Autor

Xavier Alonso Lauca Uchupailla – Ingeniero Cloud & DevOps
Cuenca – Ecuador

1 ¿Cuál es la diferencia entre nube pública, privada e híbrida?

Tipo de Nube	Descripción	Ventajas	Caso en el sector financiero
Pública	Infraestructura en proveedores como AWS a la que acceden múltiples clientes.	Elasticidad, pago por uso, innovación rápida.	Aplicaciones de canales digitales (web/móvil), microservicios.
Privada	Infraestructura dedicada para una sola organización, on-premise o en un proveedor.	Control total, cumplimiento estricto.	Core bancario, sistemas regulados.
Híbrida	Combinación de ambas, recursos distribuidos.	Flexibilidad, continuidad del negocio.	Integración de sistemas bancarios internos con la nube.

2 Tres prácticas de seguridad en la nube

1 **Mínimo privilegio e IAM Seguro**

- Roles específicos para servicios y usuarios.
- MFA obligatorio para accesos administrativos.

2**Segmentación de red Zero-Trust**

- Subredes privadas para bases de datos y backend.
- Control de tráfico mediante Security Groups y NACLs.

3**Protección de secretos y cifrado obligatorio**

- Secrets Manager para credenciales.
- Cifrado con AWS KMS en S3, RDS y EBS.

La seguridad no es opcional: es parte del diseño.

3 ¿Qué es IaC? Beneficios + dos herramientas

Infrastructure as Code (IaC): Gestión de infraestructura mediante código versionado.

Beneficios:

- Menos errores humanos
- Despliegues consistentes y auditables
- Velocidad y automatización con CI/CD

Herramienta	Características
Terraform	Multi-cloud, sintaxis HCL, estado y planes de ejecución.
CloudFormation	Nativo AWS, YAML/JSON, integra StackSets y CodePipeline.

4 Métricas esenciales para monitoreo en la nube

Categoría	Métricas
Infraestructura	CPU, memoria, IOPS, tráfico de red.
Aplicación	Latencia p95/p99, errores HTTP 4xx/5xx.
Base de datos	Conexiones activas, locks, slow queries.
Seguridad	Intentos fallidos de acceso, actividades sospechosas.
Negocio	Transacciones por minuto, tiempo de respuesta al usuario.

5 ¿Qué es Docker? Componentes principales

Docker es una plataforma para **contenerizar y ejecutar aplicaciones** de forma aislada y portable.

Componentes:

- **Dockerfile**
- **Imagen Docker**
- **Contenedor**
- **Docker Engine**
- **Registry** (ej. ECR)

6 Diseño de la Arquitectura

La arquitectura propuesta para la aplicación Demo está diseñada bajo los principios de cloud-native, priorizando seguridad, disponibilidad, automatización y cumplimiento normativo

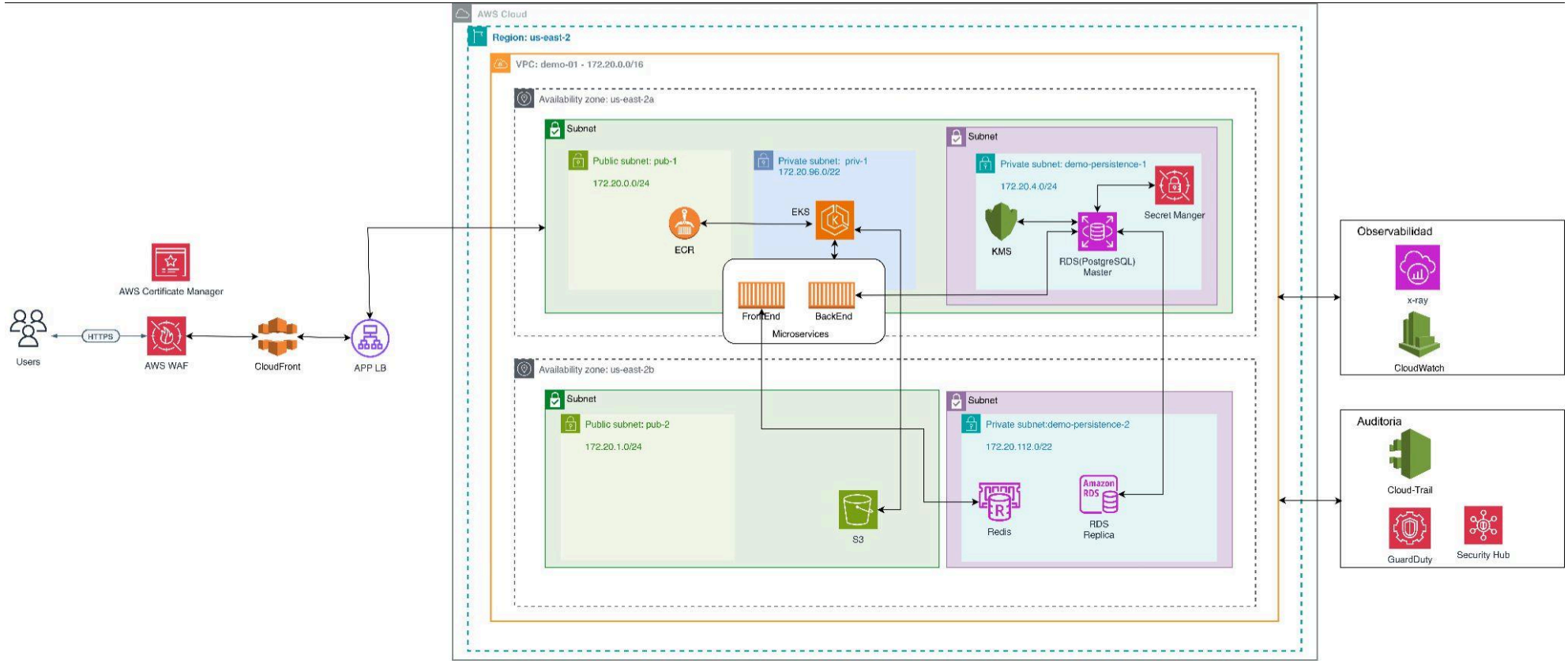
Utiliza AWS como proveedor de nube para garantizar:

