TECLAB

INSTITUTO TÉCNICO SUPERIOR

PROYECTO INTEGRADOR · ACTIVIDADES 1 A 4

# Plan de migración segura a la nube para Tech Consulting



Arquitectura en AWS, infraestructura y monitoreo, gestión de riesgos, auditoría, DevSecOps, privacidad de datos y cronograma de implementación.

| | |
|---|---|
| ASIGNATURA | Seguridad en la Nube y Protección de Datos |
| CARRERA | Tecnicatura Superior en Seguridad Informática |
| CONTENIDO | Actividades Prácticas Integradoras 1, 2, 3 y 4 |
| ESTUDIANTE | Juan Manuel Silva |
| LUGAR Y FECHA | Las Breñas, Chaco, Argentina · Octubre de 2026 |

# Índice

**Resumen ejecutivo** 3

**Introducción general** 4

**1. Parte 1 · Problemática y plan de migración** 5

1.1 Problemática del caso expuesto 6
1.2 Objetivos de la migración 8
1.3 Ventajas e impacto en el negocio 15
1.4 Síntesis de la Parte 1 18

**2. Parte 2 · Infraestructura, servicios y monitoreo** 19

2.1 Arquitectura y descripción de los servicios de AWS 20
2.2 Funcionalidades del monitoreo de sistemas cloud 26
2.3 Mejores prácticas para la migración a la nube 29
2.4 Síntesis de la Parte 2 32

**3. Parte 3 · Riesgos, auditoría y DevOps** 33

3.1 Riesgos en las arquitecturas cloud 34
3.2 Funcionalidades de la auditoría informática 38
3.3 Beneficios de la integración DevOps + Cloud 41
3.4 Síntesis de la Parte 3 45

**4. Parte 4 · Privacidad, DPO y amenazas** 46

4.1 Definición de políticas de privacidad 47
4.2 Funcionalidades del DPO 52
4.3 Tipos de ataques: insider y outsider 54
4.4 Estructura de billing 57
4.5 Cronograma de implementación 58
4.6 Síntesis de la Parte 4 59

**Conclusión general** 60

**Referencias bibliográficas** 61

# Resumen ejecutivo

Este documento reúne en un único plan las cuatro actividades prácticas de la materia. Su objeto es diseñar la **migración segura a la nube de Tech Consulting**, una empresa de productos digitales cuyos datos están dispersos, cuyos sistemas están aislados y cuya infraestructura no acompaña una demanda creciente.

### El problema

Métricas calculadas en planillas Excel con criterios propios, tres bases SQL Server on-premise sin integración, eventos de microservicios que se pierden, datos de referencia fuera de todo sistema y capacidad fija frente a la demanda.

### La propuesta

Una plataforma en la nube pública de AWS, con un data lake gobernado, bases gestionadas de alta disponibilidad, cómputo elástico y la seguridad integrada desde la primera fase, ejecutada en etapas a lo largo de nueve meses.

**3 × 2**
capas de red por zonas de disponibilidad en una VPC segmentada

**10**
riesgos evaluados con matriz de probabilidad × impacto

**5**
fases de migración, con la seguridad antes que los datos

**8**
etapas de un pipeline DevSecOps con controles automáticos

**14**
cláusulas de una política de privacidad alineada con la Ley 25.326

**9**
meses de cronograma integrado, con auditoría previa al corte

**Síntesis de las cuatro partes**

| Parte | Resultado principal |
|---|---|
| **1 · Problemática y plan** | Diagnóstico de cinco problemas, siete objetivos medibles, elección de AWS y arquitectura objetivo por capas. |
| **2 · Infraestructura y monitoreo** | VPC en tres capas y dos zonas, cómputo elástico, almacenamiento y bases gestionadas, matriz de monitoreo y buenas prácticas. |
| **3 · Riesgos, auditoría y DevOps** | Diez riesgos evaluados (cuatro altos), plan de auditoría de cinco tipos, registros inmutables y pipeline DevSecOps. |
| **4 · Privacidad, DPO y amenazas** | Política de privacidad, rol del DPO, escenarios *insider* y *outsider*, estructura de facturación y cronograma. |

**CONCLUSIÓN CENTRAL**

Los riesgos más altos del proyecto no dependen del proveedor sino de decisiones de Tech Consulting: configuración, identidades, procesos y tratamiento de datos personales. Por eso el plan antepone una fase de fundaciones seguras —identidades con mínimo privilegio, MFA, cifrado, auditoría, política de privacidad y DPO— a cualquier movimiento de datos. **En la nube la seguridad es compartida, pero la responsabilidad sobre los datos nunca se delega.**

# Introducción general

La empresa **Tech Consulting** contrata un perfil de *Cloud Architect* para construir su primera arquitectura de datos y servicios en la nube y diseñar el plan de migración de la organización. El escenario de partida es el siguiente:

- Muchas personas tienen archivos de Excel como fuente de datos, cada una con sus propios criterios para crear métricas.
- Existen tres sistemas transaccionales cuyas bases de datos están en SQL Server.
- Varios microservicios generan datos en tiempo real que no se capturan.
- Mucha información —listados de tiendas, categorías— no está en ningún sistema y es necesaria para enriquecer los datos crudos.
- Se necesita escalar procesos y cómputo para satisfacer la demanda creciente de los productos digitales.

Siguiendo la definición 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 que pueden aprovisionarse y liberarse rápidamente con un esfuerzo mínimo de gestión (Mell y Grance, 2011). Ese modelo ofrece a Tech Consulting elasticidad, pago por uso y servicios gestionados, pero también le exige asumir con claridad su parte de la responsabilidad sobre la seguridad.

El plan se desarrolla en cuatro partes, que corresponden a las cuatro actividades prácticas integradoras de la materia y se construyen una sobre otra: la **Parte 1** plantea la problemática y el plan de migración; la **Parte 2** define la infraestructura, los servicios y el monitoreo; la **Parte 3** analiza riesgos, auditoría y DevOps, y la **Parte 4** aborda la privacidad, el rol del DPO y las amenazas, junto con la facturación y el cronograma.

> **ALCANCE**
>
> La propuesta es **conceptual**: no se ejecuta la migración ni se incurre en costos. Los servicios de AWS se mencionan como referencia de diseño; las direcciones IP, los umbrales de alarma, las probabilidades de la matriz de riesgos y los plazos del cronograma son valores orientativos que deberían validarse en una evaluación detallada. La política de privacidad es un modelo sujeto a revisión legal.

Las tablas y figuras se numeran por parte (por ejemplo, *Tabla 3.4* es la cuarta tabla de la Parte 3), y las referencias bibliográficas de todo el documento se reúnen al final.

PARTE 1

# Problemática y plan de migración

Diagnóstico de la situación actual de Tech Consulting, objetivos de la migración, elección del proveedor y del modelo de nube, arquitectura objetivo en AWS, estrategia por fases y ventajas para el negocio.

1.1 Problemática del caso expuesto
1.2 Objetivos de la migración
1.3 Ventajas e impacto en el negocio
1.4 Síntesis de la Parte 1

Actividad Práctica Integradora 1 · Conceptos generales y arquitectura de nube

# 1.1 Problemática del caso expuesto

## 1.1.1 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.

## 1.1.2 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 1.1. 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 1.1. Ecosistema de datos actual: fuentes aisladas y sin integración**




**Fuente:** elaboración propia.

### 1.1.3 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 1.2. 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).

### 1.1.4 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.

## 1.2 Objetivos de la migración

### 1.2.1 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.

### 1.2.2 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).

**04** **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.

**05** **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.

**06** **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 %).

**07** **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.

### 1.2.3 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 1.3. 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. |

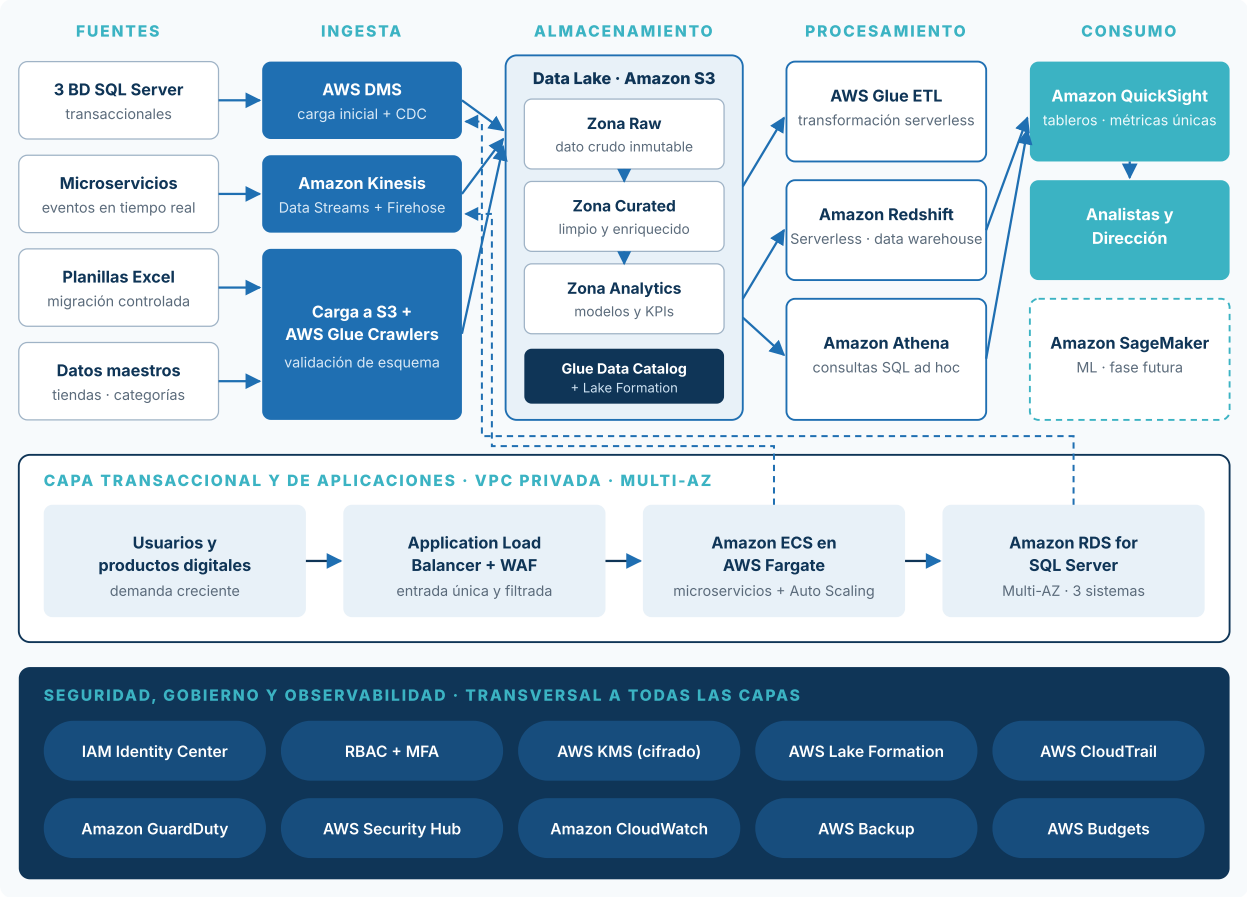
**Fuente:** elaboración propia con base en "IaaS frente a PaaS frente a SaaS" (IBM, 2018).

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.

## 1.2.4 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 1.2. 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 1.4. 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.

## 1.2.5 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.-l): 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 1.3. 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.

## 1.2.6 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.-m). La información, las cuentas y las identidades **siempre** quedan bajo responsabilidad del cliente, cualquiera sea el modelo de servicio.

**Tabla 1.5. 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.-m).

### 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 1.6. 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.

# 1.3 Ventajas e impacto en el negocio

## 1.3.1 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.

## 1.3.2 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.

### 1.3.3 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.-j). 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.-j).

### 1.3.4 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.

## 1.4 Síntesis de la Parte 1

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.

PARTE 2

# Infraestructura, servicios y monitoreo

Arquitectura de red, cómputo, almacenamiento y bases de datos en AWS; funcionalidades del monitoreo cloud y mejores prácticas para ejecutar la migración.

2.1 Arquitectura y descripción de los servicios de AWS
2.2 Funcionalidades del monitoreo de sistemas cloud
2.3 Mejores prácticas para la migración a la nube
2.4 Síntesis de la Parte 2

Actividad Práctica Integradora 2 · Infraestructura y servicios en la nube

# 2.1 Arquitectura y descripción de los servicios de AWS

## 2.1.1 Criterios de diseño

La arquitectura se apoya en la **virtualización**: AWS ejecuta las máquinas virtuales sobre su propio hipervisor (AWS Nitro System), que separa los recursos físicos de los entornos virtuales y permite que muchas instancias compartan el mismo hardware de forma aislada. Sobre esa base se aplicaron cinco criterios:

CRITERIO 1

### Aislamiento por capas

Red privada propia (VPC) dividida en subredes públicas, de aplicación y de datos. Sólo lo estrictamente necesario queda expuesto a Internet.

CRITERIO 2

### Alta disponibilidad

Todos los componentes críticos se replican en dos zonas de disponibilidad (AZ), es decir, en centros de datos físicamente separados.

CRITERIO 3

### Elasticidad

El cómputo crece y decrece automáticamente según la demanda de los productos digitales.

CRITERIO 4

### Servicios gestionados

Se prioriza DBaaS y almacenamiento gestionado para delegar en AWS el mantenimiento de infraestructura, parches y respaldos.

