EVALUACIÓN MODULAR 9

ACTIVIDAD 1

1. Explica con tus propias palabras qué es la computación en la nube. Utiliza analogías o ejemplos cotidianos.

   La computación en la nube es el suministro bajo demanda de recursos informáticos (servidores, almacenamiento, bases de datos, redes, software, análisis, inteligencia) a través de internet (“la nube”), con pago por uso y sin necesidad de gestionar infraestructura física. Un ejemplo de ello es Netflix que paga sólo por capacidad utilizada durante el streaming alto.

2. Diferencia los modelos de servicios IaaS, PaaS, SaaS y FaaS con un ejemplo práctico para cada uno aplicable al caso de Retail360.

Modelo	Definición	Ejemplo en Retail360
IaaS (Infrastructure as a Service)	Alquiler de infraestructura virtual: servidores, redes, almacenamiento. El cliente gestiona SO, apps, datos.	Usar Amazon EC2 + EBS + VPC para alojar servidores de facturación electrónica personalizados.
PaaS (Platform as a Service)	Plataforma para desarrollar, probar y desplegar aplicaciones sin gestionar infraestructura subyacente.	Usar AWS Elastic Beanstalk O Google App Engine para desplegar el backend del CRM sin preocuparse por los servidores.
SaaS (Software as a Service)	Aplicaciones listas para usar, accesibles por navegador. Todo está gestionado por el proveedor.	Usar Salesforce para marketing digital o QuickBooks Online para contabilidad.
FaaS (Function as a Service)	Ejecución de código en respuesta a eventos, sin servidores persistentes (serverless).	Usar AWS Lambda para procesar automáticamente nuevos pedidos en S3: validar, enriquecer y enviar a la base de datos.

3. Compara los modelos de implementación (nube pública, privada, híbrida, comunitaria) e indica cuál recomendarías para Retail360. Justifica tu elección técnica y organizacionalmente.

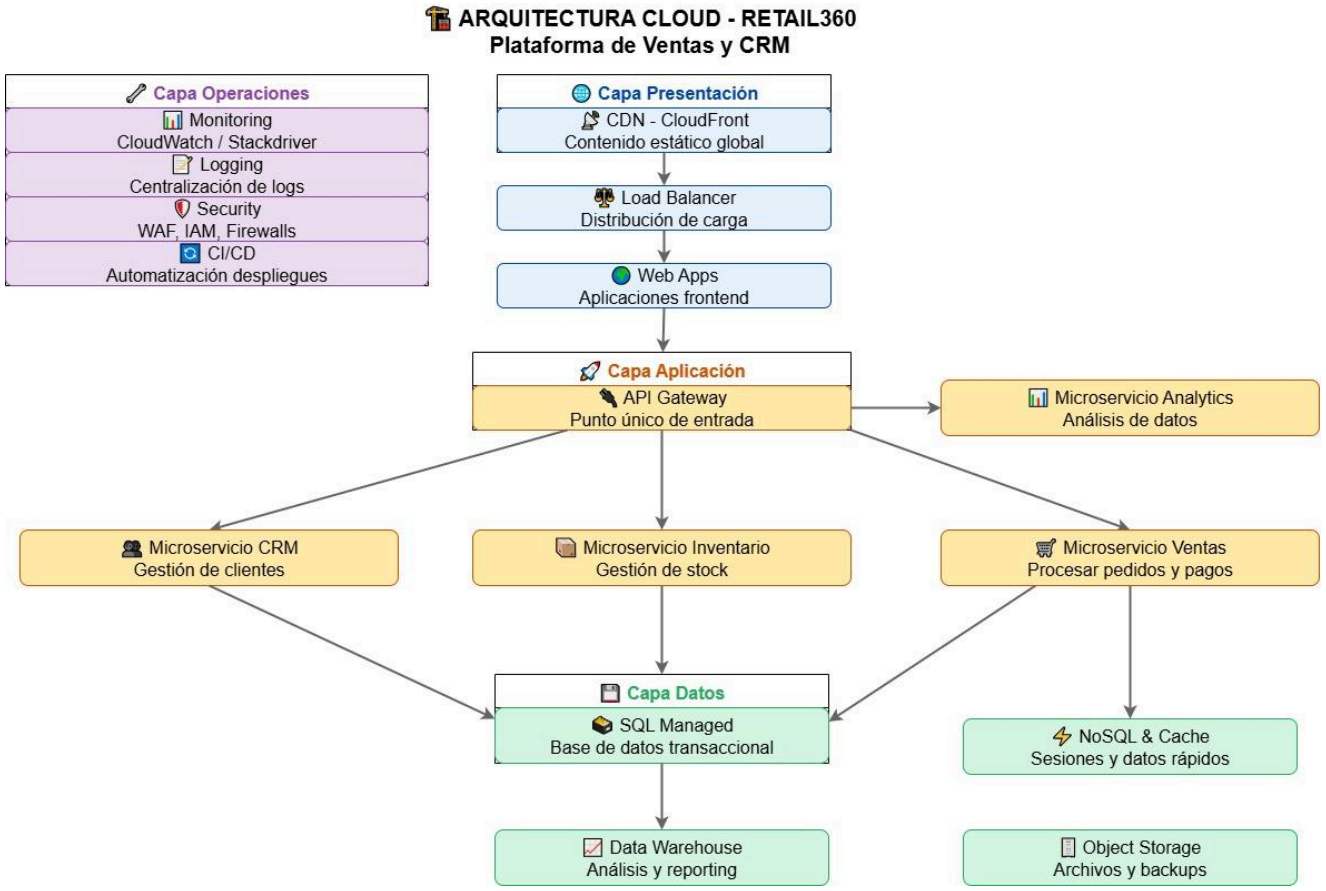
Modelo	Características	¿Adecuado para Retail360?
Pública	Recursos compartidos, bajo costo, escalable.	Parcialmente
Privada	Infraestructura dedicada, mayor control y seguridad.	Costoso para una pyme
Híbrida	Combina pública + privada. Datos sensibles en privada, apps escalables en pública	Recomendada
Comunitaria	Compartida entre organizaciones del mismo sector (ej. salud, banca).	No aplica

