TECLAB

INSTITUTO TÉCNICO SUPERIOR

ACTIVIDAD PRÁCTICA INTEGRADORA · MÓDULO 1

Plan de migración a la nube para Tech Consulting

Planteamiento de la problemática de negocio, objetivos de la migración y ventajas e impacto de adoptar una arquitectura de datos y servicios en Amazon Web Services.

ASIGNATURA	Seguridad en la Nube y Protección de Datos
CARRERA	Tecnicatura Superior en Seguridad Informática
ACTIVIDAD	Actividad 1 – Conceptos generales y arquitectura de nube
ESTUDIANTE	Juan Manuel Silva
LUGAR Y FECHA	Las Breñas, Chaco, Argentina · Octubre de 2026

Índice

Introducción 3

1. Problemática del caso expuesto 4

1.1 Contexto de la organización 4

1.2 Diagnóstico de la situación actual 4

1.3 Impacto sobre la tríada CIA 5

1.4 Síntesis del problema 5

2. Objetivos de la migración 6

2.1 Objetivo general 6

2.2 Objetivos específicos 6

2.3 Elección del proveedor y del modelo de nube 7

2.4 Arquitectura objetivo propuesta 9

2.5 Estrategia de migración por fases 10

2.6 Seguridad de la arquitectura 10

3. Ventajas e impacto en el negocio 13

3.1 Ventajas del Cloud Computing aplicadas al caso 13

3.2 Impacto financiero: de CapEx a OpEx 13

3.3 Alineación con el marco de buena arquitectura 14

3.4 Impacto por área e indicadores de éxito 14

4. Conclusiones 16

5. Referencias bibliográficas 17

Introducción

La empresa **Tech Consulting** contrata un perfil de *Cloud Architect* para diseñar su primera arquitectura de datos y servicios en la nube. El presente trabajo plantea la problemática de negocio que motiva esa decisión, define los objetivos de la migración y analiza las ventajas y el impacto que la adopción de Cloud Computing tendría sobre la organización.

Siguiendo la definición de referencia del NIST, el Cloud Computing es un modelo que permite el acceso ubicuo y bajo demanda, a través de la red, a un conjunto compartido de recursos de cómputo configurables —redes, servidores, almacenamiento, aplicaciones y servicios— que pueden aprovisionarse y liberarse rápidamente con un esfuerzo mínimo de gestión (Mell y Grance, 2011). Este modelo, que se apoya en la arquitectura cliente-servidor, permite a las empresas usar recursos de computación con garantías de seguridad, mantenimiento y fácil acceso, bajo un esquema de pago por consumo.

Para el desarrollo se integran los contenidos del Módulo 1: tipos de nube (pública, privada e híbrida), proveedores (AWS, Azure y GCP), modelos de servicio IaaS, PaaS y SaaS, el marco de buena arquitectura (*Well-Architected Framework*), la tríada CIA, el modelo de responsabilidad compartida, el control de acceso basado en roles (RBAC), la autenticación multifactor (MFA) y el modelado de amenazas con su matriz de riesgo.

> **ALCANCE DEL TRABAJO**
>
> De acuerdo con la consigna, el plan es **conceptual**: no se ejecuta la migración ni se incurre en costos. Los servicios de AWS se mencionan como referencia de diseño, y los indicadores propuestos son metas orientativas que deberían validarse en una etapa de evaluación detallada.

1 Problemática del caso expuesto

1.1 Contexto de la organización

Tech Consulting ofrece productos digitales cuya demanda crece de manera sostenida. Sin embargo, su ecosistema de datos se formó de manera orgánica, sin una estrategia común: cada área resolvió sus necesidades con las herramientas que tenía a mano. El resultado es una organización que **genera mucha información pero no logra aprovecharla** ni protegerla de forma consistente, y una infraestructura que no acompaña el ritmo del negocio.

1.2 Diagnóstico de la situación actual

A partir del escenario planteado se identifican cinco problemas concretos. La tabla resume cada uno, su consecuencia para el negocio y el riesgo de seguridad asociado.