CRITERIO 5

### Seguridad y observabilidad desde el diseño

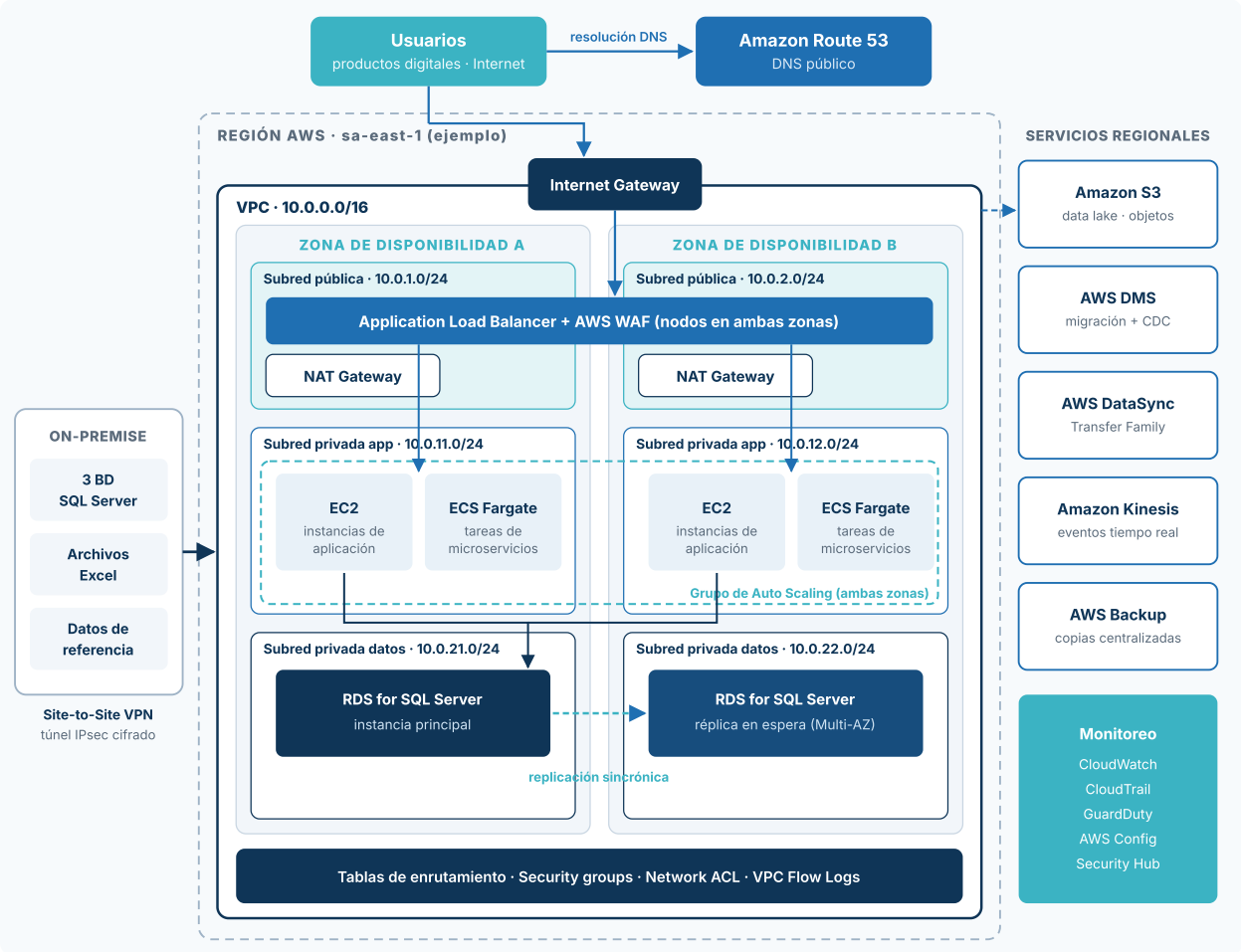
Mínimo privilegio en red e identidades, cifrado por defecto y monitoreo de todas las capas desde el primer día, no como un agregado posterior.

Como región se toma de ejemplo **América del Sur (São Paulo, `sa-east-1`)**, por ser la más cercana a la operación de la empresa y, por lo tanto, la de menor latencia para los usuarios de la región.

## 2.1.2 Vista general de la arquitectura

La Figura 2.1 muestra la arquitectura de infraestructura propuesta. Los usuarios llegan por Internet resolviendo el dominio con Amazon Route 53; el tráfico entra por el Internet Gateway hacia un balanceador ubicado en las subredes públicas, que lo distribuye entre las instancias de aplicación de las subredes privadas. Las bases de datos residen en una tercera capa, sin acceso desde Internet. El centro de datos actual se conecta a la VPC mediante una VPN cifrada durante la etapa híbrida de la migración.

**Figura 2.1. Arquitectura de infraestructura propuesta en AWS**




**Fuente:** elaboración propia. Diagrama conceptual; direcciones IP y región a modo de ejemplo. La línea punteada hacia Amazon S3 representa el acceso privado mediante un endpoint de VPC.

## 2.1.3 Servicios de red

### Amazon VPC y subredes

Una VPC es una nube privada ubicada dentro de una nube pública: aporta los beneficios de una red virtualizada propia —seguridad, control de los datos, rendimiento y flexibilidad— mientras se usan los recursos del proveedor. Para Tech Consulting se define una VPC con el bloque `10.0.0.0/16`, dividida en seis subredes: tres capas replicadas en dos zonas de disponibilidad.

**Tabla 2.1. Plan de direccionamiento de la VPC**

| Subred | Zona A | Zona B | Acceso a Internet | Recursos que aloja |
|---|---|---|---|---|
| **Pública** | `10.0.1.0/24` | `10.0.2.0/24` | Directo (IGW) | Application Load Balancer y NAT Gateway. Ningún servidor de aplicación. |
| **Privada de aplicación** | `10.0.11.0/24` | `10.0.12.0/24` | Sólo salida (NAT) | Instancias EC2 y tareas de ECS Fargate de los microservicios. |
| **Privada de datos** | `10.0.21.0/24` | `10.0.22.0/24` | Ninguno | Amazon RDS for SQL Server (principal y réplica en espera). |

**Fuente:** elaboración propia.

### Enrutamiento, Internet Gateway y NAT Gateway

El *routing* consiste en mover paquetes de una red a otra. En la VPC, ese papel lo cumple el router virtual de AWS, que decide el destino del tráfico según las **tablas de enrutamiento**: conjuntos de reglas (rutas) que indican hacia dónde se dirige el tráfico desde una subred o puerta de enlace (AWS, s. f.-e). Cada ruta se compone de una red de destino con su máscara y del siguiente salto (*target*).

- **Internet Gateway (IGW):** es la puerta de enlace que comunica la VPC con Internet. Se ubica en la frontera de la red y sólo las subredes públicas tienen una ruta hacia él.
- **NAT Gateway:** traduce las direcciones privadas de las instancias a una IP pública para que puedan salir a Internet —por ejemplo, para descargar actualizaciones—, pero **sin que los servicios externos puedan iniciar una conexión** hacia ellas (AWS, s. f.-e). Se usa la conectividad pública, con un NAT Gateway por zona para no depender de una sola. Funciona como una NAT por sobrecarga: muchas IP privadas comparten una IP pública.
- **Virtual Private Gateway + Site-to-Site VPN:** conecta el centro de datos actual con la VPC mediante un túnel IPsec cifrado durante la etapa híbrida.

**Tabla 2.2. Tablas de enrutamiento propuestas**

| Tabla | Destino | Siguiente salto (*target*) | Propósito |
|---|---|---|---|
| **rt-publica** | `10.0.0.0/16` | local | Comunicación interna de la VPC. |
| | `0.0.0.0/0` | Internet Gateway | Entrada y salida a Internet. |
| **rt-app-a / rt-app-b** | `10.0.0.0/16` | local | Comunicación interna de la VPC. |
| | `0.0.0.0/0` | NAT Gateway de su zona | Sólo salida a Internet. |
| | Red on-premise | Virtual Private Gateway | Acceso al centro de datos por VPN. |

| Tabla | Destino | Siguiente salto (*target*) | Propósito |
|---|---|---|---|
| **rt-datos** | `10.0.0.0/16` | local | Sólo tráfico interno. |
| | Red on-premise | Virtual Private Gateway | Replicación con DMS durante la migración. |

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

### Grupos de seguridad (security groups)

Un grupo de seguridad funciona como un *firewall* virtual que filtra el tráfico hacia y desde los recursos; contiene una lista de reglas y una lista de miembros, y toda máquina virtual debe tener uno asociado. Se definen grupos **encadenados**: cada capa sólo acepta tráfico del grupo de la capa anterior, no de direcciones IP sueltas.

**Tabla 2.3. Reglas de entrada de los grupos de seguridad**

| Grupo | Protocolo / puerto | Origen permitido | Justificación |
|---|---|---|---|
| **sg-alb** | HTTPS · 443 | `0.0.0.0/0` | Único punto expuesto a Internet; tráfico cifrado con TLS. |
| **sg-app** | HTTP · 8080 | sg-alb | Las aplicaciones sólo reciben tráfico del balanceador. |
| **sg-db** | TCP · 1433 (SQL Server) | sg-app y rango on-premise | La base sólo acepta conexiones de la aplicación y de la migración. |
| **Administración** | Ninguno (SSH/RDP cerrados) | — | El acceso administrativo se hace con AWS Systems Manager Session Manager, con IAM y registro de sesiones. |

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

### DNS con Amazon Route 53

El DNS traduce nombres de dominio en direcciones IP. Amazon Route 53 actuará como **DNS autoritativo** de los dominios de Tech Consulting: una **zona pública** resuelve el dominio de los productos digitales hacia el balanceador, y una **zona privada**, visible sólo dentro de la VPC, asigna nombres internos a los servicios (por ejemplo, `db.interno.techconsulting`). Además, sus *health checks* verifican la disponibilidad del sitio y permiten redirigir el tráfico ante una falla.

## 2.1.4 Servicios de cómputo

Una máquina virtual es un software que crea una capa independiente y aislada en la que se emula un ordenador completo. En la nube, sus ventajas —sin inversión en hardware, implantación rápida, elasticidad— se aprovechan a través de dos servicios complementarios:

| Servicio | Uso en Tech Consulting | Configuración propuesta |
|---|---|---|
| **Amazon EC2** | Aplicaciones que requieren control del sistema operativo: componentes de los sistemas transaccionales y herramientas internas. | AMI base endurecida; tipo de instancia según carga (familia de propósito general); volúmenes EBS cifrados; perfil de instancia con rol IAM; sin IP pública. |
| **EC2 Auto Scaling** | Responder a la demanda creciente de los productos digitales. | Mínimo de 2 instancias (una por zona); escala según uso de CPU o cantidad de solicitudes del balanceador. |
| **Amazon ECS sobre AWS Fargate** | Microservicios que hoy generan eventos en tiempo real. | Contenedores sin administrar servidores; escalado automático por tarea; envío de eventos a Amazon Kinesis. |
| **Elastic Load Balancing (ALB)** | Distribuir el tráfico entre instancias y zonas. | Terminación TLS, controles de salud y AWS WAF frente a ataques web comunes. |

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

Durante la creación de cada instancia EC2 se definen, en orden, la AMI (imagen de máquina), el tipo de instancia, los detalles de configuración (subred, rol IAM, cantidad), el almacenamiento (tamaño, tipo de volumen, cifrado y eliminación al terminar) y el grupo de seguridad. Para pruebas de concepto puede usarse una instancia de la capa gratuita, sin generar costos.

### 2.1.5 Servicios de almacenamiento

El almacenamiento en la nube debe cumplir tres requisitos: **durabilidad** (datos guardados de forma redundante), **disponibilidad** (accesibles cuando se necesiten) y **seguridad** (cifrado). AWS ofrece servicios de almacenamiento por bloques, archivos y objetos, además de servicios para migrar y proteger datos:

| Servicio | Tipo | Uso en la propuesta |
|---|---|---|
| **Amazon S3** | Objetos | Base del data lake (zonas Raw, Curated y Analytics); destino de eventos, planillas migradas y datos de referencia. Bloqueo de acceso público, cifrado y versionado activados. |
| **Amazon EBS** | Bloques | Discos de las instancias EC2, cifrados con AWS KMS y con *snapshots* automáticos. |
| **Amazon EFS** | Archivos | Sistema de archivos compartido entre instancias que lo necesiten, con escalado automático. |
| **AWS DataSync** | Migración | Transferencia en línea de los archivos existentes (planillas, listados) desde el centro de datos a S3, con verificación de integridad. |
| **AWS Transfer Family** | Transferencia | Canal SFTP gestionado para que las áreas carguen archivos de forma controlada y auditada mientras se abandona Excel como fuente. |
| **AWS Storage Gateway** | Híbrido | Acceso desde las oficinas al almacenamiento en la nube durante la convivencia on-premise y nube. |

| Servicio | Tipo | Uso en la propuesta |
|---|---|---|
| **AWS Backup y AWS Elastic Disaster Recovery** | Protección | Políticas centralizadas de copias (EBS, EFS, RDS, S3) y recuperación rápida de servidores ante desastres. |

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

### 2.1.6 Servicios de bases de datos

Las bases de datos en la nube (DBaaS) se ejecutan en la infraestructura del proveedor y aportan acceso fácil, escalabilidad y recuperación ante desastres. Para el caso se propone:

- **Amazon RDS for SQL Server (Multi-AZ):** aloja los tres sistemas transaccionales sin reescribirlos. AWS gestiona la infraestructura, los parches del motor y las copias automáticas; Tech Consulting conserva la gestión total de su información. La réplica sincrónica en otra zona asume el servicio automáticamente si la principal falla.
- **AWS Database Migration Service (DMS):** realiza la carga inicial y luego replica los cambios en forma continua (CDC) desde SQL Server on-premise, lo que reduce la ventana de corte.
- **Amazon Redshift Serverless:** data warehouse para la capa analítica y las métricas únicas, como se planteó en la Parte 1.
- **Amazon Aurora (evolución futura):** base relacional nativa de la nube que podría evaluarse más adelante si se decide modernizar los sistemas y dejar el motor SQL Server.