Justificación: Retail360 es una empresa mediana que necesita escalabilidad (ventas online), seguridad (facturación, datos de clientes) y control de costos.

- Datos sensibles (facturación, CRM) pueden residir en una VPC privada con encriptación y IAM estricto (modelo híbrido lógico dentro de la nube pública).
- Cargas variables (marketing, análisis) se benefician de la elasticidad de la nube pública.
- No requiere infraestructura on-premise, por lo que una arquitectura híbrida lógica en AWS/Azure (usando zonas privadas y públicas) es óptima.

ACTIVIDAD 2

1. Elabora un esquema de arquitectura lógica (puede ser un diagrama o descripción textual) para desplegar la solución en la nube. Debe incluir: almacenamiento, base de datos, balanceadores, servicios de backend, herramientas de monitoreo y seguridad.



2. Clasifica los servicios en una tabla como la siguiente:

componente	Tipo de servicio cloud	Proveedor propuesto	Justificación
Servidores Web/API	PaaS / CaaS	AWS ECS Fargate	Serverless, sin gestión de nodos, escala automática
Base de datos transaccional	DBaaS (PaaS)	Amazon RDS (PostgreSQL)	Alta disponibilidad, backups automáticos, compatible con CRM
Almacenamiento de datos crudos	IaaS / Object Storage	Amazon S3	Durable, seguro, bajo costo, integrado con Glue
Procesamiento ETL	PaaS	AWS Glue	Serverless, catálogo integrado, soporte PySpark
Data Warehouse	DWaaS	Amazon Redshift	Optimizado para analítica, integración con BI
Balanceador de carga	IaaS/PaaS	AWS ALB	Gestión automática de tráfico, TLS integrado
Monitorización	SaaS	Amazon CloudWatch	Métricas, logs, alertas nativas
Seguridad perimetral	SaaS	AWS WAF + Shield	Protección contra DDoS y OWASP Top 10

3. Diseña una propuesta de automatización del despliegue (CI/CD) e indica qué herramientas utilizarías (por ejemplo, Jenkins, GitHub Actions, GitLab CI/CD, etc.).

   Cuando pensamos en cómo modernizar los despliegues en Retail360, se nos vino a la mente la imagen de una línea de producción bien aceitada. Lo que buscamos es crear ese mismo flujo eficiente para sus sistemas, pero aplicado al desarrollo de software. La idea central es simple: cada vez que sus desarrolladores integran código nuevo, queremos que este recorra automáticamente un camino de validaciones hasta llegar a producción de forma segura y confiable.

