TECLAB

INSTITUTO TÉCNICO SUPERIOR

ACTIVIDAD PRÁCTICA INTEGRADORA · MÓDULO 4

Privacidad, DPO y ataques en la migración a la nube



Política de privacidad básica para Tech Consulting, funcionalidades del Data Protection Officer, ataques *insider* y *outsider*, estructura de facturación y cronograma de implementación.

ASIGNATURA	Seguridad en la Nube y Protección de Datos
CARRERA	Tecnicatura Superior en Seguridad Informática
ACTIVIDAD	Actividad 4 – Protección de datos y monitoreo
ESTUDIANTE	Juan Manuel Silva
LUGAR Y FECHA	Las Breñas, Chaco, Argentina · Octubre de 2026

Índice

Introducción 3

1. Definición de políticas de privacidad 4

1.1 Marco normativo de referencia 4

1.2 Gobierno y clasificación de los datos 4

1.3 Política de privacidad básica de Tech Consulting 5

1.4 Implementación técnica: DLP y remediación 7

2. Funcionalidades del DPO 9

2.1 El rol y su ubicación en la organización 9

2.2 Funciones aplicadas a Tech Consulting 9

2.3 Relación con los roles complementarios 10

2.4 El DPO durante la migración 10

3. Tipos de ataques: insider y outsider 11

3.1 Conceptos y diferencias 11

3.2 Ataques insider en la migración 12

3.3 Ataques outsider en la migración 12

3.4 Monitoreo activo y pasivo para detectarlos 13

4. Estructura de billing (opcional) 14

5. Cronograma de implementación (opcional) 15

6. Conclusiones 16

7. Referencias bibliográficas 17

Introducción

A lo largo de las actividades anteriores se diseñó la migración de **Tech Consulting** a Amazon Web Services (AWS): se planteó la problemática y los objetivos (Actividad 1), se definió la arquitectura de red, cómputo, almacenamiento y monitoreo (Actividad 2), y se analizaron los riesgos, la auditoría y la integración DevOps (Actividad 3). Esta última actividad se centra en las **personas y los datos personales**: qué reglas de privacidad deben regir la plataforma, quién vela por su cumplimiento y de quién hay que protegerla.

Se integran los contenidos del Módulo 4: prevención de pérdida de datos (DLP) en redes, almacenamiento y estaciones de trabajo; gobierno de datos (*data governance*); el rol del *Data Protection Officer* (DPO); los tipos de atacantes *insider* y *outsider*; las políticas *cloud-centric* y del proveedor; el GDPR y la Ley 25.326; las acciones de remediación propuestas por el BCRA, y el monitoreo activo y pasivo.

Al trasladar a la nube tres sistemas transaccionales, planillas con métricas comerciales y eventos de uso de productos digitales, la empresa pasará a concentrar en una sola plataforma datos de clientes, usuarios y empleados. Esa concentración es una ventaja para el negocio, pero también exige reglas claras y responsables definidos.

> **ALCANCE DEL TRABAJO**
>
> La propuesta es **conceptual** y no incurre en costos. La política de privacidad es un modelo básico que debería ser revisado por asesoría legal antes de publicarse. Se incluyen los dos puntos opcionales de la consigna —estructura de *billing* y cronograma—, sin estimar montos.

1 Definición de políticas de privacidad

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 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.

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 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.

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.

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 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 (1.2), el monitoreo (3.4), la matriz de riesgos de la Actividad 3 y el plan de capacitación a cargo del DPO.

2 Funcionalidades del DPO

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.

2.2 Funciones aplicadas a Tech Consulting

Tabla 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 Actividad 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.

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 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*.

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.

3 Tipos de ataques: insider y outsider

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 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.

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 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.

3.3 Ataques outsider en la migración

Tabla 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.

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:

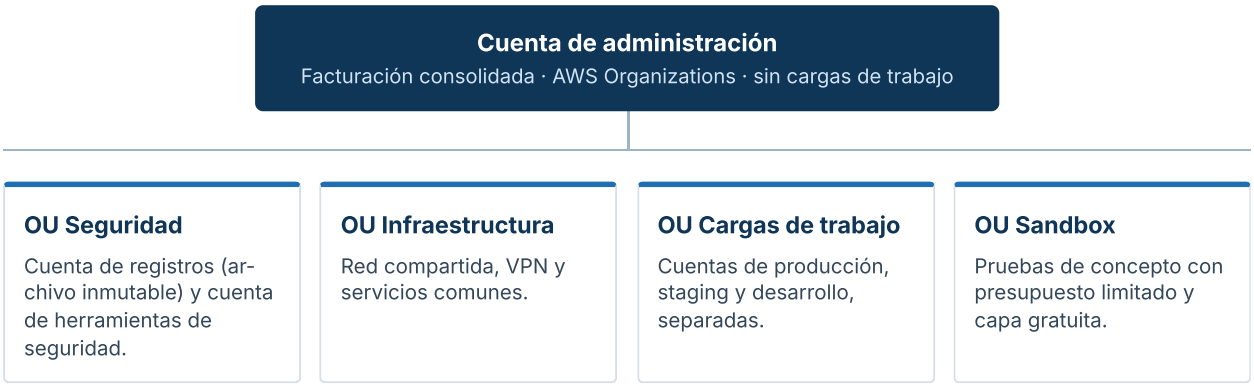
Tipo	Herramientas en la arquitectura	Qué detecta
Activo	Alarmas de Amazon CloudWatch, Amazon GuardDuty, AWS WAF, alertas de CloudTrail.	Inicios de sesión sospechosos, uso de la cuenta raíz, tráfico malicioso, exportaciones masivas, ataques web en curso.
Pasivo	Trabajos programados de Amazon Macie, IAM 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 Estructura de billing (opcional)