### 2.1.7 Equivalencias multicloud y trazabilidad con el caso

Aunque la propuesta se basa en AWS, los conceptos son multicloud. La siguiente tabla muestra los servicios equivalentes en los tres proveedores vistos en el módulo:

**Tabla 2.4. Equivalencia de servicios entre proveedores**

| Función | AWS | Microsoft Azure | Google Cloud |
|---|---|---|---|
| **Red privada virtual** | Amazon VPC | Azure Virtual Network | VPC |
| **Firewall de recursos** | Security groups | Network security groups | Reglas de firewall de VPC |
| **DNS** | Amazon Route 53 | Azure DNS | Cloud DNS |
| **Máquinas virtuales** | Amazon EC2 | Azure Virtual Machines | Compute Engine |
| **Almacenamiento de objetos** | Amazon S3 | Azure Blob Storage | Cloud Storage |
| **Base relacional gestionada** | Amazon RDS / Aurora | Azure SQL | Cloud SQL / Cloud Spanner |

| Función | AWS | Microsoft Azure | Google Cloud |
|---|---|---|---|
| **Monitoreo** | Amazon CloudWatch | Azure Monitor | Cloud Monitoring |

**Fuente:** elaboración propia con base en los contenidos del módulo y la documentación de cada proveedor.

**Tabla 2.5. Servicios que resuelven cada problema del escenario**

| Problema del escenario | Servicios de infraestructura involucrados |
|---|---|
| **Excel como fuente de datos** | AWS DataSync y Transfer Family para migrar y recibir archivos; Amazon S3 como repositorio central. |
| **Tres bases en SQL Server** | AWS DMS para migrar; Amazon RDS for SQL Server Multi-AZ en subredes privadas de datos; VPN durante la transición. |
| **Eventos en tiempo real sin capturar** | Microservicios en ECS Fargate que publican en Amazon Kinesis, con destino final en S3. |
| **Datos fuera de todo sistema** | Carga controlada en S3 y registro en tablas maestras del data lake. |
| **Escalado de procesos y cómputo** | EC2 Auto Scaling, ECS Fargate y Application Load Balancer distribuidos en dos zonas. |

**Fuente:** elaboración propia.

# 2.2 Funcionalidades del monitoreo de sistemas cloud

## 2.2.1 Concepto y objetivo

El *cloud monitoring* es el proceso de evaluar el estado de las infraestructuras de TI basadas en la nube. Permite supervisar de forma **proactiva** la disponibilidad, el rendimiento y la seguridad del entorno para detectar y corregir problemas antes de que afecten al usuario final (Cisco, s. f.).

Para Tech Consulting, el monitoreo cumple un doble rol. Desde la operación, garantiza que los productos digitales respondan bien aun con demanda creciente. Desde la seguridad, aporta la **visibilidad y trazabilidad** que hoy faltan: saber quién accedió a qué, cuándo y desde dónde, y detectar comportamientos anómalos.

## 2.2.2 Herramientas de monitoreo en AWS

| Herramienta | Enfoque | Qué aporta |
|---|---|---|
| **Amazon CloudWatch** | Rendimiento | Servicio central de monitoreo y observabilidad: métricas, registros (Logs), alarmas, paneles (Dashboards) y pruebas sintéticas de sitios web (Synthetics). |
| **VPC Flow Logs** | Red | Registro del tráfico IP aceptado y rechazado en las interfaces de red de la VPC. |
| **AWS CloudTrail** | Auditoría | Registro de todas las acciones realizadas en la cuenta: quién, qué, cuándo y desde dónde. |
| **Amazon GuardDuty** | Amenazas | Detección inteligente de amenazas a partir de CloudTrail, Flow Logs y registros de DNS. |
| **AWS Config** | Configuración | Historial de configuración de los recursos y verificación de reglas de cumplimiento (por ejemplo, “ningún bucket público”). |
| **AWS Security Hub** | Postura | Consolida los hallazgos de seguridad y los compara con estándares de buenas prácticas. |
| **RDS Performance Insights** | Bases de datos | Análisis de la carga y de las consultas más costosas de cada base. |
| **AWS Budgets y Cost Explorer** | Costos | Seguimiento del consumo y alertas ante desvíos de presupuesto. |

**Fuente:** elaboración propia con base en la documentación de AWS.

## 2.2.3 Funcionalidades aplicadas a Tech Consulting

El módulo identifica cinco funciones principales del monitoreo en la nube. La tabla las traduce a métricas y alarmas concretas para el caso (los umbrales son de ejemplo).

**Tabla 2.6. Matriz de monitoreo propuesta**

| Función | Herramienta | Métricas clave | Alarma de ejemplo |
|---|---|---|---|
| **Sitios web** | CloudWatch Synthetics, Route 53 health checks, métricas del ALB | Disponibilidad, tiempo de respuesta, errores HTTP 5xx | Más de 1 % de respuestas 5xx durante 5 minutos. |
| **Red virtual** | VPC Flow Logs, métricas de NAT Gateway y VPN | Tráfico rechazado, estado de los túneles VPN, conexiones de salida | Túnel VPN caído o pico de tráfico rechazado hacia la subred de datos. |
| **Bases de datos** | CloudWatch + RDS Performance Insights | CPU, conexiones, latencia de lectura/escritura, espacio libre, retraso de réplica | Espacio libre menor al 15 % o CPU superior al 80 % sostenida. |

| Función | Herramienta | Métricas clave | Alarma de ejemplo |
|---|---|---|---|
| **Máquinas virtuales** | CloudWatch Agent, Auto Scaling | CPU, memoria, disco, estado de las verificaciones de la instancia | Falla de verificación de estado; reemplazo automático de la instancia. |
| **Almacenamiento** | Métricas de S3, AWS Config, CloudTrail (eventos de datos) | Volumen almacenado, solicitudes, cambios de permisos, accesos | Cualquier cambio que vuelva público un bucket. |

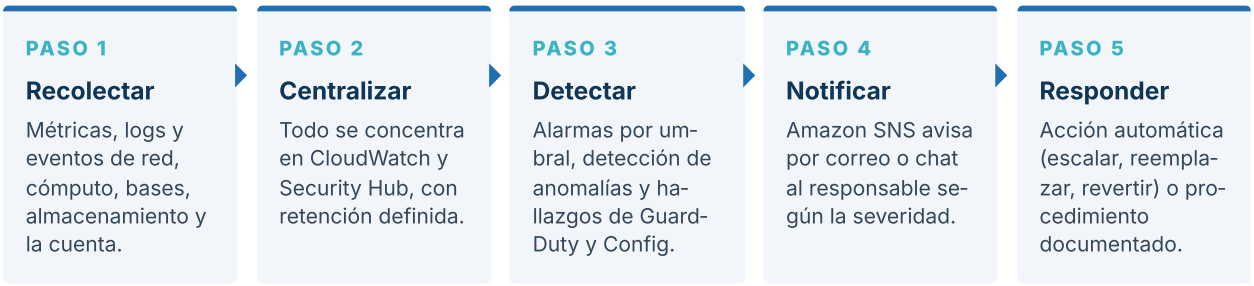
**Fuente:** elaboración propia con base en las funciones del monitoreo cloud del módulo.

A estas cinco funciones se suma el **monitoreo de seguridad**: alertas de GuardDuty (por ejemplo, inicios de sesión desde ubicaciones inusuales), uso de la cuenta raíz, intentos de acceso denegados y desactivación de CloudTrail.

## 2.2.4 Ciclo de detección y respuesta

Monitorear no es sólo mirar paneles: cada señal debe terminar en una acción. Se propone el siguiente ciclo:

**Figura 2.2. Ciclo de monitoreo, alerta y respuesta**




**Fuente:** elaboración propia.

Se definen además dos **paneles**: uno operativo (disponibilidad, latencia, uso de recursos y estado de la migración) y uno de seguridad (hallazgos abiertos, accesos denegados, cambios de configuración críticos).

## 2.2.5 Ventajas del monitoreo cloud para el caso

| Ventaja | Aplicación en Tech Consulting |
|---|---|
| **Facilidad de acceso a la información** | El estado de toda la plataforma se consulta desde la consola o los paneles, sin acceder a cada servidor. |
| **Mayor seguridad y control** | Trazabilidad de cada acción y detección temprana de amenazas y errores de configuración. |
| **Concentración en una única plataforma** | Métricas, logs y hallazgos de todas las capas reunidos en CloudWatch y Security Hub. |

| Ventaja | Aplicación en Tech Consulting |
|---|---|
| **Optimización del rendimiento** | Los datos de uso alimentan el Auto Scaling y permiten ajustar el tamaño de los recursos. |
| **Acceso simultáneo desde cualquier lugar** | Los equipos de operaciones y seguridad consultan los mismos paneles en paralelo, con permisos por rol. |

## 2.3 Mejores prácticas para la migración a la nube

Las siguientes prácticas se organizan según el momento de la migración y se alinean con los pilares del AWS Well-Architected Framework, presentados en el Módulo 1.

### 2.3.1 Planificación y fundaciones

- **Inventario y clasificación:** relevar sistemas, bases, archivos y dependencias, y clasificar la información según su sensibilidad antes de mover nada.
- **Zona de aterrizaje (*landing zone*):** crear cuentas separadas para producción, desarrollo, seguridad y registros con AWS Organizations, para aislar los entornos y limitar el impacto de un error.
- **Infraestructura como código:** definir la VPC, las subredes, las rutas y los grupos de seguridad con AWS CloudFormation, de modo que el entorno sea reproducible, revisable y versionado.
- **Diseñar el direccionamiento con tiempo:** elegir rangos IP que no se superpongan con la red on-premise, para que la VPN funcione sin conflictos.
- **Piloto controlado:** migrar primero un sistema de menor criticidad, validar y recién después avanzar con el resto.

### 2.3.2 Seguridad de red, identidades y datos

- **Defensa en profundidad en la red:** subredes privadas para aplicaciones y datos, grupos de seguridad encadenados, Network ACL como segunda barrera y AWS WAF delante del balanceador.
- **Sin puertos de administración abiertos:** no exponer SSH (22) ni RDP (3389) a Internet; usar Session Manager con registro de sesiones.
- **Endpoints de VPC:** acceder a S3 y a otros servicios por la red privada de AWS, sin pasar por Internet.
- **Identidades:** no usar la cuenta raíz en la operación diaria; usuarios y roles de IAM con mínimo privilegio, MFA obligatorio y roles de instancia en lugar de claves de acceso.
- **Cifrado en todas partes:** AWS KMS para EBS, S3 y RDS; TLS en tránsito; credenciales de bases en AWS Secrets Manager con rotación automática.
- **Bloqueo de acceso público en S3** a nivel de cuenta y versionado de los buckets críticos.

### 2.3.3 Ejecución de la migración

- **Copias de seguridad previas** de cada base y conjunto de archivos antes de iniciar.
- **Replicación continua:** usar DMS con CDC para mantener sincronizado el destino y reducir la ventana de corte.
- **Validación de datos:** habilitar la validación de DMS y la verificación de integridad de DataSync; comparar conteos y totales de control entre origen y destino.
- **Ventanas de corte acordadas** con el negocio y un **plan de vuelta atrás** documentado y probado.
- **Monitoreo activo durante la migración:** paneles específicos para seguir el avance, la latencia de réplica y los errores.

### 2.3.4 Operación, continuidad y costos

- **Alta disponibilidad:** todo componente crítico en al menos dos zonas.
- **Respaldo y recuperación:** políticas de AWS Backup con retención definida, copias en otra región y **pruebas periódicas de restauración**; un respaldo no probado no garantiza nada.
- **Gestión de parches:** AWS Systems Manager Patch Manager para las instancias EC2.
- **Etiquetado** de todos los recursos (sistema, entorno, responsable) para ordenar el inventario, los permisos y los costos.
- **Optimización de costos:** ajustar el tamaño de las instancias según el monitoreo, apagar entornos no productivos fuera de horario y configurar alertas de presupuesto.
- **Revisión continua:** aplicar periódicamente la herramienta AWS Well-Architected Tool para detectar desvíos respecto de las buenas prácticas.

### 2.3.5 Lista de verificación

**Tabla 2.7. Lista de verificación de mejores prácticas**

| Práctica | Pilar Well-Architected | Momento | Verificado |
|---|---|---|---|
| Cuentas separadas por entorno y VPC por capas | Seguridad | Planificación | ☐ |
| Infraestructura definida como código | Excelencia operativa | Planificación | ☐ |
| MFA, mínimo privilegio y cuenta raíz protegida | Seguridad | Fundaciones | ☐ |
| Cifrado con KMS y TLS en todos los servicios | Seguridad | Fundaciones | ☐ |
| CloudTrail, Config y GuardDuty activos antes de migrar | Seguridad | Fundaciones | ☐ |
| Respaldo previo y plan de vuelta atrás | Fiabilidad | Migración | ☐ |
| Validación de datos entre origen y destino | Fiabilidad | Migración | ☐ |

| Práctica | Pilar Well-Architected | Momento | Verificado |
|---|---|---|---|
| Componentes críticos en dos zonas (Multi-AZ) | Fiabilidad | Operación | ☐ |
| Auto Scaling configurado según métricas reales | Eficacia del rendimiento | Operación | ☐ |
| Alarmas y paneles operativos y de seguridad | Excelencia operativa | Operación | ☐ |
| Pruebas periódicas de restauración | Fiabilidad | Operación | ☐ |
| Etiquetado, presupuestos y ajuste de tamaño | Optimización de costos | Operación | ☐ |

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

## 2.4 Síntesis de la Parte 2

La arquitectura propuesta traduce los objetivos de la Parte 1 en una infraestructura concreta. La **VPC dividida en tres capas y dos zonas de disponibilidad** ofrece aislamiento y alta disponibilidad; el enrutamiento con Internet Gateway y NAT Gateway, junto con grupos de seguridad encadenados, asegura que sólo el balanceador quede expuesto a Internet y que las bases de datos sean inaccesibles desde el exterior.

Los servicios de cómputo (EC2 con Auto Scaling y ECS Fargate), almacenamiento (S3, EBS, EFS y los servicios de transferencia) y bases de datos gestionadas (RDS for SQL Server con DMS) dan respuesta directa a cada problema del escenario: centralizan los datos dispersos, migran los sistemas transaccionales con mínima interrupción, capturan los eventos en tiempo real y permiten escalar según la demanda.

El **monitoreo cloud** es el componente que hace que todo lo anterior sea gestionable. Con CloudWatch, CloudTrail, GuardDuty y Config, la empresa pasa de no tener visibilidad a poder medir el rendimiento, auditar cada acción y detectar amenazas de forma proactiva, con un ciclo claro que va de la señal a la respuesta.

