TECLAB

INSTITUTO TÉCNICO SUPERIOR

ACTIVIDAD PRÁCTICA INTEGRADORA · MÓDULO 2

Arquitectura básica, servicios y monitoreo en AWS

Definición de la infraestructura de red, cómputo, almacenamiento y bases de datos para la migración de Tech Consulting, funcionalidades del monitoreo cloud y mejores prácticas a implementar.

ASIGNATURA	Seguridad en la Nube y Protección de Datos
CARRERA	Tecnicatura Superior en Seguridad Informática
ACTIVIDAD	Actividad 2 – Infraestructura y servicios en la nube
ESTUDIANTE	Juan Manuel Silva
LUGAR Y FECHA	Las Breñas, Chaco, Argentina · Octubre de 2026

Índice

Introducción 3

1. Arquitectura y descripción de los servicios de AWS 4

1.1 Criterios de diseño 4

1.2 Vista general de la arquitectura 5

1.3 Servicios de red 5

1.4 Servicios de cómputo 7

1.5 Servicios de almacenamiento 8

1.6 Servicios de bases de datos 9

1.7 Equivalencias multicloud y trazabilidad con el caso 9

2. Funcionalidades del monitoreo de sistemas cloud 10

2.1 Concepto y objetivo 10

2.2 Herramientas de monitoreo en AWS 11

2.3 Funcionalidades aplicadas a Tech Consulting 11

2.4 Ciclo de detección y respuesta 12

2.5 Ventajas del monitoreo cloud para el caso 12

3. Mejores prácticas para la migración a la nube 13

3.1 Planificación y fundaciones 13

3.2 Seguridad de red, identidades y datos 13

3.3 Ejecución de la migración 14

3.4 Operación, continuidad y costos 14

3.5 Lista de verificación 14

4. Conclusiones 16

5. Referencias bibliográficas 17

Introducción

En la Actividad 1 se planteó la problemática de **Tech Consulting** y se definieron los objetivos de su migración a la nube pública de Amazon Web Services (AWS). Este trabajo da el siguiente paso: define la **arquitectura básica de infraestructura** sobre la que se apoyará esa migración, describe los servicios que la componen, explica cómo se **monitoreará** el entorno y reúne las **mejores prácticas** a aplicar.

Se integran los contenidos del Módulo 2: la virtualización de hardware y el rol del hipervisor; las redes en la nube —grupos de seguridad, VPC, enrutamiento, NAT Gateway, Internet Gateway y DNS—; el procesamiento con máquinas virtuales; los servicios de almacenamiento; las bases de datos como servicio (DBaaS), y el monitoreo de sistemas cloud.

Recordemos brevemente el escenario: la empresa trabaja con planillas Excel como fuente de datos, tiene tres sistemas transaccionales sobre SQL Server, microservicios que generan eventos en tiempo real que no se capturan, información de referencia (tiendas y categorías) que no está en ningún sistema, y necesita escalar procesos y cómputo ante una demanda creciente.

> **ALCANCE DEL TRABAJO**
>
> Siguiendo la consigna, la propuesta es **conceptual**: no se despliegan recursos ni se incurre en costos. Las direcciones IP, los umbrales de alarma y los tipos de instancia son valores de ejemplo para ilustrar el diseño y deberían ajustarse en una evaluación detallada.

