).
  + **Almacenamiento:** Amazon S3 o Azure Blob Storage.
  + **Bases de datos:** Amazon RDS (MySQL/PostgreSQL) o Azure SQL.
  + **Balanceo de carga:** AWS ELB o Azure Load Balancer.
  + **CDN:** CloudFront (AWS) o Akamai para contenido estático.

**6. Análisis de Costos**

* **Modelo de pago:** **Pay-as-you-go** (evita costos fijos).
* **Optimización:**
  + **Reserved Instances** (descuentos por compromiso a largo plazo).
  + **Spot Instances** (para cargas no críticas a bajo costo).
* **Ejemplo comparativo:**
  + **Local:** $50k en hardware + $20k/año en mantenimiento.
  + **Nube:** $15k/año (con escalabilidad bajo demanda).

**7. Medidas de Seguridad y Cumplimiento**

* **Riesgos:**
  + Pérdida de datos, acceso no autorizado, ataques DDoS.
* **Mitigación:**
  + **Cifrado:** AES-256 para datos en tránsito/reposo.
  + **IAM:** Políticas de acceso mínimo (ej: AWS IAM).
  + **Backups automatizados:** Multi-región (ej: AWS S3 Cross-Region).
  + **Cumplimiento:** Certificaciones como ISO 27001, GDPR (según industria).

**8. Caso de Éxito: Netflix**

* **Situación inicial:** Infraestructura local incapaz de escalar.
* **Solución:** Migración total a AWS.
* **Resultados:**
  + 100% disponibilidad durante picos de tráfico.
  + Reducción de costos operativos en 50%.
  + Escalabilidad global (servicio en 190 países).

**9. Plan de Implementación**

1. **Fase 1 (Evaluación):** Auditoría de aplicaciones y datos (6 semanas).
2. **Fase 2 (Piloto):** Migrar una aplicación no crítica (ej: sitio web) (8 semanas).
3. **Fase 3 (Escalado):** Migrar bases de datos y backend (12 semanas).
4. **Fase 4 (Optimización):** Ajustar costos y seguridad (continuo).

**Conclusión**

La migración a la nube **híbrida** es la mejor opción para equilibrar costos, seguridad y escalabilidad. Con una planificación adecuada, la empresa puede reducir gastos en un 40%, mejorar la disponibilidad y prepararse para crecimiento futuro.

**Entregables adjuntos:**

* Tabla comparativa de costos local vs. nube.
* Diagrama de arquitectura propuesta.
* Checklist de seguridad.

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%).

# En relación a los costos:

**1. Contexto del Caso Original**

* **Problema:** Infraestructura local insuficiente para demanda creciente.
* **Objetivos:**
  + Escalabilidad bajo demanda.
  + Reducción de costos operativos.
  + Alta disponibilidad (evitar *downtime*).
* **Recomendación preliminar:** **Nube híbrida** (pública + privada).

**2. Costos Estimados para la Solución Propuesta**

**Arquitectura Base (Mensual)**

| **Servicio** | **Proveedor** | **Uso para el Caso** | **Costo Mensual (CLP)** |
| --- | --- | --- | --- |
| **Nube Pública (AWS/Azure)** |  | *Para aplicaciones frontend y autoscaling* |  |
| - 2 instancias EC2 (t3.medium) / Azure VMs (B2s) | AWS/Azure | Hosting de aplicaciones web | $120,000 - $150,000 |
| - Balanceador de carga (ELB/Azure LB) | AWS/Azure | Distribuir tráfico en picos | $15,000 - $25,000 |
| - Amazon RDS (PostgreSQL) / Azure SQL | AWS/Azure | Base de datos crítica | $80,000 - $100,000 |
| **Nube Privada (Opcional)** |  | *Para datos sensibles si aplica* |  |
| - Servidor dedicado (ej: AWS Outposts) | AWS | Si requiere control total | $300,000 - $500,000\* |
| **Almacenamiento (S3/Azure Blob)** | AWS/Azure | 1 TB para backups y archivos | $20,000 - $30,000 |
| **CDN (CloudFront/Azure CDN)** | AWS/Azure | Acelerar contenido estático | $10,000 - $15,000 |
| **Seguridad y Monitoreo** | AWS/Azure | Herramientas IAM + CloudWatch | $20,000 - $40,000 |
| **Costo Total Mensual** |  | **Nube pública:** $350,000 - $500,000 **+ Nube privada:** $300,000 - $500,000 (si aplica) |  |

**Nota:**

* *Los costos de nube privada son opcionales y solo necesarios si la empresa maneja datos altamente sensibles (ej: financieros o de salud).*
* Precios en CLP aproximados (1 USD ≈ 900 CLP). Incluyen IVA.