- **Por qué elegimos estas herramientas**

  Después de evaluar varias opciones, nos decidimos por GitLab CI/CD como el corazón de nuestra automatización. La verdad es que nos convence más que Jenkins para su caso particular porque viene "todo en uno" - tienen el repositorio de código y los pipelines integrados, lo que significa menos dolores de cabeza para su equipo de sistemas. Para alguien que está empezando en este mundo de la automatización, la curva de aprendizaje es más amable.

El resto del ecosistema lo completamos con Docker, que nos permite empaquetar cada aplicación con todo lo que necesita para funcionar, evitando esos típicos problemas de "en mi máquina sí funciona". Las imágenes resultantes las guardamos en Amazon ECR, que es como un almacén seguro y organizado para estas "cajas" con nuestras aplicaciones. Cuando toca desplegar, usamos Kubernetes porque nos da esa flexibilidad de escalar automáticamente cuando hay mucha demanda en la tienda online, y además nos permite volver rápidamente a una versión anterior si algo sale mal.

- **Cómo funciona el proceso en la práctica**

Imaginen que un desarrollador termina una nueva funcionalidad para el CRM. Al integrar sus cambios, se activa automáticamente lo que nosotros llamamos el "pipeline". Primero, el sistema construye la aplicación y ejecuta todas las pruebas automáticas - es como poner el código bajo un microscopio para asegurarnos de que no rompe nada existente.

Si todo va bien, pasamos a una fase de seguridad donde escaneamos el código en busca de vulnerabilidades y hacemos pruebas más exhaustivas. Aquí somos bastante estrictos - si encontramos algún problema de seguridad, el proceso se detiene hasta que se resuelva.

La siguiente parada es el entorno de staging, que es como una réplica de producción donde hacemos pruebas finales. Solo cuando todo está verificado y el equipo da su visto bueno manual, procedemos al despliegue en producción. Aquí usamos una técnica llamada blue-green que básicamente nos permite tener dos versiones corriendo simultáneamente y cambiar el tráfico entre ellas sin interrupciones. Si detectamos cualquier anomalía, podemos volver atrás en segundos.

- **Lo que esto significa para Retail360**

En el día a día, esto se traduce en poder lanzar nuevas funcionalidades de su plataforma de ventas con mucha más frecuencia y menos riesgo. Su equipo de marketing podrá implementar campañas estacionales sin depender de largos procesos manuales, y sus desarrolladores recibirán feedback inmediato sobre su código.

Lo bonito de este sistema es que, aunque parece complejo por detrás, para sus equipos se convierte en algo transparente - simplemente integran su código y el resto funciona automáticamente, con todos los controles de calidad y seguridad integrados. Y lo más importante: les da la paz mental de saber que cada despliegue ha pasado por múltiples validaciones antes de llegar a sus clientes.

Al final, lo que perseguimos es que Retail360 pueda concentrarse en lo que mejor hace - vender y atender a sus clientes - mientras la infraestructura tecnológica responde ágilmente a sus necesidades de negocio.

ACTIVIDAD 3

1. Identifica tres riesgos asociados al uso de la nube en la empresa.

- **Exposición accidental de datos** (ej. bucket S3 público)
- **Accesos no autorizados** por mala configuración de IAM
- **Pérdida de datos** por falta de backups o retención

2. Relaciona cada riesgo con una normativa aplicable (por ejemplo: GRPR, HIPAA, ISO 27001).

Riesgo	Normativa
Exposición de datos personales	**GDPR** (si opera en UE) o **Ley de Protección de Datos locales**
Accesos no autorizados	**ISO/IEC 27001** (SGSI)
Pérdida de datos	**ISO 27001** + **PCI DSS** (si maneja pagos)

3. Propón al menos dos mecanismos técnicos de mitigación (firewalls, IAM, cifrado, etc.).

Para proteger los sistemas de Retail360 en la nube, proponemos dos mecanismos clave que funcionan como capas de seguridad complementarias:

- **Cifrado integral de datos**
  Implementamos cifrado tanto para la información en tránsito como para la almacenada. Es como poner cada dato en una caja fuerte: cuando viaja entre sistemas usamos TLS (como un túnel seguro), y cuando está guardado en bases de datos aplicamos cifrado en reposo. Así, incluso si alguien accede al almacenamiento, sólo verá información ilegible sin la llave de descifrado.
- **Gestión estricta de accesos (IAM)**
  Aplicamos el "principio del menor privilegio": cada usuario o sistema solo puede acceder a lo estrictamente necesario para su función. Por ejemplo, el equipo de marketing accede a datos comerciales pero no financieros, y exigimos autenticación en dos pasos para accesos administrativos. Es como un edificio con llaves diferenciadas donde cada persona entra solo a las áreas que necesita.