Por último, las **mejores prácticas** recuerdan que la seguridad de la migración depende tanto del diseño como de la disciplina: planificar antes de mover datos, aplicar mínimo privilegio y cifrado en todas partes, validar cada paso, probar las restauraciones y revisar la arquitectura de manera continua. Bajo el modelo de responsabilidad compartida, estas tareas son responsabilidad de Tech Consulting, y de su cumplimiento depende la protección de sus datos en la nube.

PARTE 3

# Riesgos, auditoría y DevOps

Identificación y evaluación de riesgos de la arquitectura, funcionalidades de la auditoría informática y beneficios de integrar la cultura DevOps con la nube.

3.1 Riesgos en las arquitecturas cloud

3.2 Funcionalidades de la auditoría informática

3.3 Beneficios de la integración DevOps + Cloud

3.4 Síntesis de la Parte 3

Actividad Práctica Integradora 3 · Virtualización y contenedores

# 3.1 Riesgos en las arquitecturas cloud

## 3.1.1 Superficie de riesgo de la arquitectura propuesta

Toda la arquitectura se apoya en la **virtualización**: AWS ejecuta las instancias sobre un hipervisor de tipo 1 (nativo), que corre directamente sobre el hardware y aísla las máquinas virtuales de distintos clientes. Por encima de esa base, cada capa agrega su propia superficie de ataque. Bajo el modelo de responsabilidad compartida, la seguridad del hipervisor y del hardware corresponde a AWS, mientras que todo lo que Tech Consulting configura —red, identidades, sistemas operativos, contenedores y datos— es responsabilidad de la empresa.

**Tabla 3.1. Capas de la arquitectura y responsable de su seguridad**

| Capa | Componentes | Responsable | Riesgo principal |
|---|---|---|---|
| **Física y virtualización** | Centros de datos, servidores, hipervisor (AWS Nitro) | AWS | Escape de máquina virtual o falla del hipervisor. |
| **Red** | VPC, subredes, rutas, security groups, VPN | Tech Consulting | Reglas demasiado permisivas y falta de segmentación. |
| **Identidades** | Cuenta raíz, usuarios, roles y políticas IAM | Tech Consulting | Credenciales robadas y privilegios excesivos. |
| **Cómputo** | Instancias EC2, contenedores en ECS Fargate | Compartido | *Malware*, imágenes vulnerables y falta de parches. |
| **Datos** | Amazon S3, RDS for SQL Server, volúmenes EBS | Tech Consulting | Exposición pública, pérdida o cifrado por *ransomware*. |
| **Operación** | Despliegues, cambios, registros | Tech Consulting | Cambios manuales no controlados y falta de trazabilidad. |

**Fuente:** elaboración propia.

## 3.1.2 Riesgos de virtualización, segmentación y aislamiento

La **segmentación de red** divide una red en subredes que funcionan como redes propias, lo que permite definir políticas detalladas para controlar el tráfico entre ellas. Segmentar implica aislar: si un segmento se ve comprometido, el atacante no debería poder moverse libremente hacia los demás.

- **Movimiento lateral:** si las capas de aplicación y datos compartieran reglas amplias, una instancia comprometida podría alcanzar directamente las bases de datos. *Control:* las tres capas de subredes de la Parte 2 y los *security groups* encadenados (cada capa sólo acepta tráfico de la anterior), sumados a Network ACL como segunda barrera.
- **Exposición accidental:** abrir puertos de administración (SSH/RDP) o asignar IP públicas a servidores internos. *Control:* sin IP públicas en subredes privadas, acceso administrativo mediante Session

Manager y reglas de AWS Config que alertan ante cualquier puerto abierto a Internet.

- **Firewall perimetral insuficiente:** los *firewalls* filtran el tráfico entrante y saliente según reglas, advierten intentos de conexión y bloquean aplicaciones riesgosas. *Control:* AWS WAF delante del balanceador y AWS Network Firewall para inspeccionar el tráfico de salida.
- **Escape de máquina virtual:** una vulnerabilidad del hipervisor permitiría a una máquina virtual acceder a otras del mismo host. Es un riesgo de baja probabilidad que el modelo de responsabilidad compartida **transfiere** al proveedor.

### 3.1.3 Riesgo de malware

El *malware* es un programa que se instala sin el conocimiento del propietario para robar información o tomar el control del sistema. En la nube no desaparece: cambia de vector. La siguiente tabla relaciona los tipos vistos en el módulo con el escenario de Tech Consulting.

**Tabla 3.2. Tipos de malware y su impacto en el caso**

| Tipo | Vector probable en Tech Consulting | Controles propuestos |
|---|---|---|
| **Virus** | Planillas Excel con macros maliciosas cargadas al data lake o compartidas entre áreas. | Escaneo de archivos en la carga a S3; bloqueo de macros en los equipos de usuario; antivirus en estaciones de trabajo. |
| **Gusano** | Propagación desde un equipo on-premise infectado hacia la VPC a través de la VPN. | Segmentación, reglas mínimas en la VPN y detección de tráfico anómalo con GuardDuty y VPC Flow Logs. |
| **Troyano** | Dependencias o imágenes de contenedor aparentemente legítimas que esconden código malicioso. | Sólo imágenes de repositorios confiables, escaneo en Amazon ECR y Amazon Inspector. |
| **Spyware** | Robo de credenciales de consola desde equipos de los administradores. | MFA obligatorio, sesiones cortas y alertas por inicios de sesión inusuales. |
| **Ransomware** | Cifrado de bases y archivos, y borrado de las copias para forzar un pago. | Copias con AWS Backup en una cuenta separada, bóveda inmutable (*Vault Lock*), S3 Object Lock y versionado. |

**Fuente:** elaboración propia con base en "¿Qué es un malware?" (2021).

Las medidas básicas del módulo —antivirus, copias de seguridad regulares, actualización de parches, control riguroso de accesos y concientización del personal— siguen vigentes; en la nube se complementan con detección gestionada (Amazon GuardDuty, incluida su protección contra *malware* en EC2 y S3) y con copias que el atacante no pueda alterar.

### 3.1.4 Puntos únicos de fallo y alta disponibilidad

La regla básica de la alta disponibilidad (HA) es la replicación de elementos. Un **punto único de fallo** (SPOF) es cualquier componente no replicado cuya falla interrumpe el servicio. La tabla revisa la arqui-

tectura en busca de SPOF.

**Tabla 3.3. Análisis de puntos únicos de fallo**

| Componente | ¿Por qué podría ser un SPOF? | Mitigación aplicada |
|---|---|---|
| **Base de datos** | Una sola instancia de SQL Server detendría los tres sistemas. | RDS Multi-AZ con réplica sincrónica y conmutación automática. |
| **Servidores de aplicación** | Una única instancia o tarea concentra todo el tráfico. | Grupo de Auto Scaling con mínimo dos instancias, una por zona. |
| **Salida a Internet** | Un solo NAT Gateway deja sin salida a ambas zonas si falla la suya. | Un NAT Gateway por zona de disponibilidad. |
| **Conexión híbrida** | Un único túnel VPN corta la replicación durante la migración. | Dos túneles VPN redundantes (los provee AWS por defecto). |
| **Región** | Toda la plataforma depende de una sola región. | Copias en otra región y procedimiento de recuperación documentado. |
| **Personas** | Un único administrador concentra el conocimiento y los accesos. | Roles compartidos, documentación, infraestructura como código y cuenta de emergencia (*break-glass*) custodiada. |

**Fuente:** elaboración propia.

### 3.1.5 Riesgos de contenedores y de infraestructura mutable

Los contenedores permiten ejecutar una aplicación de forma idéntica en cualquier entorno, pero introducen riesgos propios:

- **Imágenes vulnerables o maliciosas** descargadas de repositorios públicos sin verificación.
- **Secretos dentro de las imágenes** (contraseñas o claves escritas en el código o en el Dockerfile).
- **Contenedores con privilegios excesivos**, que ejecutan procesos como *root* o con acceso al host.
- **Falta de orquestación y control** sobre qué versión de cada servicio está en ejecución.

Por otro lado, en una **infraestructura mutable** los servidores se modifican después de implementarse: parches manuales, cambios de configuración "en caliente". Con el tiempo, cada servidor termina siendo distinto de los demás (*configuration drift*), los errores son difíciles de reproducir y no queda claro qué cambió ni quién lo cambió. Ambos riesgos se tratan en la sección 3.3 con imágenes versionadas, escaneo automático e infraestructura inmutable.

### 3.1.6 Matriz consolidada de riesgos

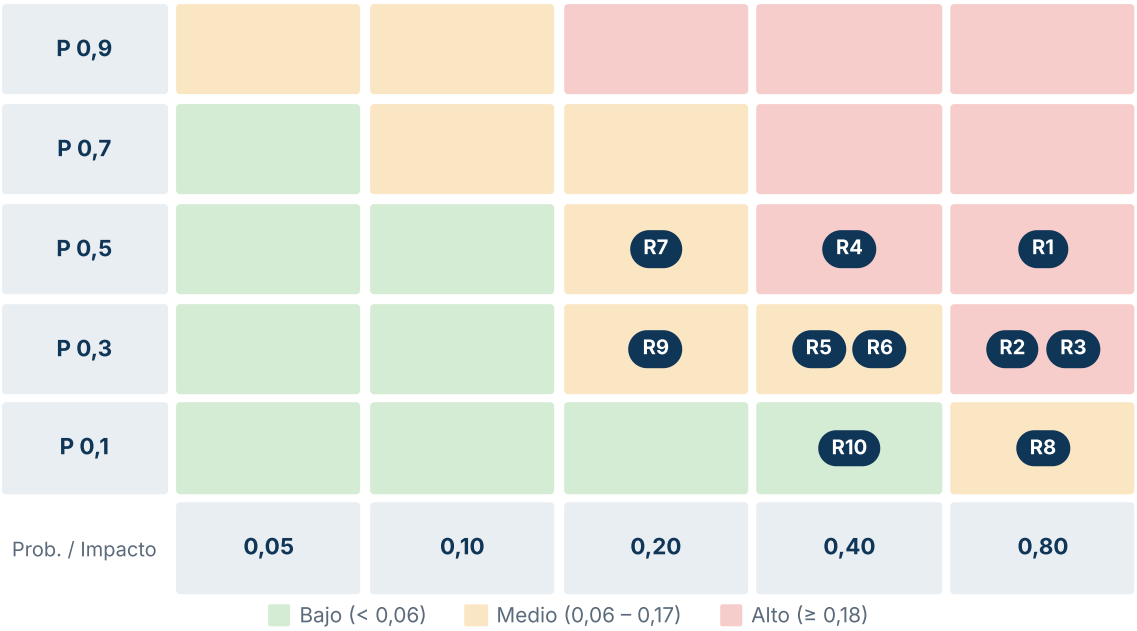
Siguiendo la metodología del Módulo 1, se estima cada riesgo con la fórmula **Riesgo = Probabilidad × Impacto**, usando las mismas escalas: bajo, menor a 0,06; medio, entre 0,06 y 0,17; alto, desde 0,18.

**Tabla 3.4. Evaluación de riesgos de la arquitectura cloud**

| # | Riesgo | P | I | Nivel | Estrategia | Tratamiento principal |
|---|---|---|---|---|---|---|
| **R1** | Configuración incorrecta que expone datos o servicios | 0,5 | 0,80 | 0,40 Alto | Mitigar | Infraestructura como código revisada, AWS Config y Security Hub. |
| **R2** | Credenciales comprometidas o abuso de privilegios | 0,3 | 0,80 | 0,24 Alto | Mitigar | MFA, mínimo privilegio, roles temporales y alertas. |
| **R3** | Ransomware sobre bases, archivos o instancias | 0,3 | 0,80 | 0,24 Alto | Mitigar | Copias inmutables en cuenta separada y pruebas de restauración. |
| **R4** | Imagen de contenedor vulnerable o con código malicioso | 0,5 | 0,40 | 0,20 Alto | Mitigar | Escaneo en el pipeline y en ECR; imágenes base aprobadas. |
| **R5** | Falla de un componente único (SPOF) | 0,3 | 0,40 | 0,12 Medio | Mitigar | Redundancia Multi-AZ en todas las capas. |
| **R6** | Movimiento lateral por segmentación insuficiente | 0,3 | 0,40 | 0,12 Medio | Mitigar | Subredes por capa, *security groups* encadenados, Network Firewall. |
| **R7** | Deriva de configuración en servidores mutables | 0,5 | 0,20 | 0,10 Medio | Evitar | Infraestructura inmutable: se reemplaza, no se modifica. |
| **R8** | Escape de máquina virtual en el hipervisor | 0,1 | 0,80 | 0,08 Medio | Transferir | Responsabilidad del proveedor; certificaciones verificables en AWS Artifact. |
| **R9** | Falta de registros para investigar un incidente | 0,3 | 0,20 | 0,06 Medio | Mitigar | Registros centralizados e inmutables (sección 3.2.3). |
| **R10** | Indisponibilidad de una región completa | 0,1 | 0,40 | 0,04 Bajo | Aceptar | Copias en otra región; se acepta el tiempo de recuperación. |

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

**Figura 3.1. Mapa de calor de los riesgos identificados**




**Fuente:** elaboración propia.

Los cuatro riesgos altos tienen un rasgo común: todos dependen de decisiones de **configuración, identidades y procesos** de Tech Consulting, no del proveedor. Por eso, como se verá a continuación, la auditoría continua y la automatización propia de DevOps son las respuestas más efectivas.