Tabla 1. Diagnóstico de la situación actual (*as-is*)

Hallazgo	Descripción	Consecuencia para el negocio	Riesgo de seguridad
P1. Excel como fuente de datos	Muchas personas mantienen sus propias planillas y cada una aplica criterios propios para construir métricas.	No existe una "única versión de la verdad": un mismo indicador arroja valores distintos según quién lo calcule. Decisiones lentas y discutibles.	Datos sensibles en equipos personales, sin control de acceso, cifrado ni respaldo. Fórmulas alterables sin trazabilidad.
P2. Tres sistemas transaccionales en SQL Server	Las bases de datos operativas residen en infraestructura propia (*on-premise*), aisladas entre sí.	Silos de información; cruzar datos entre sistemas exige trabajo manual. Mantenimiento, licencias y hardware a cargo de la empresa.	Respaldo y recuperación ante desastres dependientes de un único sitio; parches y hardening manuales.
P3. Microservicios sin captura de datos	Varios microservicios generan eventos en tiempo real que hoy se pierden.	Se desaprovecha información valiosa sobre el comportamiento de los usuarios y el uso de los productos. No hay analítica en tiempo real.	Sin eventos almacenados no hay registros para auditoría ni para detectar comportamientos anómalos.
P4. Información fuera de todo sistema	Listados de tiendas y categorías que enriquecen los datos crudos no están en ningún sistema.	Los datos raw no pueden enriquecerse ni clasificarse; reportes incompletos e inconsistentes.	Sin dueño, versionado ni controles de integridad sobre datos maestros.
P5. Falta de escalabilidad	Se necesita escalar procesos y cómputo para atender una demanda creciente de los productos digitales.	Infraestructura fija: o se sobredimensiona (capital ocioso) o se satura (caídas, lentitud, pérdida de clientes).	Picos de demanda que comprometen la disponibilidad del servicio.

Fuente: elaboración propia con base en el escenario de la actividad.

Figura 1. Ecosistema de datos actual: fuentes aisladas y sin integración



Fuente: elaboración propia.

1.3 Impacto sobre la tríada CIA

Desde la perspectiva de la ciberseguridad, la situación actual compromete los tres pilares de la tríada CIA: la **confidencialidad**, porque la información sólo debería estar disponible para personas autorizadas; la **integridad**, porque los datos deben mantenerse correctos y no ser modificados de forma accidental o maliciosa; y la **disponibilidad**, porque la información necesaria para operar debe estar accesible para los usuarios autorizados sin interrupciones (Mendiola, 2021).

Tabla 2. Pilares de la tríada CIA afectados por cada hallazgo

Pilar	Cómo se ve comprometido hoy	Hallazgos
Confidencialidad	Archivos con datos del negocio que circulan por correo, pendrives y equipos personales; no hay cifrado, gestión de identidades ni registro de quién accede a qué.	P1, P2, P4
Integridad	Cálculos heterogéneos, copias divergentes de un mismo dato y datos maestros sin control de cambios. No es posible asegurar que un número sea el correcto.	P1, P3, P4
Disponibilidad	Dependencia de un único centro de datos propio, respaldos no centralizados y capacidad fija frente a picos de demanda.	P2, P5

Fuente: elaboración propia con base en Mendiola (2021).

1.4 Síntesis del problema

> **PLANTEAMIENTO DE LA PROBLEMÁTICA DE NEGOCIO**
>
> Tech Consulting no cuenta con una **plataforma de datos centralizada, gobernada y segura** ni con una **infraestructura elástica**. Sus datos están fragmentados en planillas personales, bases aisladas, eventos que se pierden e información que no está registrada en ningún sistema. Esto le impide medir su negocio con criterios únicos, tomar decisiones basadas en datos confiables, proteger adecuadamente su información y escalar al ritmo de la demanda de sus productos digitales.

Las causas raíz pueden agruparse en tres ejes: **(a)** ausencia de gobierno de datos —no hay dueños, definiciones ni catálogo—; **(b)** infraestructura rígida basada en inversión de capital, y **(c)** seguridad no integrada desde el diseño, sin gestión centralizada de identidades, cifrado ni trazabilidad.

2 Objetivos de la migración

2.1 Objetivo general

> Diseñar e implementar de forma progresiva una **plataforma de datos y servicios en la nube pública de AWS** que centralice, gobierne y proteja la información de Tech Consulting, garantizando la tríada CIA y una capacidad de cómputo elástica que acompañe el crecimiento de sus productos digitales.

2.2 Objetivos específicos

Cada objetivo responde a un hallazgo del diagnóstico e incluye un indicador que permitirá evaluar su cumplimiento.