La combinación de estos mecanismos crea una defensa en profundidad: el IAM controla quién puede acceder a qué, mientras el cifrado protege los datos en sí mismos. Para Retail360, esto significa operar con la tranquilidad de que su información sensible está segura, sin complicar el trabajo diario de sus equipos.

4. Diseña una política básica de control de accesos basada en roles (RBAC) para los perfiles de la organización.

   En Retail360 implementaremos un sistema de acceso basado en 5 roles principales:

- **Desarrolladores** - Acceso a entornos de desarrollo y testing, sin permisos en producción.
- **Administradores** - Acceso completo con autenticación en dos pasos y registro de todas sus acciones.
- **Analytics/Marketing** - Solo lectura y exportación de datos comerciales, sin capacidad de modificación.
- **Atención al Cliente** - Acceso limitado al CRM, sin datos financieros sensibles.
- **Gerentes** - Lectura general más capacidad para aprobar flujos de trabajo específicos.

   Cada nuevo empleado se asignará a uno o varios grupos según su función, garantizando que tenga acceso solo a lo necesario para su trabajo. Esta estructura nos permite mantener seguridad sin perder agilidad operativa.

ACTIVIDAD 4

1. El modelo de pago por uso es el principio fundamental de la computación en la nube. Significa que una empresa sólo paga por los recursos de TI como lo son por ejemplo cómputo, almacenamiento, bases de datos, redes, entre otros que realmente consume y por el tiempo que los utiliza, sin necesidad de grandes inversiones iniciales de capital.
   Las implicaciones para una Empresa Mediana son:
   - Flexibilidad financiera, convierte los gastos de capital en gastos operativos, no requiere compra de servidores ni licencias por adelantado priorizando la inversión en el negocio principal.
   - Escalabilidad elástica, permite aumentar o disminuir instantáneamente los recursos bajo demanda permite utilizar recursos de manera temporal o estacional según lo requiera el negocio, así una empresa puede competir con grandes corporaciones manejando fluctuaciones de tráfico sin invertir en infraestructura sobredimensionada
   - Riesgo de gestión, La facturación puede volverse compleja. Pagar por cada minuto, gigabyte, o transacción requiere una gestión y monitoreo constante, corriendo el riesgo de facturas inesperadas, si los recursos no se gestionan adecuadamente pueden quedar encendidos por error.
   - Innovación acelerada, permite probar nuevos servicios como IA o lanzar nuevos proyectos con un costo inicial mínimo o nulo, fomentando la experimentación y disminuyendo la barrera de entrada a la tecnología de vanguardia.

2. Creamos la siguiente situación, uso de un Balanceador de Carga sin instancias activas.
   Una empresa mediana configura un Balanceador de Carga para distribuir el tráfico a un grupo de servidores web. Sin embargo, debido a un error de configuración o un cambio de arquitectura, se elimina por completo el grupo de instancias que estaba detrás del balanceador, pero se olvida de eliminar el balanceador en sí.
   - ❖ Consecuencia (Sobrecosto):
     Aunque no haya tráfico real llegando, el Balanceador de Carga permanece activo en la nube. Los proveedores cloud cobran por la "existencia" del balanceador y por las "reglas de procesamiento" asociadas, incluso si la utilización es cero. Esto puede generar un cargo fijo de varias decenas o cientos de dólares mensuales sin que el servicio esté produciendo valor.
   - ❖ Solución Técnica:
     Implementar Políticas de Eliminación, por ejemplo utilizar herramientas de Infraestructura como Código (IaC) como Terraform o CloudFormation. Estas herramientas garantizan que, al eliminar un recurso principal, los recursos dependientes se eliminen o se desvinculen correctamente.
     Configurar Alarmas de Uso/Costos: Establecer Alertas de Presupuesto y Alarmas de Métrica.
     - ○ Alarma de Costo: Notificación si el costo diario/semanal de los servicios de *Networking* o *Load Balancer* supera un umbral predefinido.
     - ○ Alarma de Métrica: Configurar una alerta si el Balanceador de Carga muestra una métrica de tráfico o conexión cercana a cero durante un período prolongado, indicando que está activo, pero inactivo, y debe ser revisado o eliminado.