# 3.2 Funcionalidades de la auditoría informática

## 3.2.1 Concepto y beneficios

La auditoría informática es un estudio profesional que realizan especialistas en ciberseguridad, generalmente ajenos a la empresa, con el objetivo de detectar las vulnerabilidades y amenazas de la tecnología que sostiene la estrategia de negocio (“Por qué es necesario hacer una auditoría de seguridad informática”, s. f.). En un entorno cloud, la auditoría verifica que los controles diseñados realmente estén funcionando y que la organización pueda demostrarlo.

| Beneficio | Aplicación en Tech Consulting |
|---|---|
| **Detecta debilidades en los sistemas de seguridad** | Errores de código en los microservicios y configuraciones inseguras en la cuenta de AWS. |
| **Identifica posibles actuaciones fraudulentas** | Accesos no autorizados a datos comerciales o cambios de permisos sin justificación. |
| **Mejora los controles internos** | Verifica que RBAC, MFA y cifrado se apliquen igual en todos los entornos. |

| Beneficio | Aplicación en Tech Consulting |
|---|---|
| **Elimina puntos débiles** | Cada hallazgo genera una acción correctiva con responsable y fecha. |
| **Mantiene los sistemas actualizados** | Controla el nivel de parches de instancias, imágenes y dependencias. |

## 3.2.2 Tipos de auditoría aplicados al caso

**Tabla 3.5. Plan de auditorías propuesto**

| Tipo | Alcance en Tech Consulting | Herramientas de apoyo | Frecuencia |
|---|---|---|---|
| **Web** | Productos digitales y APIs expuestas a través del balanceador. | Pruebas de penetración autorizadas, OWASP ZAP, registros de AWS WAF. | Anual y ante cambios mayores. |
| **Código fuente** | Microservicios, scripts de procesamiento de datos e infraestructura como código. | SonarQube (análisis estático), revisión de dependencias, escaneo de plantillas IaC. | Continua, en cada cambio (pipeline). |
| **Redes** | VPC, *security groups*, rutas, VPN y salida a Internet. | VPC Flow Logs, AWS Config, Network Access Analyzer. | Trimestral y continua. |
| **Dispositivos e infraestructura** | Instancias, imágenes y contenedores. La infraestructura física la audita AWS. | Amazon Inspector, Systems Manager, informes SOC e ISO en AWS Artifact. | Continua; revisión semestral. |
| **Forense** | Investigación posterior a un incidente: qué pasó, cómo y qué datos se afectaron. | CloudTrail, Amazon Detective, *snapshots* de volúmenes aislados. | Ante cada incidente. |

**Fuente:** elaboración propia con base en "Qué es una auditoría de seguridad informática: tipos y fases" (2021).

La auditoría de la infraestructura física merece una aclaración: en la nube, Tech Consulting no puede ingresar a los centros de datos de AWS. Se apoya, en cambio, en los informes de auditorías independientes que el proveedor publica (SOC 1/2/3, ISO 27001), disponibles en AWS Artifact. Es la aplicación directa del modelo de responsabilidad compartida a la auditoría.

## 3.2.3 Registros de auditoría en la nube

Sin registros no hay auditoría posible. Se propone registrar, centralizar y proteger las siguientes fuentes:

**Tabla 3.6. Registros de auditoría propuestos**

| Registro | Qué responde | Retención sugerida |
|---|---|---|
| **AWS CloudTrail** | ¿Quién hizo qué acción sobre la cuenta, cuándo y desde dónde? | Al menos 1 año |
| **Eventos de datos de S3** | ¿Quién leyó, modificó o borró cada objeto del data lake? | 1 año |

| Registro | Qué responde | Retención sugerida |
|---|---|---|
| **VPC Flow Logs** | ¿Qué tráfico se aceptó o rechazó entre subredes y hacia Internet? | 90 días |
| **Auditoría de SQL Server (RDS)** | ¿Quién consultó o modificó datos sensibles en las bases transaccionales? | 1 año |
| **Registros del ALB y de AWS WAF** | ¿Qué solicitudes recibieron los productos digitales y cuáles se bloquearon? | 90 días |
| **Registros de contenedores e instancias** | ¿Qué hizo cada aplicación y qué errores generó? | 30 a 90 días |
| **Historial de AWS Config** | ¿Cómo estaba configurado cada recurso en una fecha dada? | 1 año |

**Fuente:** elaboración propia. Los plazos son orientativos y deben ajustarse a la normativa aplicable.

> **PROTECCIÓN DE LOS REGISTROS**
>
> Los registros se envían a una **cuenta de archivo separada**, a la que los administradores de producción no tienen acceso de escritura. Se almacenan en S3 con cifrado, **Object Lock** (no se pueden borrar ni modificar durante el período de retención) y la validación de integridad de CloudTrail activada. Así, aun si un atacante obtiene privilegios en producción, no puede borrar sus huellas.

## 3.2.4 Funcionalidades y proceso de auditoría

Integrando lo anterior, la auditoría informática aporta cinco funcionalidades a la plataforma de Tech Consulting:

FUNCIONALIDAD 1

### Trazabilidad

Reconstruir cualquier acción sobre la cuenta, la red o los datos, con usuario, hora y origen.

FUNCIONALIDAD 2

### Detección

Identificar accesos indebidos, configuraciones inseguras y comportamientos anómalos.

FUNCIONALIDAD 3

### Control continuo

Evaluar en forma automática el cumplimiento de reglas con AWS Config, Security Hub y AWS Audit Manager.

FUNCIONALIDAD 4

### Evidencia y cumplimiento

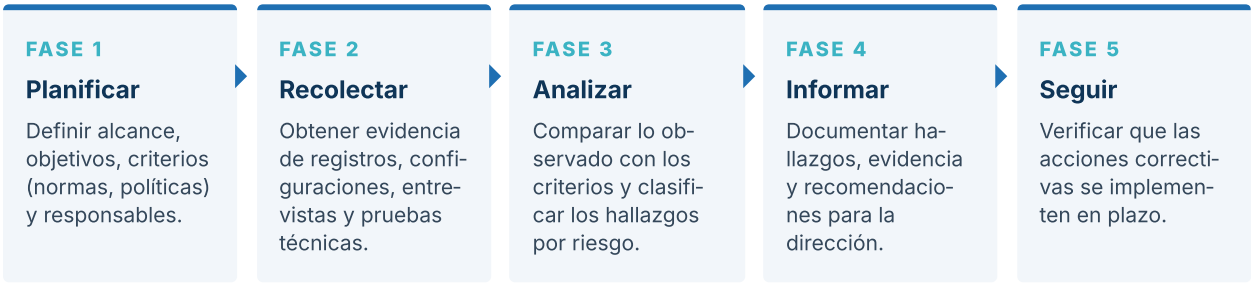
Demostrar ante terceros el tratamiento adecuado de los datos personales, conforme a la Ley 25.326.

FUNCIONALIDAD 5

**Investigación forense y mejora**

Ante un incidente, determinar causa, alcance y datos afectados, y convertir las conclusiones en nuevos controles.

**Figura 3.2. Fases del proceso de auditoría**




**Fuente:** elaboración propia.

# 3.3 Beneficios de la integración DevOps + Cloud

## 3.3.1 Qué es y qué no es DevOps

DevOps —contracción de *Development* y *Operations*— es una cultura que busca mejorar la agilidad en la entrega de servicios de TI mediante la comunicación transparente, la colaboración y la integración entre desarrollo y operaciones, desde la planificación y el diseño del software hasta su despliegue en producción ("DevOps, el nuevo lenguaje entre áreas de desarrollo y operaciones", s. f.). Se resume en tres componentes: **colaboración + procesos + herramientas**.

Es tan importante entender qué **no** es: no es sólo automatización, no es sólo usar servicios cloud, no es una herramienta que se instala y no es un equipo nuevo aislado del resto de TI. Para Tech Consulting esto significa que adoptar DevOps implica cambiar la forma de trabajar entre quienes desarrollan los productos digitales, quienes operan la plataforma y quienes la protegen. Cuando la seguridad se integra en ese ciclo desde el inicio se habla de **DevSecOps**.

## 3.3.2 Pipeline CI/CD propuesto

El núcleo técnico de DevOps es la automatización del ciclo de entrega:

- **Integración continua (CI):** los desarrolladores integran su código a un repositorio común varias veces al día; cada integración se compila y se prueba automáticamente.
- **Entrega continua (CD):** el software queda siempre listo para desplegarse; el pase a producción requiere una aprobación humana.

- **Despliegue continuo:** el pase a producción es totalmente automático y sólo una prueba fallida lo detiene.

Para Tech Consulting se propone comenzar con **entrega continua** (con aprobación manual antes de producción) y evolucionar a despliegue continuo para los microservicios de menor criticidad una vez que las pruebas automáticas sean confiables.

**Figura 3.3. Pipeline DevSecOps propuesto para los microservicios**




**Fuente:** elaboración propia. En rojo, las etapas de control de seguridad; en turquesa, las de operación.

### 3.3.3 Contenedores, orquestación e infraestructura inmutable

**Docker** automatiza la implementación de aplicaciones como contenedores portátiles y autosuficientes que pueden ejecutarse en la nube o localmente. Aporta modularidad, capas y control de versiones de imágenes, implementación rápida y restauración de versiones anteriores. Los microservicios de Tech Consulting se empaquetan como imágenes Docker y se almacenan, versionadas, en Amazon ECR.

Para administrarlos se requiere un **orquestador**. Kubernetes es el estándar de la industria y organiza los contenedores en *pods*, *nodos* y *clústeres* bajo un plano de control. En la propuesta se usa **Amazon ECS sobre Fargate**, un orquestador gestionado más simple de operar; si en el futuro la empresa necesitara portabilidad entre proveedores, podría migrar a **Amazon EKS** (Kubernetes gestionado) sin cambiar las imágenes.

Finalmente, se adopta la **infraestructura inmutable**: los servidores y contenedores nunca se modifican después de implementarse. Si algo necesita actualizarse, se construye una nueva imagen (con EC2 Image Builder para las AMI o con el pipeline para los contenedores), se valida y reemplaza a la anterior, que se retira.

| Aspecto | Infraestructura mutable (actual) | Infraestructura inmutable (propuesta) |
|---|---|---|
| **Actualizaciones** | Parches y cambios sobre el servidor en ejecución. | Se reemplaza el servidor por uno nuevo a partir de una imagen actualizada. |
| **Consistencia** | Cada servidor diverge con el tiempo (deriva de configuración). | Todos los entornos son idénticos: desarrollo, prueba y producción. |
| **Vuelta atrás** | Difícil: hay que deshacer cambios manuales. | Inmediata: se vuelve a desplegar la imagen anterior. |
| **Seguridad** | Un atacante puede persistir en un servidor de larga vida. | Los servidores se renuevan con frecuencia, lo que elimina persistencias. |
| **Auditoría** | Cambios difíciles de rastrear. | Cada versión está registrada en el repositorio y en el pipeline. |

**Fuente:** elaboración propia con base en Alvarado (2021).

### 3.3.4 Beneficios para Tech Consulting

El módulo enumera siete beneficios de implementar una cultura DevOps. La tabla los vincula con los problemas del escenario y con los riesgos de la sección 3.1.

**Tabla 3.7. Beneficios de DevOps + Cloud aplicados al caso**

| Beneficio | Cómo se concreta en Tech Consulting | Riesgo o problema que reduce |
|---|---|---|
| **Mejora la comunicación** | Desarrollo, operaciones y seguridad comparten repositorio, pipeline y paneles de monitoreo. | Silos entre áreas; métricas con criterios propios. |
| **Escalabilidad en los servicios** | Contenedores e infraestructura como código permiten replicar y escalar servicios en minutos. | Demanda creciente de productos digitales. |
| **Mayor seguridad** | Controles automáticos en cada cambio, imágenes escaneadas y configuraciones revisadas antes de llegar a producción. | R1, R4, R7. |
| **Reducción de costos** | Menos trabajo manual, menos incidentes y entornos de prueba que se crean y destruyen bajo demanda. | Capacidad ociosa y retrabajo. |
| **Seguimiento continuado** | El monitoreo de CloudWatch y los registros de auditoría forman parte del ciclo. | R9; detección tardía de fallas. |
| **Publicaciones más frecuentes** | Cambios pequeños y frecuentes, más fáciles de probar y de revertir. | Despliegues grandes y riesgosos. |
| **Software de mejor calidad** | Pruebas automáticas y análisis de código en cada integración. | Errores de programación que llegan a producción. |

**Fuente:** elaboración propia con base en los contenidos del módulo.

La combinación con la nube es lo que hace posibles estos beneficios: sin infraestructura programable y bajo demanda, no se podrían crear entornos idénticos en minutos, reemplazar servidores en lugar de parchearlos ni escalar en forma automática. DevOps aporta el *cómo trabajar*, y la nube, el *dónde* hacerlo con elasticidad.

### 3.3.5 Cómo medir los beneficios

Para verificar que la adopción de DevOps funcione, se proponen las cuatro métricas del programa de investigación DORA (Forsgren et al., 2018), ampliamente utilizadas en la industria:

| | | |
|---|---|---|
| **Frecuencia** de despliegue: cuántas veces se publica a producción por semana. | **Lead time** tiempo desde que un cambio se integra hasta que llega a producción. | **Tasa de fallo** porcentaje de cambios que provocan incidentes o requieren vuelta atrás. |
| **MTTR** tiempo medio para restaurar el servicio tras una falla. | **Hallazgos** vulnerabilidades críticas detectadas en el pipeline antes de producción. | **Cumplimiento** porcentaje de recursos que cumplen las reglas de AWS Config. |

**Fuente:** elaboración propia con base en Forsgren et al. (2018). Las dos últimas son métricas de seguridad complementarias.

## 3.4 Síntesis de la Parte 3

El análisis de riesgos muestra que la arquitectura cloud de Tech Consulting está bien protegida en las capas que gestiona el proveedor —hardware, hipervisor, centros de datos—, pero que los **riesgos más altos se ubican del lado de la empresa**: configuraciones incorrectas, credenciales comprometidas, *ransomware* e imágenes de contenedor vulnerables. La segmentación de red, la eliminación de puntos únicos de fallo y las copias inmutables reducen esos riesgos, pero sólo si se aplican y se mantienen de forma consistente.

Ahí aparece el valor de la **auditoría informática**. Con registros centralizados e inalterables, un plan que combina auditorías web, de código, de redes, de infraestructura y forenses, y controles automáticos continuos, la organización puede verificar que sus controles funcionan, detectar desvíos a tiempo y demostrar el cumplimiento de sus obligaciones de protección de datos.

Por último, la **integración DevOps + Cloud** transforma la seguridad de una revisión puntual en una práctica cotidiana. Un pipeline CI/CD con controles de seguridad, contenedores versionados e infraestructura inmutable hace que cada cambio sea pequeño, probado, trazable y reversible. Así se atacan en su origen varios de los riesgos identificados, al tiempo que se obtienen los beneficios de negocio buscados desde la Parte 1: escalabilidad, calidad, menor costo operativo y capacidad de responder a una demanda creciente.