- Escalabilidad automática ante variaciones de demanda
- Alta disponibilidad (Multi-AZ) y tolerancia a fallos
- Seguridad por diseño (Zero Trust + cifrado obligatorio)
- Automatización mediante IaC y CI/CD
- Observabilidad completa de infraestructura y aplicación

Componentes de la arquitectura en AWS

Capa	Servicio AWS	Descripción
CDN y seguridad web	**Amazon CloudFront + AWS WAF**	Entrega de contenido estático y dinámico con baja latencia y protección frente a ataques web (OWASP Top 10).
Balanceador	**Application Load Balancer (ALB)**	Termina TLS y distribuye tráfico hacia los contenedores frontend y backend.
Frontend	**Amazon EKS – FrontEnd**	Contenedores con la aplicación que atiende las solicitudes de los usuarios.
Backend	**Amazon EKS – Backend**	Microservicios en contenedores que exponen APIs REST/GraphQL y acceden a la capa de datos.

Base de datos	**Amazon Aurora PostgreSQL (RDS)**	Base de datos relacional en configuración Multi-AZ con backups automáticos y cifrado con KMS.
Cache	**Amazon ElastiCache for Redis**	Cache de lecturas frecuentes y almacenamiento de sesiones, mejora el rendimiento y reduce carga en la base de datos.
Almacenamiento de objetos	**Amazon S3 (buckets privados)**	Almacena imágenes y contenido estático. Acceso mediante roles IAM y presigned URLs.
Red	**Amazon VPC** con subredes públicas y privadas, Security Groups y NACLs	Segmentación de tráfico, exposición pública solo del ALB y componentes externos.
Secretos y cifrado	**AWS Secrets Manager + AWS KMS**	Almacenamiento seguro de contraseñas y claves, cifrado en reposo para S3, RDS y EBS.
Monitoreo y trazas	**Amazon CloudWatch + CloudWatch Logs + AWS X-Ray**	Métricas técnicas, logs centralizados, seguimiento de peticiones end-to-end.
Auditoría y seguridad avanzada	**AWS CloudTrail + Amazon GuardDuty + AWS Security Hub**	Registro de acciones sobre la cuenta, detección de amenazas y panel consolidado de seguridad.
IaC	**Terraform**	Define VPC, ECS, RDS, S3, WAF, IAM, etc. como código.
CI/CD	**AWS CodePipeline + CodeBuild** (o GitHub Actions)	Pipelines para build, test, seguridad y despliegue de infra y aplicaciones.


AWS Cloud
Region: us-east-2
VPC: demo-01 - 172.20.0.0/16
Availability zone: us-east-2a
Subnet
Public subnet: pub-1
172.20.0.0/24
Private subnet: priv-1
172.20.96.0/22
Subnet
Private subnet: demo-persistence-1
172.20.4.0/24
EKS
ECR
KMS
Secret Manger
RDS(PostgreSQL)
Master
FrontEnd
BackEnd
Microservices
Availability zone: us-east-2b
Subnet
Public subnet: pub-2
172.20.1.0/24
Subnet
Private subnet:demo-persistence-2
172.20.112.0/22
S3
Redis
RDS
Replica
AWS Certificate Manager
Users
HTTPS
AWS WAF
CloudFront
APP LB
Observabilidad
x-ray
CloudWatch
Auditoria
Cloud-Trail
GuardDuty
Security Hub