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 1. Estructura de cuentas y facturación consolidada



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

Tabla 9. Componentes de la estructura de billing

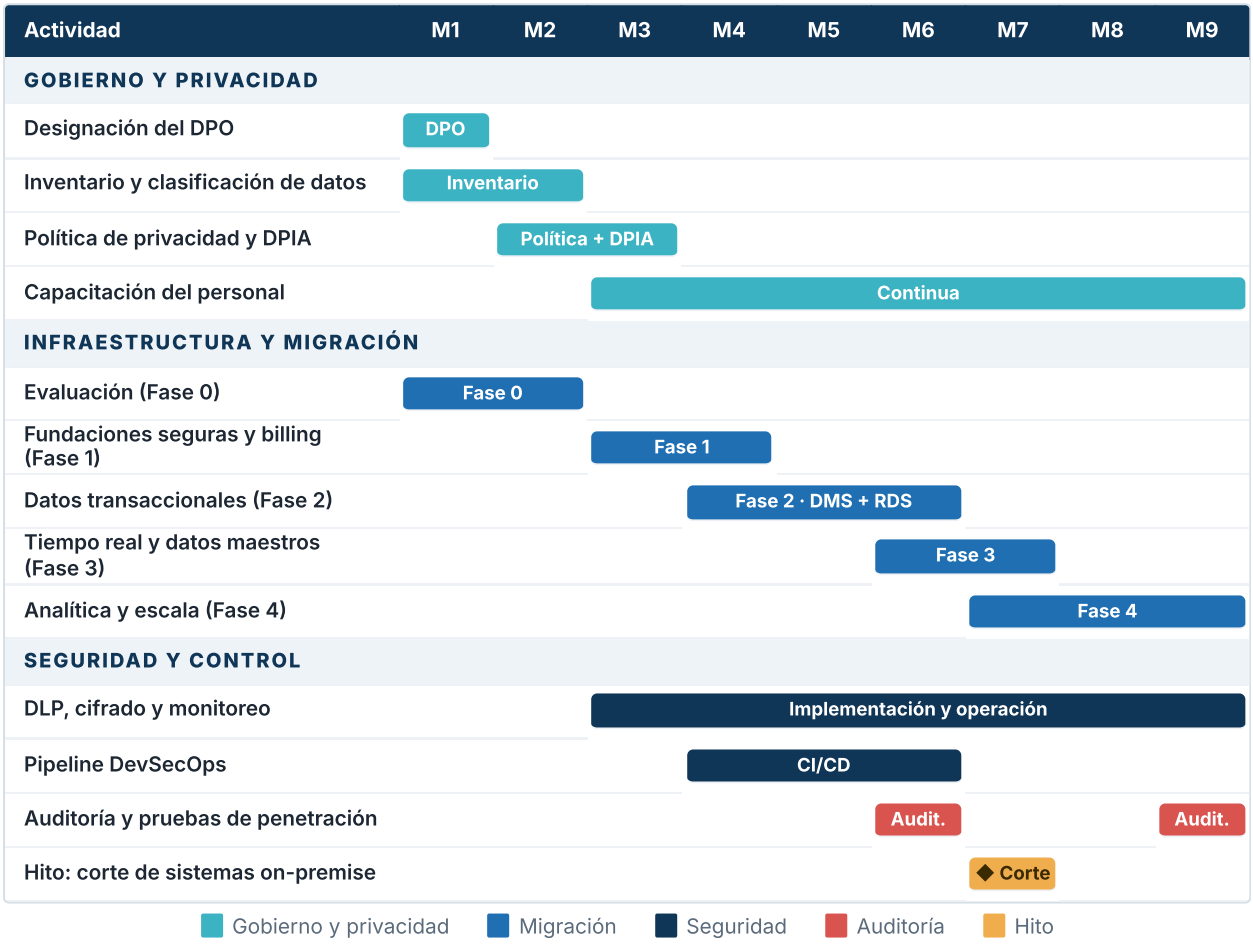
Componente	Propósito
Facturación consolidada	Una única factura para todas las cuentas, con detalle por cuenta y descuentos por volumen compartidos.
Etiquetas de asignación de costos	Etiquetas obligatorias en cada recurso: `sistema`, `entorno`, `centro-de-costo` y `responsable`, para atribuir el gasto 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.

5 Cronograma de implementación (opcional)

El cronograma integra las fases técnicas definidas en las actividades 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 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 actividades: **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.

6 Conclusiones

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 actividades, 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.

7 Referencias bibliográficas

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

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

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

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

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

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

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/

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

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/

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

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

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

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

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/

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.

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