O1

Establecer una única fuente de verdad

Reemplazar las planillas Excel como fuente de datos por un *data lake* centralizado con un catálogo de métricas oficial: cada KPI tiene una única definición, un responsable y un origen trazable.

Responde a P1 · Indicador: porcentaje de KPIs corporativos calculados desde la plataforma oficial (meta: 100 %).

O2

Migrar los tres sistemas transaccionales

Trasladar las bases SQL Server a un servicio gestionado con alta disponibilidad, sin pérdida de datos y con el mínimo tiempo de inactividad posible, mediante replicación continua.

Responde a P2 · Indicador: registros validados entre origen y destino (meta: 100 %); ventana de corte acordada con el negocio.

O3

Capturar los datos en tiempo real

Incorporar un canal de *streaming* que reciba los eventos de los microservicios y los almacene para analítica, auditoría y detección de anomalías.

Responde a P3 · Indicador: porcentaje de microservicios integrados; latencia de ingesta de los eventos (meta orientativa: menor a 1 minuto).

O4 **Digitalizar y gobernar los datos maestros**

Registrar tiendas, categorías y demás datos de referencia en tablas maestras con dueño asignado, versionado y validaciones, para enriquecer los datos crudos.

Responde a P4 · Indicador: porcentaje de datos de referencia con responsable y control de cambios.

O5 **Garantizar escalabilidad elástica**

Ejecutar los procesos y servicios sobre cómputo que escale automáticamente según la demanda, evitando tanto la saturación como la capacidad ociosa.

Responde a P5 · Indicador: disponibilidad del servicio durante picos de demanda; tiempo de respuesta percibido por los usuarios.

O6 **Seguridad y cumplimiento desde el diseño**

Aplicar gestión de identidades con RBAC y mínimo privilegio, MFA obligatorio, cifrado en reposo y en tránsito, y registro de auditoría de todas las acciones.

Transversal · Indicador: usuarios con MFA (meta: 100 %); uso diario de la cuenta raíz (meta: 0); recursos cifrados (meta: 100 %).

O7 **Asegurar la continuidad del negocio**

Definir objetivos de punto y de tiempo de recuperación (RPO/RTO) e implementar respaldos automáticos y redundancia entre zonas de disponibilidad.

Transversal · Indicador: pruebas de restauración exitosas por período; cumplimiento de RPO/RTO acordados.

2.3 Elección del proveedor y del modelo de nube

El módulo presenta a los tres proveedores líderes del mercado: **AWS**, destacado por su experiencia y servicio al cliente; **Microsoft Azure**, por la rapidez y navegabilidad de su portal; y **Google Cloud Platform**, por su seguridad. Los tres se ubican en el cuadrante de líderes y la elección debe responder a las necesidades computacionales de la organización.

Para Tech Consulting se propone **Amazon Web Services (AWS)** por los siguientes motivos:

- **Catálogo completo para el caso:** ofrece servicios gestionados específicos para cada necesidad —migración de bases (AWS DMS), SQL Server gestionado (Amazon RDS), streaming (Amazon Kinesis), data lake (Amazon S3, AWS Glue, AWS Lake Formation) y analítica (Amazon Redshift, Amazon QuickSight)—.
- **Compatibilidad con SQL Server:** Amazon RDS for SQL Server permite trasladar los tres sistemas sin reescribirlos.
- **Marco de buena arquitectura documentado:** los seis pilares del AWS Well-Architected Framework guían el diseño y su revisión.
- **Madurez y ecosistema:** amplia documentación, capa gratuita para pruebas de concepto y comunidad, lo que reduce la curva de aprendizaje del equipo.

En cuanto al **tipo de nube**, el destino es una **nube pública**, en la que el cliente no necesita mantener infraestructura propia. Durante la transición, la empresa operará temporalmente en un esquema **híbrido**: los sistemas on-premise y la nube convivirán conectados mediante una VPN cifrada hasta completar la migración.