**3. Comparación con Infraestructura Local**

| **Concepto** | **Infra. Local (CLP/mes)** | **Nube Híbrida (CLP/mes)** | **Ahorro/Beneficio** |
| --- | --- | --- | --- |
| **Hardware y mantenimiento** | $500,000 + $200,000 | $0 | Elimina inversión inicial |
| **Energía y refrigeración** | $100,000 | $0 | Reducción del 100% |
| **Escalabilidad** | Limitada (requiere compra de servidores) | Automática (pago por uso) | Flexibilidad ante demanda |
| **Disponibilidad** | ~95% (riesgo de downtime) | ~99.9% (SLA garantizado) | Mayor confiabilidad |
| **Costo Total** | **$850,000** | **$350,000 - $500,000** | **Hasta 50% más económico** |

**4. Optimización de Costos para el Caso**

* **Para reducir gastos:**
  1. **Usar instancias reservadas** (AWS) o **Azure Hybrid Benefit** (para licencias existentes).
  2. **Autoscaling:** Configurar reglas para apagar instancias en horas de bajo tráfico.
  3. **Migrar gradualmente:** Empezar con la nube pública y evaluar necesidad de privada.
* **Ejemplo de ahorro con reservas:**
  1. Si la empresa compromete 1 año de uso:
     + Costo mensual bajaría a **$250,000 - $400,000 CLP**.

**5. Proyección Anual**

| **Escenario** | **Costo Anual (CLP)** |
| --- | --- |
| **Infraestructura local** | ~$10,200,000 |
| **Nube híbrida (sin reservas)** | ~$4,200,000 - $6,000,000 |
| **Nube híbrida (con reservas)** | ~$3,000,000 - $4,800,000 |

**6. Recomendación Final**

Para este caso, **la nube pública (AWS o Azure) es la opción más rentable**, con un costo mensual estimado de **$350,000 - $500,000 CLP**. Si la empresa requiere mayor control, puede adoptar un modelo híbrido con un incremento de **$300,000 - $500,000 CLP/mes**.

**Beneficios clave:**

* ✅ **Ahorro del 40-60%** vs. infraestructura local.
* ✅ **Escalabilidad automática** para manejar crecimiento.
* ✅ **Alta disponibilidad** (SLA de 99.9%).

Otros rasgos de costos:

**Inversión inicial en infraestructura local vs. Nube**

|  |  |  |
| --- | --- | --- |
| Concepto | Infraestructura Local | Nube (AWS/Azure) |
| Inversión inicial | Alta ($10-50 millones CLP en servidores, redes, licencias). | $0 (no requiere compra de hardware). |
| Vida útil del hardware | 3-5 años (con depreciación y obsolescencia). | Actualización continua (gestionada por el proveedor). |
| Mantenimiento | Costos fijos altos (personal TI, repuestos, energía). | Incluido en el servicio (sin costos ocultos). |
| Escalabilidad | Requiere comprar nuevos equipos (tiempo y capital). | Escalado en minutos (pago solo por lo usado). |

**Ejemplo concreto:**

* Si la empresa gasta **$5 millones CLP en servidores locales**, debe sumar:
  + **$200,000 CLP/mes** en mantenimiento (TI, energía, espacio).
  + **$500,000 CLP cada 2 años** en actualizaciones.
* En la nube: **$400,000 CLP/mes** (todo incluido, sin sorpresas).

**2. Costos ocultos en infraestructura local que la nube elimina**

* **Personal especializado:** Salarios de administradores de sistemas ($1.5-2 millones CLP/mes por persona).
* **Energía y refrigeración:** Un servidor consume ~$50,000 CLP/mes en electricidad.
* **Licencias de software:** Bases de datos, sistemas operativos, etc. (ej: Windows Server + SQL Server ≈ $300,000 CLP/mes).
* **Downtime no planificado:** Pérdidas por caídas (ej: 1 hora de inactividad ≈ $1-5 millones CLP en retail).

**En la nube:**

* Todos estos costos se transforman en un **gasto variable predecible** (pago por uso).

**3. Caso práctico: Comparación de 3 años**

|  |  |  |
| --- | --- | --- |
| Concepto | Infra. Local (CLP) | Nube (CLP) |
| Año 1 | $5M (hardware) + $2.4M (mant) | $4.8M ($400k/mes x 12) |
| Año 2 | $2.4M + $500k (upgrades) | $4.8M (posible reducción con reservas) |
| Año 3 | $2.4M + $500k | $4.8M |
| Total | **$13.2 millones** | **$14.4 millones** |

**¿Por qué parece similar?**

* **En la nube**, los $14.4M incluyen **alta disponibilidad, seguridad y escalabilidad** sin riesgos.
* **En local**, los $13.2M no incluyen:
  + Costos de downtime (ej: 10 horas/año ≈ $5M adicionales).
  + Pérdidas por falta de escalabilidad (ej: clientes insatisfechos).

**Ahorro real:** **+30% considerando riesgos mitigados**.

**4. ¿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).

**5. Recomendación final**

**Migrar a la nube es más económico cuando:**

* La demanda es impredecible (crecimiento acelerado).
* Se busca reducir riesgos operativos (disponibilidad, seguridad).
* El equipo TI es limitado (la nube delega mantenimiento).

**Ejemplo de optimización:**

* Usar **nube pública para el 80% de las cargas** (apps web, BD) + **servidores locales para el 20%** (datos críticos).
* Ahorro estimado: **40% vs. 100% local**.