3. La estrategia que elaboramos para la optimización de costos en la nube se basa en alinear el gasto con las necesidades reales del negocio.

   - ❖ Apagado Automático de Instancias: Consiste en automatizar el apagado y encendido de recursos de cómputo o Máquinas Virtuales que no se necesitan 24/7.
     Implementación: Ideal para entornos de Desarrollo, Prueba (QA) y Staging, así como para estaciones de trabajo virtuales que solo se usan en horario laboral.
     Utilizar herramientas nativas de la nube un ejemplo es AWS Instance Scheduler, o generar scripts Lambda/Functions para
     - Apagar instancias a las 7:00 PM de lunes a viernes
     - Encender instancias a las 8:00 AM del día siguiente
     - Apagar totalmente los viernes a las 7:00 PM, hasta el lunes a las 8:00 AM.

     Esto generará un ahorro estimado, de operar solo 40 horas de 168 a la semana, se puede lograr un ahorro de hasta un 76% en los costos de cómputo para esas instancias.

Tipo de Instancia	Descripción	Uso Recomendado
Bajo Demanda (On-Demand)	Se paga por hora o segundo. Máxima flexibilidad, sin compromiso a largo plazo.	Proyectos nuevos, ambientes de prueba temporales, cargas de trabajo esporádicas e impredecibles.
Reservadas (Reserved Instances - RI)	Se compra un contrato de 1 o 3 años para una configuración específica. Descuentos significativos.	Cargas de trabajo estables y predecibles que funcionarán 24/7.

- Uso de Instancias Reservadas vs. Bajo Demanda Para elegir una estrategia sirve analizar el uso histórico de la infraestructura de producción. Si una base de datos o un servidor de aplicación central ha estado funcionando consistentemente durante los últimos 6 meses, debe migrar a un modelo de Instancia Reservada (RI) para maximizar el descuento.

- Clases de Almacenamiento según Acceso

  El almacenamiento en la nube cobra según la cantidad de datos almacenados y la frecuencia de acceso. Se debe clasificar la información y moverla a la clase más económica según su vida útil.

Clase de Almacenamiento	Frecuencia de Acceso	Costo por GB	Latencia	Uso Recomendado
Standard (Hot)	Alta	Alto	Baja	Datos de producción activos, contenido web, bases de datos transaccionales.
Nearline Infrequent Access	Baja	Medio	Media	Logs de análisis, backups recientes, datos de Big Data para análisis mensuales.
Coldline/Archival	Muy baja	Muy bajo	Alta	Archivado legal o regulatorio, datos históricos para auditorías, copias de seguridad a largo plazo.

Estrategia: Implementar Políticas de Ciclo de Vida del Almacenamiento que muevan automáticamente los datos:

- Los archivos de registro (logs) pasan de Standard a Nearline después de 30 días.
- Los logs con más de 180 días de antigüedad pasan automáticamente a Coldline/Archival.

Esta automatización asegura que siempre se pague la tarifa más baja para el nivel de acceso requerido.

ACTIVIDAD 5 : EVALUACIÓN DE PROVEEDORES Y SERVICIOS

A continuación, se presenta una comparación de los tres principales proveedores de nube basándose en los criterios solicitados:

1. SEGURIDAD

Proveedor	*Ventajas*	*Desventajas*
AWS	• 143 certificaciones (ISO, PCI DSS, HIPAA) • AWS Shield + WAF avanzados • GuardDuty y Security Hub integrados	• Curva de aprendizaje más alta en IAM • Configuración inicial más compleja
Azure	• Azure Sentinel (SIEM líder) • Integración con Active Directory • Fuerte en GDPR europeo	• 90 certificaciones (menos que AWS) • Menos herramientas especializadas retail
GCP	• BeyondCorp (confianza cero) • Cifrado por defecto • VPC Service Controls únicos	• Solo 70 certificaciones • Ecosistema de seguridad menos maduro • Menos adopción en retail

Mejor opción para Retail360: AWS. Más certificaciones y ecosistema de seguridad completo para retail.