Tabla 3. Modelos de servicio utilizados en la solución

Modelo	Servicios de AWS en la propuesta	Qué gestiona Tech Consulting
IaaS	Amazon S3 (almacenamiento), Amazon VPC (red), Site-to-Site VPN	Configuración de red, políticas de acceso a buckets, clasificación y cifrado de los datos.
PaaS	Amazon RDS for SQL Server, AWS Glue, Amazon Kinesis, Amazon ECS sobre AWS Fargate, Amazon Redshift Serverless, AWS DMS	Sus aplicaciones, modelos de datos, usuarios y permisos. AWS gestiona sistema operativo, parches del motor y backups automáticos.
SaaS	Amazon QuickSight (tableros e informes)	Usuarios, permisos sobre tableros y las definiciones de las métricas.

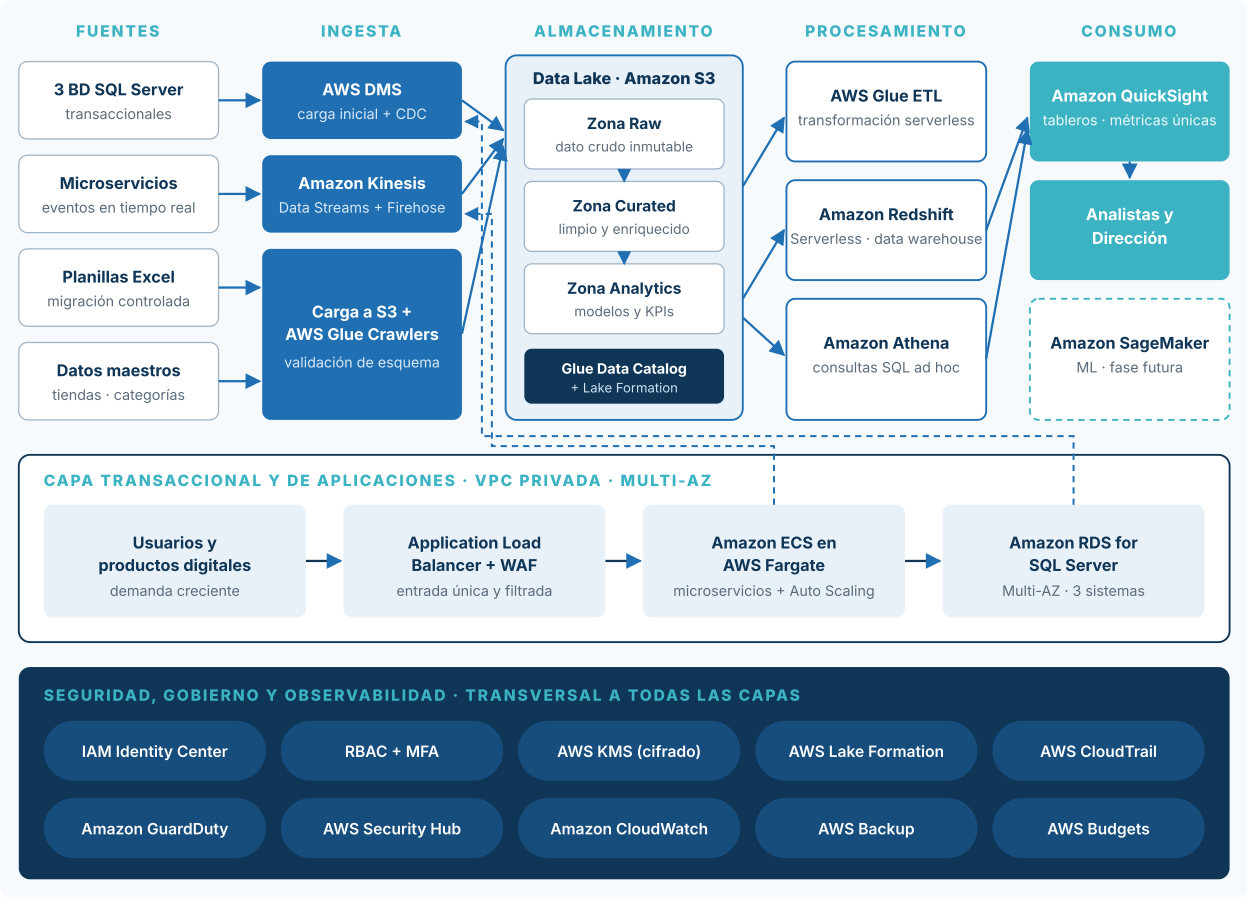
Fuente: elaboración propia con base en “IaaS frente a PaaS frente a SaaS” (IBM, 2018).