En síntesis, riesgos, auditoría y DevOps no son temas aislados, sino un ciclo: se identifican los riesgos, se automatizan los controles en el pipeline, se audita su cumplimiento y lo aprendido vuelve a alimentar la gestión de riesgos.

PARTE 4

# Privacidad, DPO y amenazas

Política de privacidad, funciones del Data Protection Officer, ataques insider y outsider, estructura de facturación y cronograma de implementación.

4.1 Definición de políticas de privacidad
4.2 Funcionalidades del DPO
4.3 Tipos de ataques: insider y outsider
4.4 Estructura de billing
4.5 Cronograma de implementación
4.6 Síntesis de la Parte 4

Actividad Práctica Integradora 4 · Protección de datos y monitoreo

# 4.1 Definición de políticas de privacidad

## 4.1.1 Marco normativo de referencia

Todas las acciones que una empresa realiza sobre una nube, y las políticas que aplica el proveedor, deben regirse por lineamientos legales. Se distinguen dos niveles: las **políticas *cloud-centric***, que define Tech Consulting sobre sus propios datos y usuarios, y las **políticas del proveedor** (*cloud service provider-centric*), que AWS aplica sobre su infraestructura y documenta en sus acuerdos de tratamiento de datos.

**Tabla 4.1. Normativa aplicable a Tech Consulting**

| Norma | Ámbito | Aplicación en el caso |
|---|---|---|
| **Ley 25.326 de Protección de los Datos Personales** | Argentina | Marco principal: la empresa opera en el país. Establece principios de tratamiento, derechos de los titulares y requisitos para la transferencia internacional de datos. Su autoridad de control es la Agencia de Acceso a la Información Pública (AAIP). |
| **Reglamento General de Protección de Datos (GDPR)** | Unión Europea | Aplicable si los productos digitales tienen usuarios en la UE. Se adopta además como **estándar de buenas prácticas**: DPO, evaluaciones de impacto y notificación de brechas. |
| **Lei Geral de Proteção de Dados (LGPD)** | Brasil | Referencia si se atienden usuarios en Brasil; útil también porque la región de ejemplo de la arquitectura es São Paulo. |
| **Guía de Supervisión de Prevención de Pérdida de Información (BCRA)** | Argentina | Lineamiento técnico para organizar el DLP según el estado de los datos (en tránsito, en reposo, en equipos de usuarios y en servicios de terceros). |

**Fuente:** elaboración propia con base en los contenidos del módulo.

Como los datos se alojarán en una región de AWS fuera de la Argentina, la política debe contemplar el régimen de **transferencia internacional** de la Ley 25.326: verificar que el destino ofrezca un nivel de protección adecuado o, en su defecto, respaldar la transferencia con las garantías contractuales que admite la normativa.

## 4.1.2 Gobierno y clasificación de los datos

El *data governance* es un sistema de decisiones y responsabilidades sobre la información que define quién puede tomar qué acciones, con qué datos, cuándo y con qué métodos (Power Data, s. f.). Para Tech Consulting, esto responde directamente al problema de origen: hoy cada persona tiene sus propias planillas y criterios. La política de privacidad se apoya en una **clasificación de datos** en cuatro niveles, cada uno con un dueño (*data owner*) y controles mínimos.

**Tabla 4.2. Esquema de clasificación de la información**

| Nivel | Ejemplos en Tech Consulting | Controles mínimos |
|---|---|---|
| Público | Catálogo de productos, información comercial publicada. | Control de integridad; sin restricciones de lectura. |
| Interno | Listados de tiendas y categorías, métricas agregadas. | Acceso sólo para empleados autenticados; cifrado en reposo. |
| Confidencial | Datos de clientes y usuarios (nombre, correo, domicilio), datos de empleados, contratos. | RBAC por necesidad de conocer, cifrado en reposo y en tránsito, registro de accesos, DLP. |
| Restringido | Credenciales, claves de cifrado, datos sensibles (salud, origen, etc.) si existieran, información financiera. | Acceso nominal y aprobado, MFA, enmascaramiento, Secrets Manager / KMS, alertas ante cualquier acceso. |

**Fuente:** elaboración propia.

### 4.1.3 Política de privacidad básica de Tech Consulting

A continuación se presenta el modelo de política. Está redactada para ser publicada a usuarios y clientes, y a la vez sirve como compromiso interno.

DOCUMENTO MODELO

# Política de Privacidad y Protección de Datos Personales

Tech Consulting · Versión 1.0 · Vigencia: desde su aprobación por la Dirección · Revisión: anual

## 1. Objeto y alcance

Esta política establece cómo Tech Consulting recolecta, usa, almacena, comparte y protege los datos personales de clientes, usuarios de sus productos digitales, empleados y proveedores. Se aplica a todos los sistemas, incluidos los alojados en servicios de nube, y a todo el personal y terceros que traten datos en nombre de la empresa.

## 2. Responsable del tratamiento

Tech Consulting es responsable de las bases de datos que administra. Las consultas sobre privacidad se dirigen al Delegado de Protección de Datos (DPO) a través del canal indicado en la cláusula 13.

## 3. Datos que se recolectan

- **Identificación y contacto:** nombre, correo electrónico, teléfono y domicilio.
- **Datos de cuenta y uso:** credenciales (almacenadas de forma cifrada), preferencias y eventos de uso de los productos digitales.
- **Datos técnicos:** dirección IP, dispositivo, navegador y registros de seguridad.
- **Datos comerciales:** operaciones y transacciones con la empresa.

No se recolectan datos sensibles salvo que sean imprescindibles y con consentimiento expreso.

## 4. Finalidades

Prestar y mejorar los productos digitales; gestionar la relación comercial; elaborar métricas y análisis internos, preferentemente con datos agregados o seudonimizados; garantizar la seguridad de la plataforma y prevenir fraudes; y cumplir obligaciones legales. Los datos no se usarán para fines incompatibles con los informados.

## 5. Base legal y consentimiento

El tratamiento se realiza con el consentimiento libre, expreso e informado del titular o, cuando la ley lo permite, por la ejecución de un contrato o el cumplimiento de una obligación legal. El consentimiento puede revocarse en cualquier momento.

## 6. Principios

Tech Consulting trata los datos conforme a los principios de licitud, finalidad, **minimización** (sólo los datos necesarios), calidad y exactitud, seguridad y confidencialidad, y responsabilidad proactiva.

## 7. Almacenamiento y transferencias

Los datos se alojan en infraestructura de nube de Amazon Web Services, que actúa como encargado del tratamiento bajo un acuerdo de procesamiento de datos. Cuando el alojamiento implique una transferencia internacional, se realizará cumpliendo los requisitos de la Ley 25.326 y con garantías contractuales adecuadas. Los datos no se venden ni se ceden a terceros con fines comerciales.

## 8. Medidas de seguridad

Cifrado de los datos en reposo y en tránsito; control de acceso basado en roles con mínimo privilegio; autenticación multifactor; segmentación de redes; registro y auditoría de accesos; herramientas de prevención de pérdida de datos (DLP); copias de seguridad protegidas; y capacitación periódica del personal.

### 9. Conservación

Los datos se conservan sólo durante el tiempo necesario para la finalidad que motivó su recolección o el que exija la ley. Vencido ese plazo, se eliminan o se anonimizan de forma segura.

### 10. Derechos de los titulares

Los titulares pueden ejercer sus derechos de **acceso, rectificación, actualización, supresión, oposición y portabilidad**, en forma gratuita. Conforme a la Ley 25.326, el acceso se responde dentro de los 10 días corridos y la rectificación o supresión dentro de los 5 días hábiles de recibido el pedido. El titular puede, además, presentar reclamos ante la AAIP.

### 11. Encargados y terceros

Todo proveedor que trate datos por cuenta de Tech Consulting debe firmar un acuerdo que lo obligue a aplicar medidas de seguridad equivalentes, a usar los datos sólo para el servicio contratado y a permitir auditorías.

### 12. Incidentes de seguridad

Ante una brecha que afecte datos personales, la empresa activará su plan de respuesta, contendrá el incidente y, siguiendo el estándar del GDPR, notificará a la autoridad competente y a los afectados cuando corresponda, en un plazo objetivo no mayor a 72 horas desde su detección.

### 13. Contacto

Delegado de Protección de Datos (DPO): *privacidad@techconsulting.com* (dirección de ejemplo). Las solicitudes se registran y responden dentro de los plazos legales.

### 14. Actualizaciones

Esta política se revisa al menos una vez al año y ante cambios relevantes en los tratamientos, los sistemas o la normativa. Las modificaciones sustanciales se comunican a los titulares.

**Fuente:** elaboración propia con base en la Ley 25.326 y en los principios del GDPR. Modelo orientativo, sujeto a revisión legal.

## 4.1.4 Implementación técnica: DLP y remediación

Una política sin controles técnicos es sólo una declaración. La prevención de pérdida de datos (DLP) es la solución que busca evitar fugas de información cuyo origen está dentro de la propia organización, usando reglas de negocio para clasificar y proteger la información confidencial (Proofpoint, s. f.). El módulo distingue tres tipos, que se aplican así:

**Tabla 4.3. Tipos de DLP aplicados a la arquitectura**

| Tipo de DLP | Qué protege en Tech Consulting | Controles y herramientas |
|---|---|---|
| **DLP en redes** | Datos que circulan entre subredes, hacia Internet y por la VPN con las oficinas. | AWS Network Firewall con reglas de salida, VPC Flow Logs, duplicación de tráfico (*traffic mirroring*) para análisis puntual con Wireshark. |

| Tipo de DLP | Qué protege en Tech Consulting | Controles y herramientas |
|---|---|---|
| **DLP en almacenamiento** | Data lake en S3, bases RDS y archivos compartidos. | Amazon Macie para descubrir y clasificar datos personales en S3 (equivalente en AWS a Azure Purview); Lake Formation para permisos por columna; alertas ante buckets públicos. |
| **DLP en estaciones de trabajo** | Equipos de los empleados que hoy guardan planillas con datos. | Bloqueo de puertos USB, antivirus, cifrado de disco, listas de sitios permitidos, restricción de descargas de software, bloqueo de redes wifi públicas y gestión de contraseñas. |

**Fuente:** elaboración propia con base en Infotecs (2019).

Siguiendo la Guía del BCRA, las acciones de remediación se organizan según el estado del dato:

- **En tránsito:** TLS obligatorio, VPN cifrada y bloqueo de protocolos inseguros.
- **En reposo:** cifrado con AWS KMS, versionado, copias inmutables y descubrimiento periódico de datos personales.
- **En equipos de usuarios:** las planillas con datos personales se migran a la plataforma y se eliminan de los equipos; los controles de DLP de estaciones evitan nuevas copias.
- **En servicios de terceros:** inventario de proveedores, acuerdos de tratamiento y revisión de sus certificaciones.

Las buenas prácticas de DLP del módulo —priorizar y clasificar datos, monitorear de forma constante, analizar riesgos y formar a los empleados— quedan cubiertas por la clasificación (4.1.2), el monitoreo (4.3.4), la matriz de riesgos de la Parte 3 y el plan de capacitación a cargo del DPO.

# 4.2 Funcionalidades del DPO

## 4.2.1 El rol y su ubicación en la organización

De la mano del gobierno de datos surge el ***Data Protection Officer*** (DPO), o delegado de protección de datos: un especialista en el derecho de protección de datos que trabaja junto al responsable del tratamiento. Para Tech Consulting se proponen tres condiciones para que el rol sea efectivo:

CONDICIÓN 1

### Independencia

El DPO no recibe instrucciones sobre cómo ejercer sus funciones ni puede ser sancionado por cumplirlas.

CONDICIÓN 2

### Reporte a la Dirección

Informa directamente al máximo nivel de la empresa, no a las áreas que supervisa.

CONDICIÓN 3

### Participación temprana

Interviene desde el diseño de cada proyecto que trate datos personales, empezando por la migración.

CONDICIÓN 4

### Recursos y acceso

Cuenta con tiempo, presupuesto y acceso de lectura a registros y sistemas para poder supervisar.

Para evitar conflictos de interés, el DPO no debería ser a la vez quien decide los medios del tratamiento (por ejemplo, el CTO o el responsable de TI). En una empresa del tamaño de Tech Consulting, el rol puede cubrirse con una persona interna con dedicación parcial o con un servicio externo especializado.

## 4.2.2 Funciones aplicadas a Tech Consulting

**Tabla 4.4. Funciones del DPO y actividades concretas**

| Función (según el módulo) | Actividades concretas en Tech Consulting |
|---|---|
| **Informar y asesorar a la empresa y a sus empleados sobre sus obligaciones** | Aprobar la política de privacidad; asesorar a desarrollo y datos en cada nuevo tratamiento; dictar capacitaciones anuales y una inducción para cada nuevo empleado. |
| **Supervisar el cumplimiento de las políticas, la formación del personal y las auditorías** | Mantener el registro de actividades de tratamiento; revisar los permisos sobre datos confidenciales; participar en las auditorías definidas en la Parte 3 y dar seguimiento a los hallazgos. |
| **Gestionar la documentación y la notificación de fugas en un máximo de 72 horas** | Coordinar la respuesta ante brechas con el equipo de seguridad; evaluar la gravedad; redactar y enviar las notificaciones; llevar el registro de incidentes. |

| Función (según el módulo) | Actividades concretas en Tech Consulting |
|---|---|
| **Estudiar el impacto y supervisar las evaluaciones de impacto** | Liderar la evaluación de impacto (DPIA) de la migración y de cada nuevo producto digital; validar la clasificación de datos y las medidas de minimización. |
| **Cooperar con la autoridad de control y actuar como enlace** | Ser el punto de contacto con la AAIP; atender requerimientos y responder las solicitudes de los titulares dentro de los plazos legales. |

**Fuente:** elaboración propia con base en las funciones del DPO presentadas en el módulo.

### 4.2.3 Relación con los roles complementarios

El módulo menciona cuatro roles complementarios al DPO. La matriz RACI aclara quién hace qué en las actividades clave de privacidad: **R** = responsable de ejecutar, **A** = quien aprueba y rinde cuentas, **C** = consultado, **I** = informado.