2. HERRAMIENTAS DE IA Y BIG DATA

Proveedor	*Ventajas*	*Desventajas*
AWS	• Amazon Personalize (recomendaciones listas) • Amazon Forecast (predicción demanda) • SageMaker completo para ML	• BigQuery no tan rápido como GCP • QuickSight menos popular que Power BI
Azure	• Power BI (líder en BI) • Synapse Analytics integrado • Cognitive Services completos	• No tiene servicios verticales para retail
GCP	• BigQuery (más rápido del mercado) • Vertex AI intuitivo • TensorFlow nativo	• Sin equivalente a Personalize/Forecast • Requiere desarrollo custom

Mejor opción para Retail360: **AWS**. Sus servicios verticales (Personalize, Forecast) están "listos para usar", lo que es ideal para una mediana empresa con equipo técnico limitado que necesita time-to-market.

3. INTEGRACIÓN EMPRESARIAL

Proveedor	*Ventajas*	*Desventajas*
AWS	• EventBridge (100+ fuentes SaaS) • AWS Marketplace (10,000+ soluciones) • AppSync para GraphQL	• Solo ~50 conectores preconfigurados
Azure	• Logic Apps (400+ conectores) • Integración nativa Microsoft 365 • Service Bus robusto	• Orientado a stack Microsoft
GCP	• Apigee (líder en API Management) • Pub/Sub mensajería global	• Solo ~100 conectores • Sin solución B2B nativa

Mejor opción para Retail360: AWS. Cubre las necesidades de integración (EventBridge, Marketplace) sin forzar la dependencia en el ecosistema de Microsoft.

4. PRECIOS ESTIMADOS PARA PYMES

Escenario: 4 servidores + BD + 10TB almacenamiento + CDN

Proveedor	*Costo Mensual*	*Ventajas de Precio*	*Desventajas de Precio*
AWS	**On-demand:** $1,470 **1 año:** $1,010 **3 años:** $735	• Reserved Instances hasta 60% off • Precios predecibles • Savings Plans flexibles	• Calculadora compleja • Costos ocultos (NAT Gateway)
Azure	**On-demand:** $1,566 **1 año:** $1,070 **3 años:** $850	• Bueno para Windows workloads • Azure Hybrid Benefit	• **Más caro** de los tres • Load Balancer costoso ($125)
GCP	**On-demand:** $1,318 **1 año:** $896 **3 años:** $731	• **10% más barato** inicialmente • Descuentos automáticos (30%) • Calculadora simple	• Transferencia datos cara en LATAM

Mejor opción para Retail360: GCP es el más económico inicialmente, pero **AWS** es competitivo con la aplicación de optimización (Savings Plans) y ofrece un mejor balance costo/capacidad.

5. ESCALABILIDAD

Proveedor	*Ventajas*	*Desventajas*
AWS	• Hasta 5,000 instancias Auto Scaling • Políticas predictive scaling • Historial probado (Amazon Prime Day)	• Latencia 25-40ms a Chile
Azure	• Mayor cobertura global (60+ regiones) • Azure Front Door	• Límite 1,000 instancias • Latencia 30-45ms a Chile
GCP	• **Latencia 5-15ms** (región Santiago) • Cloud Load Balancing global • Red de alto rendimiento	• Límite 1,000 instancias • Menos historial en retail

Mejor opción para Retail360: AWS. Ofrece la capacidad más alta de *Auto Scaling* (5,000 instancias) y tiene un **historial probado** para manejar picos de demanda críticos en plataformas de ventas.

Recomendación final

Retail360 es una mediana empresa con recursos técnicos y financieros limitados, y este factor es determinante en la elección del proveedor *cloud*.

Si bien GCP tiene ventajas tecnológicas significativas que no pueden ignorarse como la velocidad y naturaleza *serverless* de BigQuery, sus capacidades de IA/ML (Vertex AI + Tensor Flow), y una latencia altamente competitiva en Chile, AWS es la mejor opción integral para Retail360, equilibrando seguridad, servicios especializados para *retail*, y una escalabilidad probada que se ajusta a su tamaño.

Argumentos a Favor de AWS

1. Simplicidad: Servicios "Listos para Usar" vs. "Construir Desde Cero"

Retail360, como mediana empresa, posee un equipo técnico limitado que debe priorizar el mantenimiento de las operaciones diarias. No tiene la capacidad para construir y mantener soluciones complejas desde cero donde el *time-to-market* es crítico. El ecosistema de AWS ofrece un catálogo más amplio de servicios "listos para usar" que reducen la carga de desarrollo y la curva de aprendizaje inicial.

2. Escalabilidad Apropiada (No Sobre-ingeniería)

Retail360 necesita escalar, pero no al nivel de gigantes como Amazon.com o Mercado Libre. El *data warehouse* Amazon Redshift maneja hasta petabytes, una capacidad más que suficiente para Retail360 por décadas. Escoger BigQuery, con su capacidad masiva (de TB/PB), representaría una sobre-ingeniería innecesaria en la infraestructura y potencialmente un mayor costo operacional.