Se priorizan servicios **PaaS gestionados** porque permiten que la organización se concentre en sus datos y productos en lugar de administrar servidores, y porque transfieren al proveedor gran parte de las tareas operativas y de seguridad de la infraestructura.

2.4 Arquitectura objetivo propuesta

La arquitectura se organiza en capas con responsabilidades separadas: **fuentes**, **ingesta**, **almacenamiento** en un data lake por zonas, **procesamiento y analítica**, y **consumo**. A ellas se suman una capa transaccional y de aplicaciones escalable y una capa transversal de seguridad, gobierno y observabilidad.

Figura 2. Arquitectura objetivo (*to-be*) en AWS



Fuente: elaboración propia. Diagrama conceptual; los servicios son de referencia y no implican implementación. Las líneas punteadas indican la replicación continua (CDC) desde RDS y los eventos de los microservicios hacia la capa de ingesta.

Tabla 4. Cómo responde la arquitectura a cada hallazgo

Hallazgo	Componente propuesto	Resultado esperado
P1. Excel	Data lake en S3 + catálogo de datos + Amazon QuickSight con métricas oficiales	Una única definición por KPI; las planillas dejan de ser fuente y pasan a ser, a lo sumo, una vista de consumo.
P2. SQL Server	Amazon RDS for SQL Server Multi-AZ + AWS DMS con replicación continua (CDC)	Bases gestionadas, con backups automáticos y réplica en otra zona; datos replicados al lago para cruzarlos.

Hallazgo	Componente propuesto	Resultado esperado
P3. Tiempo real	Amazon Kinesis Data Streams + Data Firehose hacia la zona Raw	Los eventos dejan de perderse y quedan disponibles para analítica y auditoría.
P4. Datos sin sistema	Tablas maestras en la zona Curated, con dueño, versión y validaciones (Glue)	Datos de referencia confiables que enriquecen los datos crudos.
P5. Escalabilidad	Amazon ECS sobre AWS Fargate con Auto Scaling, servicios serverless (Glue, Redshift Serverless, Athena)	La capacidad crece y decrece con la demanda; se paga sólo por lo consumido.

Fuente: elaboración propia.

2.5 Estrategia de migración por fases

Para reducir riesgos, la migración se plantea de forma incremental. AWS propone distintas estrategias según cada carga de trabajo (AWS, s. f.-c): para los tres sistemas transaccionales se recomienda **redefinir la plataforma** (*replatform*), es decir, trasladarlos a RDS sin modificar su lógica; para los datos analíticos y en tiempo real, en cambio, se plantea **rediseñar** (*refactor*) hacia una arquitectura de data lake. Las planillas Excel se **retiran** progresivamente como fuente de datos.

Figura 3. Hoja de ruta de la migración



Fuente: elaboración propia.

La Fase 1 se ubica deliberadamente antes de mover cualquier dato: la seguridad no se agrega al final, sino que es la base sobre la que se construye la plataforma.

2.6 Seguridad de la arquitectura

Modelo de responsabilidad compartida

La seguridad en la nube es una responsabilidad compartida entre el proveedor y el cliente: AWS es responsable de la seguridad *de* la nube (centros de datos, hardware, red física y virtualización), mientras

que Tech Consulting es responsable de la seguridad *en* la nube (AWS, s. f.-b). La información, las cuentas y las identidades **siempre** quedan bajo responsabilidad del cliente, cualquiera sea el modelo de servicio.

Tabla 5. Distribución de responsabilidades en la solución propuesta

Componente	Responsabilidad de AWS	Responsabilidad de Tech Consulting
Amazon S3 (IaaS)	Durabilidad, hardware, red física y disponibilidad del servicio.	Políticas de bucket, bloqueo de acceso público, cifrado, clasificación de datos.
Amazon RDS (PaaS)	Sistema operativo, parches del motor, backups automáticos y conmutación Multi-AZ.	Usuarios y permisos de la base, cifrado habilitado, grupos de seguridad, calidad del dato.
ECS en Fargate (PaaS)	Servidores subyacentes y aislamiento de la infraestructura de cómputo.	Imágenes de contenedor seguras, secretos, roles de tarea, código de los microservicios.
Amazon QuickSight (SaaS)	Aplicación, plataforma e infraestructura completas.	Quién ve cada tablero, seguridad a nivel de fila, definiciones de métricas.