**Tabla 4.5. Matriz RACI de privacidad**

| Actividad | DPO | CIO | CSO | CDIO | CTO | Cloud Architect |
|---|---|---|---|---|---|---|
| **Aprobar la política de privacidad** | R | A | C | C | I | I |
| **Clasificar los datos y asignar dueños** | C | A | C | R | I | C |
| **Implementar controles técnicos (cifrado, DLP, RBAC)** | C | I | A | I | C | R |
| **Evaluación de impacto (DPIA) de la migración** | R | A | C | C | C | C |
| **Responder a un incidente con datos personales** | R | I | A | I | C | C |
| **Atender solicitudes de los titulares** | A | I | I | R | C | I |

**Fuente:** elaboración propia. CIO: *Chief Information Officer*; CSO: *Chief Security Officer*; CDIO: *Chief Digital Information Officer*; CTO: *Chief Technology Officer*.

### 4.2.4 El DPO durante la migración

| Fase de la migración | Intervención del DPO |
|---|---|
| **Evaluación** | Inventario de datos personales en planillas, bases y microservicios; registro de tratamientos; inicio de la DPIA. |
| **Fundaciones seguras** | Validar que cifrado, RBAC, MFA y registros cumplan la política antes de mover datos. |

| Fase de la migración | Intervención del DPO |
|---|---|
| **Migración de datos** | Aprobar la región de alojamiento y las garantías de transferencia; verificar que se apliquen la minimización y la eliminación de copias en equipos de usuarios. |
| **Analítica** | Asegurar que las métricas usen datos agregados o seudonimizados cuando sea posible. |
| **Operación** | Auditorías periódicas, capacitación, revisión anual de la política e indicadores de cumplimiento. |

Indicadores sugeridos para el rol: porcentaje de solicitudes de titulares respondidas en plazo, porcentaje de empleados capacitados, cantidad de tratamientos con DPIA vigente, y tiempo entre la detección de un incidente y su notificación.

# 4.3 Tipos de ataques: insider y outsider

## 4.3.1 Conceptos y diferencias

Un ***insider***, o amenaza interna, es un riesgo que se origina dentro de la organización: una persona que trabaja o trabajó en ella y conoce sus sistemas. Un ***outsider*** es una persona ajena a la empresa, habitualmente un ciberdelincuente. Entre los atacantes externos suelen distinguirse los *white hat* (hackers éticos que reportan las vulnerabilidades), los *grey hat* (de ética ambigua, que ofrecen corregir fallas a cambio de dinero) y los *black hat* (que vulneran sistemas con fines económicos o personales), que son el perfil habitual del *outsider* (Juanes, 2017).

**Tabla 4.6. Comparación entre amenazas insider y outsider**

| Aspecto | Insider | Outsider |
|---|---|---|
| **Origen** | Empleados, ex empleados, contratistas, proveedores con acceso. | Ciberdelincuentes, grupos organizados, competidores. |
| **Acceso inicial** | Ya lo tiene: credenciales y permisos legítimos. | Debe obtenerlo: *phishing*, vulnerabilidades, configuraciones expuestas. |
| **Conocimiento** | Alto: sabe dónde están los datos valiosos. | Variable; debe hacer reconocimiento previo. |
| **Motivación** | Espionaje, venganza, ganancia personal, distracción o desconocimiento. | Económica (rescate, venta de datos), ideológica o de reputación. |
| **Detección** | Difícil: su actividad parece normal. | Más visible: genera anomalías de origen, volumen o comportamiento. |

| Aspecto | Insider | Outsider |
|---|---|---|
| **Control principal** | Mínimo privilegio, segregación de funciones, DLP, auditoría. | Perímetro, parches, MFA, detección de amenazas. |

**Fuente:** elaboración propia con base en Juanes (2017) y los contenidos del módulo.

## 4.3.2 Ataques insider en la migración

La migración es un momento de especial exposición: se mueven grandes volúmenes de datos, se otorgan permisos temporales amplios y conviven dos entornos. El módulo distingue tres tipos de *insiders*:

**Tabla 4.7. Escenarios de ataque interno y controles**

| Tipo | Escenario en Tech Consulting | Controles |
|---|---|---|
| **Malicioso o trabajador infiel** | Un analista copia planillas con datos de clientes a un pendrive antes de que se migren y eliminen. Un administrador con permisos amplios exporta una base o intenta borrar los registros. | DLP en estaciones (bloqueo USB), mínimo privilegio, permisos temporales con vencimiento, registros en cuenta separada e inmutable, alertas de Macie y CloudTrail ante exportaciones masivas. |
| **Participante involuntario** | Un empleado cae en un *phishing* y entrega sus credenciales, o sube por error un archivo con datos personales a un bucket público. | MFA resistente al *phishing*, capacitación, bloqueo de acceso público en S3, AWS Config y Macie. |
| **Cooperador necesario** | Un empleado o contratista facilita su acceso a un tercero externo a cambio de dinero. | Cuentas nominales, no compartir credenciales, detección de accesos desde ubicaciones o dispositivos inusuales (GuardDuty). |
| **Ex empleado** | Una persona desvinculada conserva accesos a la consola o a la VPN. | Baja de accesos (*de-provisioning*) el mismo día, identidades centralizadas y revisión periódica de usuarios activos. |

**Fuente:** elaboración propia.

## 4.3.3 Ataques outsider en la migración

**Tabla 4.8. Ataques externos según la etapa de la migración**

| Ataque | Etapa crítica | Objetivo | Controles |
|---|---|---|---|
| **Phishing y robo de credenciales** | Todas | Acceder a la consola de AWS o a cuentas de usuarios. | MFA, no usar la cuenta raíz, alertas por inicios de sesión anómalos. |
| **Explotación de configuraciones expuestas** | Durante y después | Encontrar buckets públicos, puertos abiertos o claves filtradas en repositorios. | Infraestructura como código revisada, AWS Config, escaneo de secretos en el pipeline. |

| Ataque | Etapa crítica | Objetivo | Controles |
|---|---|---|---|
| **Intercepción (*man-in-the-middle*)** | Durante | Capturar datos mientras viajan del centro de datos a la nube. | VPN IPsec, TLS en DMS y DataSync, verificación de integridad. |
| **Inyección SQL y ataques web** | Después | Extraer datos de las bases a través de los productos digitales. | AWS WAF, consultas parametrizadas, auditoría de código. |
| **Ransomware** | Después | Cifrar datos y copias para exigir un rescate. | Copias inmutables en cuenta separada, mínimo privilegio, pruebas de restauración. |
| **Denegación de servicio (DDoS)** | Después | Dejar fuera de línea los productos digitales. | AWS Shield, CloudFront, WAF y Auto Scaling. |
| **Cadena de suministro** | Todas | Introducir código malicioso mediante dependencias o imágenes de terceros. | Imágenes base aprobadas y escaneo de dependencias en el pipeline. |

**Fuente:** elaboración propia.

Un *outsider* que obtiene credenciales válidas se comporta, a partir de ese momento, como un *insider*. Por eso los controles de identidad y la detección de comportamientos anómalos protegen frente a ambos tipos de amenaza.

### 4.3.4 Monitoreo activo y pasivo para detectarlos

El **monitoreo activo** detecta en tiempo real eventos en aplicaciones, redes y servicios para evitar daños o robos de información. El **monitoreo pasivo** no es en tiempo real: se ejecuta en procesos *batch* o en momentos específicos. Ambos son necesarios y se complementan:

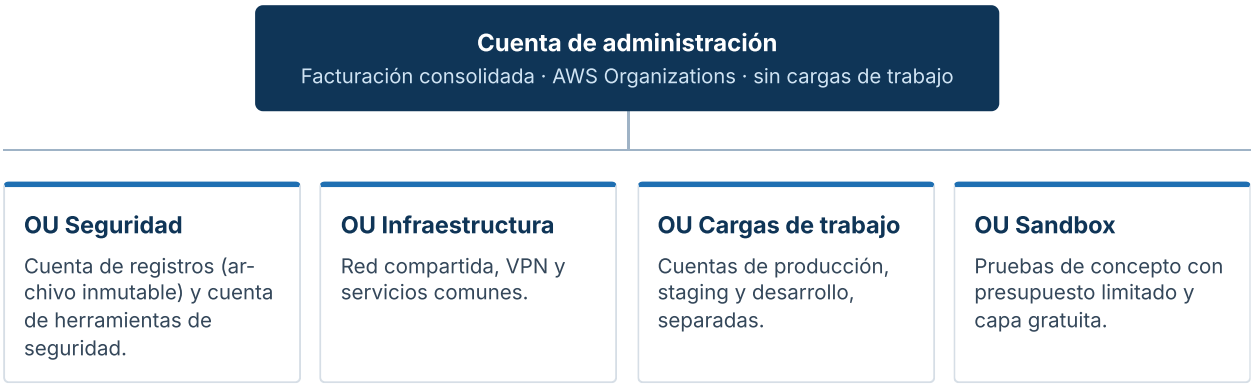
| Tipo | Herramientas en la arquitectura | Qué detecta |
|---|---|---|
| **Activo** | Alarmas de Amazon CloudWatch, Amazon GuardDuty, AWS WAF, alertas de CloudTrail. | Inicios de sesión sospechosos, uso de la cuenta raíz, tráfico malicioso, exportaciones masivas, ataques web en curso. |
| **Pasivo** | Trabajos programados de Amazon Macie, IAM Access Analyzer, consultas periódicas de registros con Amazon Athena, revisiones de accesos. | Datos personales en ubicaciones indebidas, permisos excesivos, cuentas inactivas, patrones que sólo aparecen al analizar períodos largos. |

Para una visión **multiplataforma** —por ejemplo, para integrar la red on-premise durante la etapa híbrida— pueden sumarse herramientas de código abierto como Prometheus, Grafana u OpenNMS, que consolidan métricas de distintos entornos en un mismo panel.

# 4.4 Estructura de billing

La facturación en la nube se basa en el pago por uso, lo que requiere una estructura que permita saber **quién consume qué y por qué**. Sin estimar montos, se propone la siguiente organización con AWS Organizations y facturación consolidada:

**Figura 4.1. Estructura de cuentas y facturación consolidada**




**Fuente:** elaboración propia con base en la documentación de AWS Organizations.

**Tabla 4.9. Componentes de la estructura de billing**

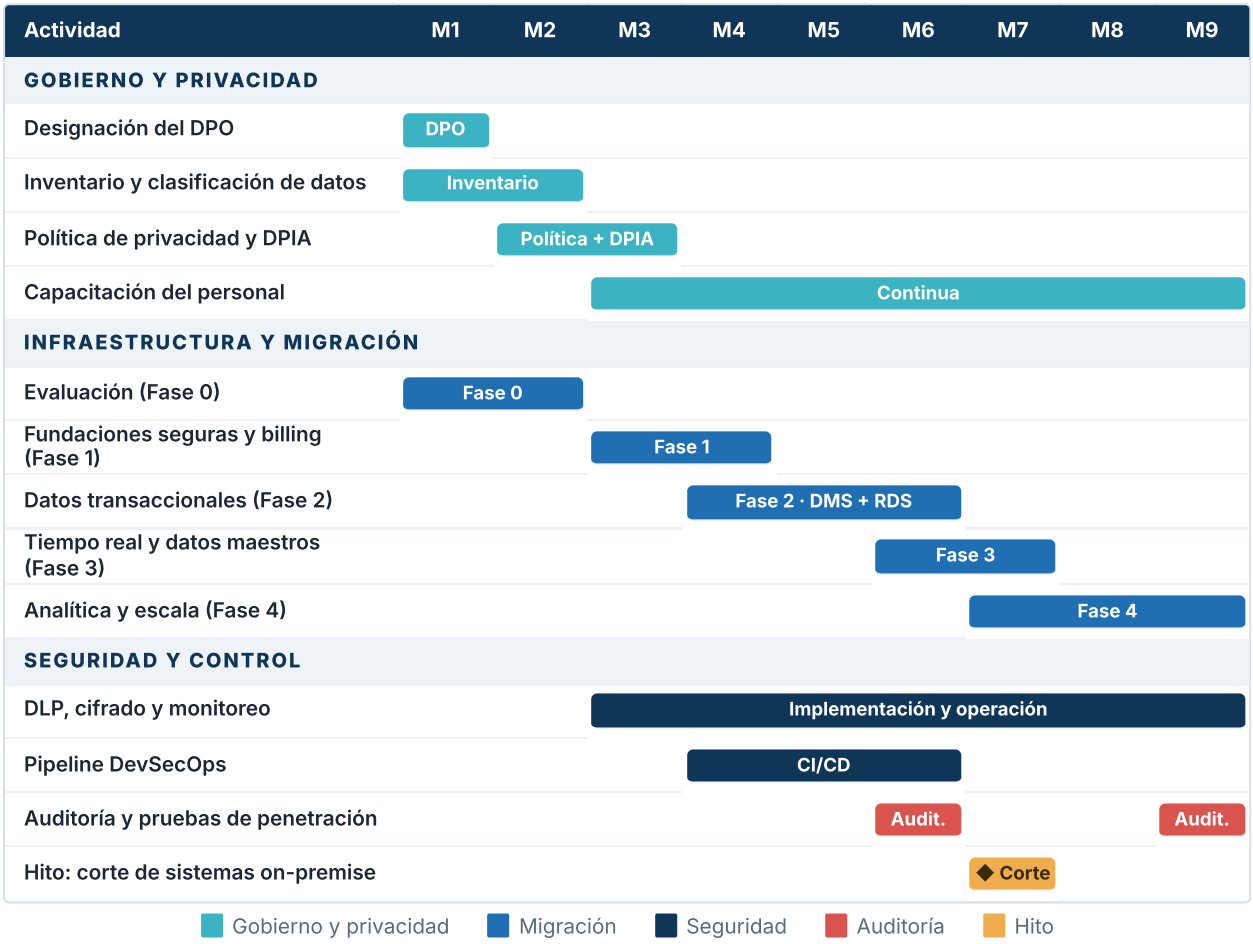
| Componente | Propósito |
|---|---|
| **Facturación consolidada** | Una única factura para todas las cuentas, con detalle por cuenta y descuentos por volumen compartidos. |
| **Etiquetas de asignación de costos** | Etiquetas obligatorias en cada recurso: `sistema`, `entorno`, `centro-de-costo` y `responsable`, para atribuir el gasto a cada área. |
| **AWS Budgets** | Presupuestos por cuenta y por sistema, con alertas al 50 %, 80 % y 100 % del valor definido. |
| **AWS Cost Explorer y detección de anomalías** | Análisis de tendencias y alertas ante consumos inusuales, que también pueden revelar un incidente de seguridad (por ejemplo, minería de criptomonedas). |
| **Políticas de control de servicios (SCP)** | Impedir el uso de regiones o servicios no aprobados, lo que limita el gasto y refuerza la seguridad. |
| **Responsables FinOps** | Revisión mensual del consumo entre finanzas, TI y cada área usuaria; ajuste de tamaño de recursos. |

Esta estructura también apoya la privacidad y la seguridad: la cuenta de registros queda aislada del resto, la de producción separada de las de prueba, y las alertas de costo funcionan como una señal adicional de actividad anómala.