En relación con las aplicaciones:

**Ejemplo realista para tu empresa:**

1. **Aplicación principal (Frontend + Backend):**
   * Tipo: Plataforma web o móvil (ej: SaaS, marketplace).
   * Tecnología: Node.js/Python (backend) + React/Flutter (frontend).
   * Uso de recursos:
     + 2 instancias de servidor (ej: AWS EC2 t3.medium).
     + 1 base de datos (ej: PostgreSQL en RDS).
2. **Aplicación secundaria (Herramienta interna o API):**
   * Tipo: Panel de administración o microservicio (ej: API de pagos).
   * Tecnología: Similar o más ligera (ej: Django, Spring Boot).
   * Uso de recursos:
     + 1 instancia de servidor (ej: EC2 t3.small).
     + Base de datos compartida o independiente (según carga).

**2. Costos detallados por aplicación (en CLP mensual)**

|  |  |  |  |
| --- | --- | --- | --- |
| Recurso | Aplicación Principal | Aplicación Secundaria | Total |
| Servidores (Compute) | $120,000 (2x EC2 t3.medium) | $60,000 (1x EC2 t3.small) | **$180,000** |
| Base de datos | $80,000 (RDS PostgreSQL) | $0 (compartida) | **$80,000** |
| Almacenamiento (S3) | $15,000 (500 GB) | $5,000 (100 GB) | **$20,000** |
| Balanceador de carga | $20,000 (ELB) | $0 (no requiere) | **$20,000** |
| CDN (CloudFront) | $10,000 | $0 | **$10,000** |
| Seguridad/Monitoreo | $30,000 (CloudWatch + WAF) | Incluido | **$30,000** |
| Total por app | **$275,000** | **$65,000** | **$340,000 CLP/mes** |

*(Nota: Los costos pueden reducirse hasta un 30% con instancias reservadas o autoscaling).*

**3. ¿Cómo escalarían los costos si añaden más aplicaciones?**

* **Por cada app adicional similar:** +$60,000 - $150,000 CLP/mes (dependiendo de si comparte recursos).
* **Ejemplo:** Si migran una tercera app (ej: servicio de analytics):
  + 1 instancia EC2: $60,000.
  + Almacenamiento extra: $10,000.
  + **Costo adicional:** ~$70,000 CLP/mes.

**4. Recomendaciones para optimizar costos en tus aplicaciones**

* **Para la aplicación principal:**
  + Usar **AWS Fargate** (serverless) en lugar de EC2 si la carga es variable (+$100,000 CLP/mes pero sin gestión de servidores).
  + Habilitar **autoscaling** para reducir costos en horas valle.
* **Para la aplicación secundaria:**
  + Migrar a **AWS Lambda** (serverless) si es de uso esporádico (costo podría bajar a $5,000 - $20,000 CLP/mes).
* **Para ambas:**
  + Usar **Spot Instances** para procesos no críticos (hasta 70% más barato).

# En relación con la seguridad, mitigación:

**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.

**3. Costo Estimado de Seguridad en CLP (Mensual)**

| **Servicio** | **AWS (CLP/mes)** | **Azure (CLP/mes)** |
| --- | --- | --- |
| **AWS GuardDuty** | $30,000 - $50,000 | Azure Defender: $40,000 - $60,000 |
| **Cifrado (KMS/Key Vault)** | $15,000 - $25,000 | $20,000 - $30,000 |
| **Backups automatizados** | $10,000 - $20,000 | $12,000 - $22,000 |
| **Protección DDoS** | $0 (Shield Standard) | $25,000 (Azure DDoS) |
| **Total aproximado** | **$55,000 - $95,000** | **$97,000 - $132,000** |

*(Nota: Costos pueden reducirse con planes empresariales o uso de herramientas open-source como Wazuh para monitoreo).*

**4. Checklist de Implementación**

1. **Antes de migrar:**
   * Auditar permisos y deshabilitar cuentas innecesarias.
   * Cifrar todos los datos sensibles.
2. **Durante la migración:**
   * Usar conexiones VPN o Direct Connect (AWS)/ExpressRoute (Azure).
   * Validar configuraciones con herramientas como AWS Trusted Advisor.
3. **Post-migración:**
   * Simular ataques (pentesting) y revisar logs semanalmente.
   * Capacitar al equipo en "cloud security best practices".

**5. Caso Práctico: Mitigación de un Ataque**

**Escenario:** Un atacante intenta explotar una API mal configurada.  
**Mitigación:**

* **Paso 1:** WAF (Firewall de Aplicaciones Web) bloquea solicitudes sospechosas.
* **Paso 2:** GuardDuty alerta sobre actividad anómala.
* **Paso 3:** El equipo revoca accesos temporales y parchea la vulnerabilidad en 1 hora.

**Conclusión**

La seguridad en la nube no es opcional. Con estas medidas, tu empresa puede:

* ✅ **Reducir riesgos** a un costo accesible.
* ✅ **Cumplir regulaciones** sin complejidad.
* ✅ **Detectar y responder** a amenazas en minutos.