Fuente: elaboración propia con base en AWS (s. f.-b).

Gestión de identidades, RBAC y MFA

- **Cuenta raíz protegida:** se usa sólo para tareas excepcionales, con MFA físico; la operación diaria se realiza con usuarios y roles de IAM.
- **RBAC con mínimo privilegio:** se definen grupos por función —por ejemplo, *Administradores de plataforma*, *Ingenieros de datos*, *Analistas* (sólo lectura sobre la zona Analytics) y *Auditoría* (sólo lectura de registros)—. Las aplicaciones usan roles de IAM, nunca credenciales fijas.
- **MFA obligatorio** para todos los usuarios humanos, combinando el factor de conocimiento (contraseña) con un factor de posesión (aplicación autenticadora o llave física).
- **Revisiones periódicas de accesos** (*provisioning* y *de-provisioning*) para mitigar el riesgo de asignaciones temporales olvidadas, una desventaja conocida del RBAC.

Protección de los datos

Cifrado en reposo con claves gestionadas en AWS KMS y en tránsito mediante TLS; permisos a nivel de tabla y columna con Lake Formation; registro de toda acción en CloudTrail; detección de amenazas con GuardDuty y verificación continua de configuraciones con Security Hub. Cada control contribuye a un pilar de la tríada: cifrado y RBAC a la *confidencialidad*, versionado y auditoría a la *integridad*, Multi-AZ y backups a la *disponibilidad*.

Modelado de amenazas y matriz de riesgo

Aplicando el modelado de amenazas en sus cuatro pasos —diagramar, identificar amenazas, mitigar y validar— se evalúan los principales riesgos de la migración con la fórmula **Riesgo = Probabilidad × Impacto** y las escalas vistas en el módulo (Barato, 2014). Se considera riesgo **bajo** a un valor menor a 0,06; **medio**, entre 0,06 y 0,17; y **alto**, a partir de 0,18.

Tabla 6. Matriz de riesgos de la migración

#	Amenaza / riesgo	P	I	Riesgo	Estrategia	Tratamiento
R1	Exposición de datos por configuración incorrecta de almacenamiento o permisos	0,5	0,80	0,40 Alto	Mitigar	Bloqueo de acceso público, cifrado por defecto, Lake Formation, Security Hub.
R2	Compromiso de credenciales privilegiadas	0,3	0,80	0,24 Alto	Mitigar	MFA, no usar la cuenta raíz, mínimo privilegio, alertas de GuardDuty.
R3	Resistencia al cambio de los usuarios de Excel	0,7	0,20	0,14 Medio	Mitigar	Patrocinio de la dirección, capacitación y migración gradual de cada métrica.
R4	Pérdida o inconsistencia de datos durante la migración	0,3	0,40	0,12 Medio	Mitigar	Respaldos previos, validación de DMS, ensayos de corte y plan de vuelta atrás.
R5	Gasto descontrolado por recursos sobredimensionados	0,5	0,20	0,10 Medio	Mitigar	Presupuestos y alertas, etiquetado de recursos, revisión mensual de consumo.
R6	Dependencia del proveedor (*vendor lock-in*)	0,5	0,10	0,05 Bajo	Aceptar	Formatos abiertos en el data lake y documentación de la arquitectura.
R7	Indisponibilidad de una zona del proveedor	0,1	0,40	0,04 Bajo	Transferir	Despliegue Multi-AZ y SLA del proveedor; backups en otra región.

Fuente: elaboración propia con base en la matriz de Barato (2014). P = probabilidad; I = impacto.

Los dos riesgos altos (R1 y R2) se relacionan con la configuración y las identidades, es decir, con aspectos que el modelo de responsabilidad compartida deja del lado del cliente. Por eso la hoja de ruta coloca la gestión de identidades y los controles preventivos en la Fase 1. Como el modelado de amenazas es un proceso dinámico, la matriz debe revisarse en cada fase.

3 Ventajas e impacto en el negocio

3.1 Ventajas del Cloud Computing aplicadas al caso

El módulo identifica cinco ventajas principales de la nube para las empresas. A continuación se analiza cómo se concreta cada una en Tech Consulting.

VENTAJA 1

Eficiencia y ahorro

Se deja de comprar y mantener servidores, licencias de hardware e instalaciones. Los procesos de datos se ejecutan bajo demanda y se detienen al terminar, sin capacidad ociosa.