1 Arquitectura y descripción de los servicios de AWS

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

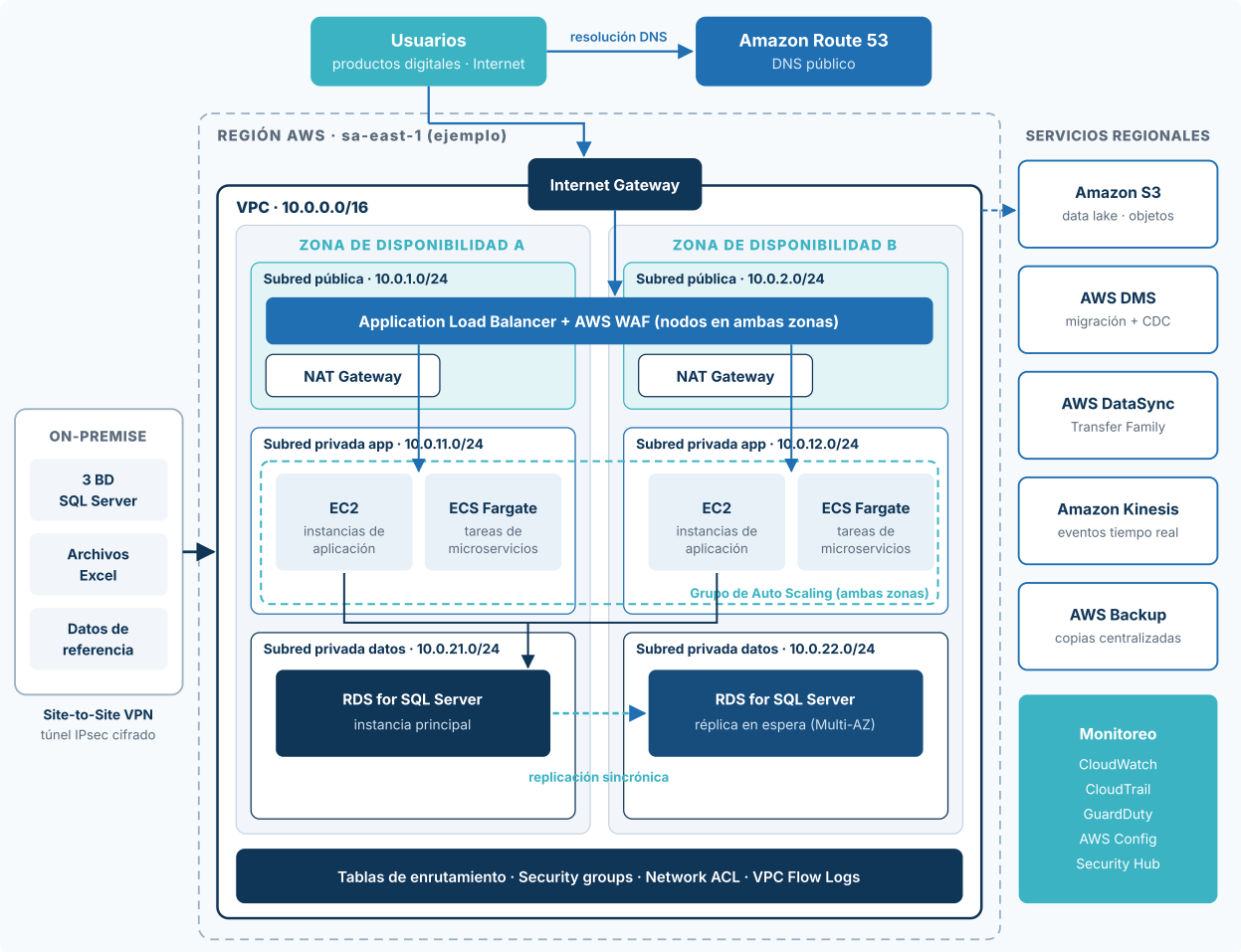
Mínimo privilegio en red e identidades, cifrado por defecto y monitoreo de todas las capas desde el primer día, no como un agregado posterior.

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.

1.2 Vista general de la arquitectura

La Figura 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 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.

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 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. 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 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.-d).

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.

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.-b).

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.

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).

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 Actividad 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.

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 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 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 Funcionalidades del monitoreo de sistemas cloud

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 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.

2.3 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 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.

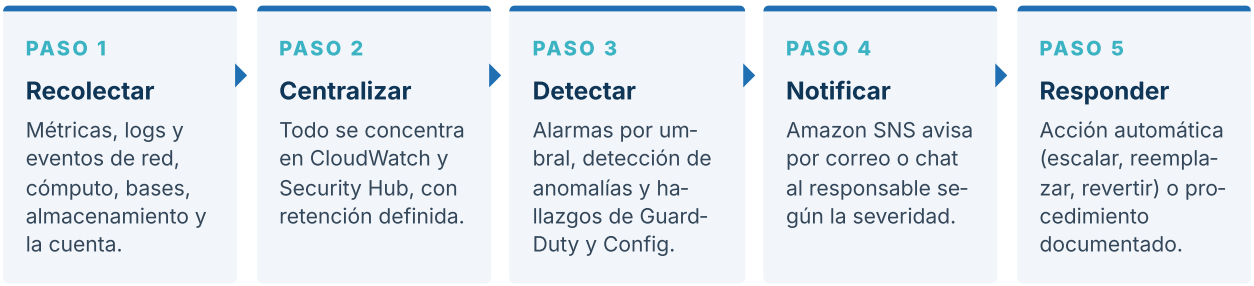
Fuente: elaboración propia con base en las funciones del monitoreo cloud del módulo.

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.

2.4 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. 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).

2.5 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.

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.

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.

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.

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.

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.

3.5 Lista de verificación

Tabla 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.-c).

4 Conclusiones

La arquitectura propuesta traduce los objetivos de la Actividad 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.

5 Referencias bibliográficas

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 EC2*. https://aws.amazon.com/es/ec2/

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

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

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

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

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

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

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

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

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

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

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

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

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