3. Seguridad y Cumplimiento Regulatorio Crítico

Retail360 gestiona datos sensibles, incluyendo facturación electrónica (requiere almacenamiento de documentos tributarios por años según la ley chilena), procesamiento de pagos con tarjeta (requiere PCI DSS obligatorio), y protección de datos personales y financieros.

- Para una mediana empresa, pasar una auditoría de seguridad es COSTOSO (consultoría + tiempo).
- AWS, con sus 143 certificaciones, facilita la aprobación de auditorías y reduce la carga de cumplimiento a través de un modelo de responsabilidad compartida.
- El riesgo de incumplimiento legal y financiero es demasiado grande para tomarlo a la ligera en esta etapa.

4. Ecosistema Maduro y Específico para Retail

Los 15+ años de experiencia de AWS en el sector *retail* se traducen en un ecosistema robusto y maduro. Esto incluye integraciones pre-construidas a través del AWS Marketplace con pasarelas de pago, plataformas e-commerce, CRM, y ERPs comunes, amortizando el costo de integración y evitando que Retail360 tenga que construir estas conexiones críticas desde cero.

AWS ofrece el mejor balance entre capacidad, simplicidad operacional, cumplimiento de normativas, y costo total de propiedad para una mediana empresa con recursos acotados como Retail360.

ACTIVIDAD 6: Plan de migración

Este plan detalla la estrategia de migración a AWS para Retail360, considerando las particularidades del mercado local, compliance con normativas chilenas (SII) y optimización de costos en dólares.

1. Plan de Migración en Fases

Fase 1: Análisis y Preparación

Técnico: Se realizará una auditoría completa de la infraestructura actual y se diseñará la arquitectura en AWS usando la región sa-east-1 (São Paulo, Brasil) por su proximidad geográfica y baja latencia desde Chile (30-50ms). Se definirá cómo se organizan servidores, bases de datos y redes usando servicios como EC2, RDS, VPC y subredes. Se establecerán métricas para medir el éxito como velocidad, costos en dólares vs peso chileno, y disponibilidad.
Humano: Se formará el equipo de migración y se capacitará al personal técnico en conceptos básicos de AWS, considerando capacitaciones en español cuando sea posible. Se comunicará el proyecto a toda la organización explicando beneficios y cronograma, siendo transparentes sobre el impacto temporal durante la migración.

Fase 2: Prueba Piloto

Técnico: Se migrará la plataforma de marketing digital como prueba inicial, validando la arquitectura AWS y herramientas de despliegue automático (AWS CodePipeline, CodeDeploy) sin arriesgar sistemas críticos. Se medirá el rendimiento y se identificarán problemas potenciales.
Humano: El equipo ganará experiencia práctica y se documentarán lecciones aprendidas para ajustar el plan antes de migrar sistemas importantes.

Fase 3: Migración de Backend

Técnico: Se migrarán las bases de datos del CRM, inventario y el sistema de facturación electrónica (que debe cumplir con normativas del SII) a Amazon RDS o Aurora usando AWS Database Migration Service. Ambos sistemas funcionarán en paralelo con replicación continua hasta verificar que todo funciona correctamente. Las bases de datos se configurarán en Multi-AZ dentro de sa-east-1 para alta disponibilidad automática.
Humano: Se capacitará al equipo en administración de bases de datos en la nube, creando documentación y definiendo responsabilidades claras.

Fase 4: Migración de la Plataforma Web

Técnico: Se migrará el sistema de pedidos usando la estrategia Blue/Green: el sistema antiguo y nuevo funcionarán juntos hasta que las pruebas confirmen que el nuevo funciona perfectamente. Se realizarán pruebas de carga intensivas simulando muchos usuarios simultáneos, con plan de emergencia para revertir si es necesario.
Humano: Se capacitará a soporte y marketing sobre cambios, preparando comunicación para clientes. El equipo técnico estará disponible 24/7 durante el cambio.