VENTAJA 2

Seguridad de datos

Los datos salen de los equipos personales y pasan a un entorno con cifrado, identidades centralizadas, MFA y auditoría, sobre una infraestructura que cumple estándares internacionales.

VENTAJA 3

Escalabilidad

Los microservicios y procesos escalan automáticamente ante el crecimiento de la demanda de los productos digitales, y se reducen cuando la demanda baja.

VENTAJA 4

Movilidad

Analistas y directivos acceden a tableros e información oficial desde cualquier lugar y dispositivo autorizado, con los mismos controles de acceso.

VENTAJA 5

Recuperación ante desastres

Bases replicadas en varias zonas de disponibilidad, respaldos automáticos y copias en otra región permiten recuperar la operación ante fallas técnicas, cortes de energía o desastres naturales, algo difícil de lograr con un único centro de datos propio.

3.2 Impacto financiero: de CapEx a OpEx

La migración transforma la estructura de costos de TI. Hoy la empresa opera con gastos de capital (**CapEx**): compra de servidores, almacenamiento, infraestructura de centro de datos y personal técnico dedicado a mantenerlos. En la nube, el gasto pasa a ser operativo (**OpEx**), con un modelo de pago por uso.

Aspecto	Situación actual (CapEx)	Situación propuesta (OpEx)
Inversión inicial	Compra anticipada de hardware dimensionado para el pico.	Sin costos iniciales de infraestructura.
Crecimiento	Nuevas compras con plazos de adquisición e instalación.	Se suman recursos sólo cuando se necesitan.

Aspecto	Situación actual (CapEx)	Situación propuesta (OpEx)
Baja demanda	Equipos ociosos ya pagados.	Se deja de pagar por lo que no se usa.
Mantenimiento	Hardware, parches y renovación tecnológica a cargo de la empresa.	Delegado al proveedor en los servicios gestionados.
Previsibilidad	Costos fijos, aunque no se aprovechen.	Costos variables, controlables con presupuestos y alertas.

Fuente: elaboración propia con base en los contenidos del módulo. No se incluyen montos, ya que la consigna excluye la estimación de costos.

Además, el acuerdo de nivel de servicio (SLA) del proveedor establece indicadores medibles de disponibilidad, lo que permite a Tech Consulting, a su vez, comprometer niveles de servicio más exigentes con sus propios clientes.

3.3 Alineación con el marco de buena arquitectura

El AWS Well-Architected Framework describe conceptos, principios de diseño y prácticas recomendadas para diseñar y ejecutar cargas de trabajo en la nube (AWS, s. f.-a). La propuesta se alinea con sus pilares de la siguiente manera:

Pilar	Aplicación en la propuesta
Excelencia operativa	Infraestructura definida como código, despliegues automatizados, monitoreo con CloudWatch y procedimientos documentados.
Seguridad	RBAC, MFA, cifrado, Lake Formation, CloudTrail, GuardDuty y Security Hub. Seguridad incorporada desde la Fase 1.
Fiabilidad	RDS Multi-AZ, servicios distribuidos, backups automáticos, RPO/RTO definidos y pruebas de restauración.
Eficacia del rendimiento	Servicios serverless y Auto Scaling que ajustan el tipo y la cantidad de recursos a la carga real.
Optimización de costos	Pago por uso, apagado automático de procesos, etiquetado de recursos y control con AWS Budgets.
Sostenibilidad	Uso de servicios gestionados y elásticos que evitan capacidad ociosa y reducen el consumo energético asociado.

Fuente: elaboración propia con base en AWS (s. f.-a).

3.4 Impacto por área e indicadores de éxito

Área	Impacto esperado
Dirección	Decisiones basadas en indicadores únicos y confiables, disponibles en tableros actualizados; visibilidad del negocio en tiempo cercano al real.

Área	Impacto esperado
Análisis de datos	Menos tiempo en recopilar y conciliar planillas, más tiempo en analizar. Posibilidad futura de modelos predictivos.
Tecnología	Menor carga operativa sobre infraestructura; foco en desarrollar productos. Entornos de prueba disponibles en minutos.
Seguridad y cumplimiento	Control centralizado de accesos, trazabilidad completa y mejor postura para cumplir con la Ley 25.326 de Protección de Datos Personales.
Clientes	Productos digitales más estables y rápidos aun en picos de demanda.