# 4.5 Cronograma de implementación

El cronograma integra las fases técnicas definidas en las partes anteriores con las acciones de privacidad y seguridad de este trabajo. Los plazos están expresados en meses relativos al inicio del proyecto y son orientativos.

**Figura 4.2. Cronograma integrado de la migración**




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

La secuencia respeta un principio que atraviesa las cuatro partes: **ningún dato personal se migra antes de que existan la política, el DPO, la clasificación y los controles de seguridad**. La auditoría previa al corte verifica que esas condiciones se cumplan, y la del último mes valida la operación ya estabilizada.

## 4.6 Síntesis de la Parte 4

La migración de Tech Consulting a la nube no es sólo un cambio de infraestructura: al concentrar en una plataforma los datos que hoy están dispersos en planillas, bases aisladas y eventos que se pierden, la empresa asume una responsabilidad mayor sobre los datos personales de sus clientes, usuarios y empleados. La **política de privacidad** propuesta traduce esa responsabilidad en compromisos concretos —finalidades, principios, derechos de los titulares, medidas de seguridad, plazos— alineados con la Ley 25.326 y con las buenas prácticas del GDPR, y se sostiene en controles técnicos de DLP para redes, almacenamiento y estaciones de trabajo.

El **DPO** es la figura que mantiene viva esa política: asesora, supervisa, evalúa el impacto de cada nuevo tratamiento, gestiona los incidentes y actúa como enlace con la autoridad de control. Su independencia y su participación desde el diseño de la migración, junto con una distribución clara de responsabilidades con el CIO, el CSO, el CDIO y el CTO, evitan que la privacidad quede como una tarea de nadie.

El análisis de **ataques *insider* y *outsider*** muestra que las amenazas internas —maliciosas, involuntarias o facilitadas— son tan relevantes como las externas, y que la frontera entre ambas se diluye cuando un atacante externo obtiene credenciales válidas. Mínimo privilegio, MFA, DLP, registros inmutables y la combinación de monitoreo activo y pasivo protegen frente a ambos perfiles.

Como cierre de las cuatro partes, el plan para Tech Consulting queda completo: una problemática y objetivos claros, una arquitectura segura y escalable en AWS, una gestión de riesgos apoyada en auditoría y DevOps, y un marco de privacidad con responsables, estructura de costos y cronograma. La conclusión que atraviesa todo el trabajo es que, en la nube, **la seguridad y la protección de los datos son responsabilidad compartida, pero la responsabilidad sobre los datos personales nunca se delega**: es de la organización, y debe estar presente desde el primer día del proyecto.

# Conclusión general

El recorrido de las cuatro partes muestra que la migración de Tech Consulting a la nube no es un cambio de servidores, sino una transformación de cómo la empresa gestiona, protege y aprovecha su información. En la nube, la seguridad es compartida con el proveedor, pero la responsabilidad sobre la configuración, las identidades y los datos personales **nunca se delega**.

La **Parte 1** identificó que el problema de fondo es de gobierno de datos: la información existe, pero está fragmentada, carece de criterios comunes y no está protegida de forma consistente. La respuesta fue un plan en la nube pública de AWS, con servicios gestionados, un data lake con métricas únicas y una migración por fases que antepone la seguridad a los datos.

La **Parte 2** tradujo ese plan en una infraestructura concreta: una VPC segmentada en tres capas y dos zonas de disponibilidad, cómputo elástico, almacenamiento y bases gestionadas, y un esquema de monitoreo que convierte cada señal en una acción. Las mejores prácticas dejaron claro que la seguridad de la migración depende tanto del diseño como de la disciplina operativa.

La **Parte 3** sometió esa arquitectura a un análisis de riesgos y encontró que los riesgos altos —configuraciones incorrectas, credenciales comprometidas, *ransomware* e imágenes vulnerables— dependen de la empresa y no del proveedor. La auditoría informática y la cultura DevSecOps, con controles automáticos e infraestructura inmutable, son las herramientas para tratarlos de forma continua.

La **Parte 4** puso el foco en las personas y los datos personales: una política de privacidad alineada con la Ley 25.326 y el GDPR, un DPO independiente que la mantenga viva, controles contra amenazas internas y externas, una estructura de facturación que también aporta seguridad y un cronograma en el que ningún dato personal se migra antes de que existan las reglas y los controles.

### Principios que atraviesan todo el plan

| Principio | Cómo se aplica |
|---|---|
| **Seguridad por diseño** | La fase de fundaciones seguras precede a la migración de datos (Partes 1 y 4). |
| **Mínimo privilegio** | RBAC, roles temporales, subredes por capa y grupos de seguridad encadenados (Partes 2 y 3). |
| **Defensa en profundidad** | WAF, segmentación, cifrado, DLP, detección de amenazas y copias inmutables (Partes 2, 3 y 4). |
| **Diseño para la falla** | Multi-AZ, eliminación de puntos únicos de fallo y pruebas de restauración (Partes 2 y 3). |
| **Trazabilidad** | Registros centralizados e inmutables, auditoría continua y matriz de responsabilidades (Partes 3 y 4). |
| **Mejora continua** | Revisión Well-Architected, matriz de riesgos viva y ciclo DevSecOps (Partes 1, 2 y 3). |

# Referencias bibliográficas


Agencia de Acceso a la Información Pública. (s. f.). *Protección de datos personales*. https://www.argentina.gob.ar/aaip/datospersonales

Alvarado, G. (2021). *Beneficios y retos de la infraestructura inmutable + Tutorial: Packer, Ansible y Terraform*. https://galvarado.com.mx/post/beneficios-retos-y-como-lograr-infraestructura-inmutable-con-packer-ansible-y-terraform/

Amazon Web Services. (s. f.-a). *Almacenamiento en la nube de AWS*. https://aws.amazon.com/es/products/storage/

Amazon Web Services. (s. f.-b). *Amazon CloudWatch*. https://aws.amazon.com/es/cloudwatch/

Amazon Web Services. (s. f.-c). *Amazon EC2*. https://aws.amazon.com/es/ec2/

Amazon Web Services. (s. f.-d). *Amazon Macie*. https://aws.amazon.com/es/macie/

Amazon Web Services. (s. f.-e). *Amazon Virtual Private Cloud: Guía del usuario*. https://docs.aws.amazon.com/es_es/vpc/latest/userguide/

Amazon Web Services. (s. f.-f). *AWS Artifact*. https://aws.amazon.com/es/artifact/

Amazon Web Services. (s. f.-g). *AWS CloudTrail: Guía del usuario*. https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/

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

Amazon Web Services. (s. f.-i). *AWS Organizations: facturación consolidada*. https://docs.aws.amazon.com/es_es/awsaccountbilling/latest/aboutv2/consolidated-billing.html

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

Amazon Web Services. (s. f.-k). *Controlar el tráfico hacia los recursos mediante grupos de seguridad*. https://docs.aws.amazon.com/es_es/vpc/latest/userguide/VPC_SecurityGroups.html

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

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

Amazon Web Services. (s. f.-n). *¿Qué es DNS?* https://aws.amazon.com/es/route53/what-is-dns/

Andrés, R. (2017). *Qué es una máquina virtual, cómo funciona y para qué sirve*. Computer Hoy. https://computerhoy.com/noticias/software/que-es-maquina-virtual-como-funciona-que-sirve-46606

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

Banco Central de la República Argentina. (2020). *Guía de supervisión de prevención de pérdida de información (DLP)*. http://www.bcra.gov.ar/SistemasFinancierosYdePagos/prevencion-de-perdida-de-informacion.asp

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

Bejerano, P. (2017). *¿Para qué sirven los contenedores en software?* Think Big. https://blogthinkbig.com/para-que-sirven-los-contenedores-en-software

Castillo, J. (2018). *Qué es la virtualización y para qué sirve*. Profesional Review. https://www.profesionalreview.com/2018/11/05/que-es-virtualizacion/

Cisco. (s. f.). *¿Qué es el monitoreo de la nube?* https://www.cisco.com/c/es_mx/solutions/cloud/what-is-cloud-monitoring.html

¿Cómo cumplir con la GDPR? (2018). *Expansión*. https://expansion.mx/bespoke-ad/2018/06/08/como-cumplir-con-la-gdpr

DevOps, el nuevo lenguaje entre áreas de desarrollo y operaciones. (s. f.). *World EADAIT*. https://worldaedait.com.mx/devops-el-nuevo-lenguaje-entre-areas-de-desarrollo-y-operaciones/

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

Forsgren, N., Humble, J. y Kim, G. (2018). *Accelerate: The science of lean software and DevOps*. IT Revolution Press.

Hernández Caballero, L. (2018). *La nueva ley de protección de datos GDPR entrará en vigor el 25 de mayo*. https://blog.interdominios.com/la-nueva-ley-de-proteccion-de-datos-gdpr/

Hipervisor: el medio para la virtualización. (2020). *IONOS Digital Guide*. https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-hypervisor/

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

Información sobre Docker. (2022). *Microsoft*. https://docs.microsoft.com/es-es/dotnet/architecture/containerized-lifecycle/what-is-docker

Infotecs. (2019). *Data Loss Prevention – DLP*. https://infotecs.mx/blog/data-loss-prevention.html

Infotecs. (2019). *Gateway*. https://infotecs.mx/blog/gateway.html

Integración continua y entrega continua. (s. f.). *Aplyca*. https://www.aplyca.com/es/blog/integracion-continua-y-entrega-continua-cicd

Jiménez, J. (2021). *Qué es NAT y cómo actúa en nuestra red*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/que-es-nat-red/

Juanes, G. (2017). *[Infografía] ¿Quién es el ciberdelincuente? Del intrusismo a la maestría*. Cuadernos de Seguridad. https://cuadernosdeseguridad.com/2017/10/infografia-quien-es-el-ciberdelincuente-del-intrusismo-a-la-maestria/

Kubernetes: ventajas del gestor de contenedores. (2019). *IONOS Digital Guide*. https://www.ionos.es/digitalguide/servidores/know-how/que-es-kubernetes/

Ley 25.326 de Protección de los Datos Personales. (2000). Honorable Congreso de la Nación Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

López, A. (2019). *¿Qué es seguridad informática? Segmentación de redes de datos*. LinkedIn. https://www.linkedin.com/pulse/qu%C3%A9-es-seguridad-inform%C3%A1tica-segmentaci%C3%B3n-de-redes-datos-arturo-lopez

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/

Microsoft. (2022). *Introducción a las cuentas de almacenamiento*. https://docs.microsoft.com/es-es/azure/storage/common/storage-account-overview

Microsoft. (2022). *Qué es Azure Purview*. https://docs.microsoft.com/es-es/azure/purview/overview

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

Por qué es necesario hacer una auditoría de seguridad informática. (s. f.). *Blog de Seguridad para Empresas*. https://uss.com.ar/corporativo/auditoria-de-seguridad-informatica/

Power Data. (2018). *GDPR: lo que debes saber sobre el reglamento general de protección de datos*. https://www.powerdata.es/gdpr-proteccion-datos

Power Data. (s. f.). *Desmitificando el data governance: qué, cuándo, dónde y por qué*. https://www.powerdata.es/data-governance

Proofpoint. (s. f.). *Qué es DLP o prevención de pérdida de datos*. https://www.proofpoint.com/es/threat-reference/dlp

Puyol, J. (2022). *¿Qué es el data governance o gobernanza de datos?* Confilegal. https://confilegal.com/20161120-data-governance/

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

¿Qué es la segmentación de la red? (s. f.). *Palo Alto Networks*. https://www.paloaltonetworks.es/cyberpedia/what-is-network-segmentation

¿Qué es un malware?: Tipos y maneras de evitar ataques de este tipo. (2021). *Red Seguridad*. https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html

Qué es una auditoría de seguridad informática: tipos y fases. (2021). *Ambit*. https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases

Rackspace. (s. f.). *Qué es una nube privada virtual*. https://www.rackspace.com/es-ar/library/what-is-virtual-private-cloud

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (Reglamento General de Protección de Datos). (2016). *Diario Oficial de la Unión Europea*, L 119.

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/

Smaldone, J. (2008). *Virtualización de hardware*. https://blog.smaldone.com.ar/2008/09/20/virtualizacion-de-hardware/

SPOF Single Point Of Failure o punto simple de fallo. (s. f.). *HispaLinux*. https://www.ibiblio.org/pub/linux/docs/LuCaS/Presentaciones/200103hispalinux/paredes/html/x27.html

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

TECLAB Instituto Técnico Superior. (s. f.-b). *Seguridad en la Nube y Protección de Datos: Módulo 2. Infraestructura y servicios en la nube* [Material de cátedra].

TECLAB Instituto Técnico Superior. (s. f.-c). *Seguridad en la Nube y Protección de Datos: Módulo 3. Virtualización y contenedores* [Material de cátedra].

TECLAB Instituto Técnico Superior. (s. f.-d). *Seguridad en la Nube y Protección de Datos: Módulo 4. Protección de datos y monitoreo* [Material de cátedra].

VMware. (s. f.). *¿Qué es un hipervisor?* https://www.vmware.com/latam/topics/glossary/content/hypervisor.html