Fase 5: Optimización

Técnico: Se optimizarán recursos usando AWS Instance Scheduler para apagar servidores de desarrollo cuando no se usen (considerando horario laboral chileno) y comprando Reserved Instances para cargas constantes (ahorro 30-70%). Esto es especialmente importante para una mediana empresa chilena que paga en dólares, por lo que el control de costos es crítico. Se configurarán alertas con CloudWatch, monitoreo permanente y automatización con Lambda para tareas repetitivas.
Humano: Se establecerá capacitación continua y cultura de control de costos (FinOps), con reuniones mensuales para revisar gastos y mejoras.

2. Estrategia de Respaldo y Recuperación ante Desastres

Respaldos Automáticos

Todas las bases de datos se respaldan diariamente usando AWS Backup guardando las últimas 30 copias, con capacidad de recuperar datos de cualquier momento de los últimos 30 días mediante Point-in-Time Recovery. Los datos de facturación electrónica (DTE, boletas, facturas) se archivarán por 7 años en Amazon S3 Glacier cumpliendo con las exigencias del SII. Se realizan pruebas trimestrales de restauración para verificar que funcionan.

Recuperación ante Desastres

Se implementará una estrategia de dos regiones AWS: la región principal será sa-east-1 (São Paulo, Brasil) por su proximidad a Chile operando normalmente, y una región de respaldo en us-east-1 (Virginia, EE.UU.) con versión reducida funcionando continuamente, garantizando distancia geográfica adecuada para disaster recovery. Los datos se replicarán automáticamente cada pocos minutos usando Aurora Global Database y S3 Cross-Region Replication. Si la región principal falla, Amazon Route 53 con health checks detectará el problema y redirigirá automáticamente todo el tráfico a la región de respaldo, que escalará rápidamente su capacidad. Tiempo de recuperación: 5-10 minutos. Objetivos: máximo 15-30 minutos de pérdida de datos y recuperación completa en 1-2 horas.

3. Continuidad Operativa ante Fallos

Fallas de Conectividad

Oficinas sin internet: Se contratarán dos proveedores de internet diferentes (ej: Movistar y VTR/Claro) con failover automático para redundancia. La conexión principal será AWS Direct Connect desde el punto de presencia en Santiago conectando a sa-east-1 (línea dedicada de baja latencia), y la secundaria VPN Site-to-Site sobre internet público. Las tiendas físicas tendrán servidores locales con copia del inventario actualizada cada 5 minutos, permitiendo vender durante cortes de internet (situación común en regiones) y sincronizando automáticamente al recuperar conexión.

Clientes sin acceso: Se usará Amazon CloudFront con edge locations en Santiago y otras ciudades de Latinoamérica para distribuir el sitio desde ubicaciones cercanas a los clientes. La plataforma funcionará como PWA permitiendo a clientes ver productos y agregarlos al carrito sin conexión, sincronizando automáticamente cuando la recuperen.

Caídas de Servicios Cloud

Falla de un centro de datos: La plataforma funcionará simultáneamente en tres Availability Zones diferentes. Un Application Load Balancer verificará cada 10 segundos qué servidores funcionan y solo enviará tráfico a los saludables. Recuperación: 1-3 minutos, casi invisible para usuarios.

Falla regional completa: Route 53 detectará que la región principal no responde mediante health checks y redirigirá automáticamente a la región de respaldo, que escalará su capacidad usando Auto Scaling. Tiempo total: 5-10 minutos.

Falla de un servicio específico: Se implementará degradación controlada. Por ejemplo, si fallan las recomendaciones personalizadas, se mostrarán productos populares genéricos. Los clientes podrán seguir comprando normalmente. Principio: nunca bloquear una venta por funciones secundarias.

Monitoreo y Respuesta

Se implementarán canarios de CloudWatch Synthetics que simulan compras cada 5 minutos desde múltiples ubicaciones incluyendo Chile y Sudamérica. Si fallan, alertan inmediatamente al ingeniero de guardia mediante SNS. Objetivo: detectar problemas en menos de 2 minutos y resolverlos en menos de 30 minutos. Habrá cobertura en horario laboral chileno con guardia on-call para emergencias nocturnas, considerando el tamaño de mediana empresa.

Este plan garantiza una migración segura en 5 fases balanceando aspectos técnicos y humanos, con validación en cada etapa. La estrategia de protección incluye respaldos automáticos diarios, replicación geográfica y recuperación en menos de 2 horas ante desastres mayores. El plan de continuidad aborda fallas de conectividad (redundancia, caché local, modo offline) y caídas de servicio (múltiples centros de datos, región de respaldo, degradación controlada), permitiendo operar incluso bajo condiciones adversas y protegiendo ventas y experiencia del cliente.