Indicadores propuestos para medir el éxito de la migración

100 %
de KPIs corporativos con definición única y origen trazable

100 %
de usuarios humanos con MFA y acceso por rol

0
planillas Excel como fuente oficial de datos al cierre de la Fase 4

< 1 min
de latencia orientativa en la ingesta de eventos en tiempo real

RPO/RTO
acordados con el negocio y verificados con pruebas periódicas

↓ tiempo
de elaboración de reportes respecto de la línea base actual

Fuente: elaboración propia. Valores orientativos a validar en la Fase 0.

4 Conclusiones

El caso de Tech Consulting muestra que el principal problema no es tecnológico sino de **gobierno y estructura de los datos**: la información existe, pero está fragmentada, carece de criterios comunes y no está protegida de manera consistente. A ello se suma una infraestructura rígida que no acompaña el crecimiento de los productos digitales.

La migración a una nube pública como AWS permite atacar ambos frentes. Por un lado, una plataforma de datos centralizada —data lake por zonas, catálogo y métricas únicas— convierte la información dispersa en un activo confiable para la toma de decisiones. Por otro, los servicios gestionados y elásticos aportan escalabilidad, alta disponibilidad y un modelo de costos OpEx alineado con la demanda real.

Desde la seguridad informática, la conclusión más relevante es que **migrar a la nube no traslada automáticamente la responsabilidad de proteger los datos**. El modelo de responsabilidad compartida deja del lado del cliente la información, las identidades y la configuración, que son precisamente los focos de los riesgos más altos identificados en la matriz. Por eso el plan antepone una fase de fundaciones seguras —RBAC con mínimo privilegio, MFA, cifrado y auditoría— a cualquier movimiento de datos, y se apoya en el marco de buena arquitectura para revisar el diseño de forma continua.

Finalmente, un enfoque gradual por fases, con indicadores medibles y una matriz de riesgos viva, permite que la transformación sea controlada: cada etapa entrega valor al negocio y, al mismo tiempo, mejora la confidencialidad, la integridad y la disponibilidad de la información de la organización.

5 Referencias bibliográficas

Amazon Web Services. (s. f.-a). *AWS Well-Architected*. https://aws.amazon.com/es/architecture/well-architected/

Amazon Web Services. (s. f.-b). *Modelo de responsabilidad compartida*. https://aws.amazon.com/es/compliance/shared-responsibility-model/

Amazon Web Services. (s. f.-c). *Migration strategies*. AWS Prescriptive Guidance. https://docs.aws.amazon.com/prescriptive-guidance/latest/large-migration-guide/migration-strategies.html

Amazon Web Services. (s. f.-d). *AWS Identity and Access Management: Guía del usuario*. https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/

Autenticación multifactor o MFA. (2021). *Computer Weekly*. https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA

Barato, J. (2014). *Gestión eficaz de los riesgos del proyecto*. http://jose-barato.blogspot.com/2014/04/gestion-eficaz-de-los-riesgos-del.html

Edward, M. (2021). *Ventajas del cloud computing*. Acktib. https://acktib.com/ventajas-del-cloud-computing/

IBM. (2018). *IaaS frente a PaaS frente a SaaS*. https://www.ibm.com/mx-es/cloud/learn/iaas-paas-saas

Ley 25.326 de Protección de los Datos Personales. (2000). Boletín Oficial de la República Argentina.

Mell, P. y Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Mendiola, L. (2021). *Los tres pilares de la ciberseguridad*. Artek. https://artek.edu.mx/noticia_eventos/los-tres-pilares-de-la-ciberseguridad/

Oracle. (s. f.). *¿Qué es el cloud computing?* https://www.oracle.com/ar/cloud/what-is-cloud-computing/

Qué es el modelado de amenazas – Ejemplos. (s. f.). *Ciberseguridad*. https://ciberseguridad.com/herramientas/modelado-amenazas-ejemplos/

Role based access control: ¿cómo funciona el control de acceso basado en roles? (2020). *IONOS Digital Guide*. https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-role-based-access-control-rbac/

TECLAB Instituto Técnico Superior. (s. f.). *Seguridad en la Nube y Protección de Datos: Módulo 1. Conceptos generales y arquitectura de nube* [Material de cátedra].