1. *¿Cuál es la diferencia entre nube publica, privada e hibrida?*
    a. *La nube privada implica que los recursos de la nube (Servidores, Almacenamiento, Redes, etc…) están dedicados a una sola organización o propietario, estos recursos mayormente están en un Data Center local y son compartidos por una red privada.*
    b. *Mientras que la nube publica la infraestructura esta alojada en un proveedor de servicios como Digital Ocean, Azure, Google o AWS, estos proveedores venden los servicios de la nube a través de internet.*
    c. *La nube hibrida no es más que la combinación de la nube privada y la nube publica de manera que la organización puede aprovechar las bondades de ambas.*
2. *Describa tres prácticas de seguridad en la nube*
    a. *Modelo de confianza cero: Este modelo se rige asumiendo que ningún acceso es confiable por defecto. Cada acceso debe ser verificado, para garantizar que quien intenta acceder es realmente quien debe tener permiso.*
    b. *Principio de privilegio mínimo: Este principio indica que cada entidad debe operar únicamente con los permisos mínimos necesarios para realizar sus funciones.*
    c. *Rbac: significa accesos basados en roles esto implica que debe haber grupos de roles con permisos específicos para realizar acciones específicas.*
3. *¿Qué es la IaC, y cuáles son sus principales beneficios?, Mencione 2 herramientas de IaC y sus principales características.*
    a. *IaC es la práctica Devops que te brinda la capacidad de gestionar (Eliminar, Crear, Modificar, etc…) la infraestructura TI a través de código, ya sea en la nube u on-premise, este código es guardado en archivos de configuración de manera que permite versionar el estado de la infraestructura.*
    b. *Las principales ventajas de IaC son las siguientes:*
        i. *Velocidad en la creación de ambientes.*
        ii. *automatización de la infraestructura.*
        iii. *Consistencia entre los ambientes o replicaciones.*
        iv. *Trazabilidad de los cambios en la infraestructura.*
        v. *Estandarización y versionado del código de la infraestructura.*
        vi. *Seguridad gracias a DevSecOps, análisis de las plantillas, entre otras.*
        vii. *Escalabilidad ya que permite crear o modificar n cantidad de ambientes con facilidad.*
    c. *Principales Herramientas IaC:*

        i. *Terraform*
            1. *Trabaja con múltiples proveedores de nube*
            2. *Usa lenguaje declarativo*
            3. *Modular*
            4. *Se puede automatizar la infra en flujo CI/CD*
            5. *Guarda el estado de la infraestructura en premisa o en la nube*
            6. *Archivos declarativos se pueden versionar*
            7. *Se puede trabajar en colaborativo usando git*
            8. *idempotentes*
            9. *Detección de cambios*
            10. *Permite ver los cambios antes de aplicarlos*
        ii. *CloudFormation*
            1. *Propietario de AWS*
            2. *Nativo para todos los servicios de AWS*
            3. *detección de cambios*
            4. *Usa lenguaje declarativo*
            5. *Aplica plantillas a través de distintas regiones o cuentas*
            6. *Se puede automatizar la infra en flujo CI/CD*
            7. *Se pueden usar plantillas versionadas desde git*
            8. *idempotentes*
            9. *Rollback automáticos*
            10. *Permite ver los cambios antes de aplicarlos*

11. *Manejo de dependencias*

iii. *Azure Bicep*

1. *Propietario de Azure*
2. *Nativo para todos los servicios de Azure*
3. *Usa lenguaje declarativo*
4. *Modular*
5. *Se puede trabajar en colaborativo usando git*
6. *idempotentes*
7. *Manejo de dependencias*
8. *Se puede automatizar la infra en flujo CI/CD*
9. *Azure administra el estado de la infraestructura*
10. *Permite ver los cambios antes de aplicarlos*

4. *¿Qué métricas considera esenciales para el monitoreo de soluciones en la nube? Las principales métricas a monitoreas son las siguientes:*
   a. *Latencia*
   b. *Trafico*
   c. *Errores*
   d. *Saturación*
   e. *Uso de Hardware (Disco, CPU, RAM)*
   f. *Logs*
   g. *Eventos de autoscaling*

5. *Que es Docker y cuales son sus componentes principales*

Docker es una aplicación creada para la gestión (creación, ejecución, descarga o publicación) de contenedores o imágenes. Los principales componentes son los siguientes:

- *Docker daemon*
- *Docker client*
- *Docker registry.*

6. *Caso practico*

Cree un diseño de arquitectura para una aplicación nativa de nube considerando los siguientes componentes:

Fronend: una aplicación web que los clientes utilizaran para navegación
Backend: Servicios que se comuniquen con la base de datos y el frontend
Base de datos: un sistema de gestión de base de datos que almacene información.
Almacenamiento de objetos: para gestionar imágenes y contenido estático.

Diseño

Seleccione un proveedor de servicios de nube (AWS, AZURE, GCP) y sustente su selección

Diseñe una arquitectura de nube. Incluya diagramas que representen la arquitectura y justifique sus decisiones de diseño

Plataforma Cloud Seleccionada

AWS:

He seleccionado AWS debido a que su especialidad son los microservicios y aplicaciones nativas en la nube.

Componentes:

- *Route 53*
- *CloudFront*

- *Buckets S3*
- *Api Gateway*
- *Aplication Load Balance*
- *ECS Cluster*
- *AWS RDS Aurora*
- *IAM*
- *SECURITY GROUP*
- *WAF*
- *HTTPS*
- *Secret Manager*
- *HSM*
- *CloudWatch*
- *X-Ray*
- *EventBridge*

Detalles de la arquitectónicas:

Frontend:

Route 53: para gestionar el dominio en la misma plataforma que la aplicacion

CloudFront para incluir CDN ayudando a reducir la latencia para los clientes y agregar una capa de seguridad con WAF.

Buckets S3 (Opcional Amplify) para Alojamiento del website y almacenamiento de objetos por el precio y es un servicio global, también permite versiona miento de archivos y políticas de acceso.

Tambien es ideal para una aplicación de tamaño mediana.

Backend:

ECS Fargate permite el despliegue de contenedores sin la necesidad de administrar EKS, está la opción de usar EKS siempre y cuando la empresa cuente con una gran cantidad de servicios en contenedores.

Base de datos:

RDS Aurora por su eficiencia superior, gestión de backups, failover, y almacenamiento.

Seguridad:

Subnets privadas para mayor seguridad del Backend y DB.

IAM para administrar permisos por roles.

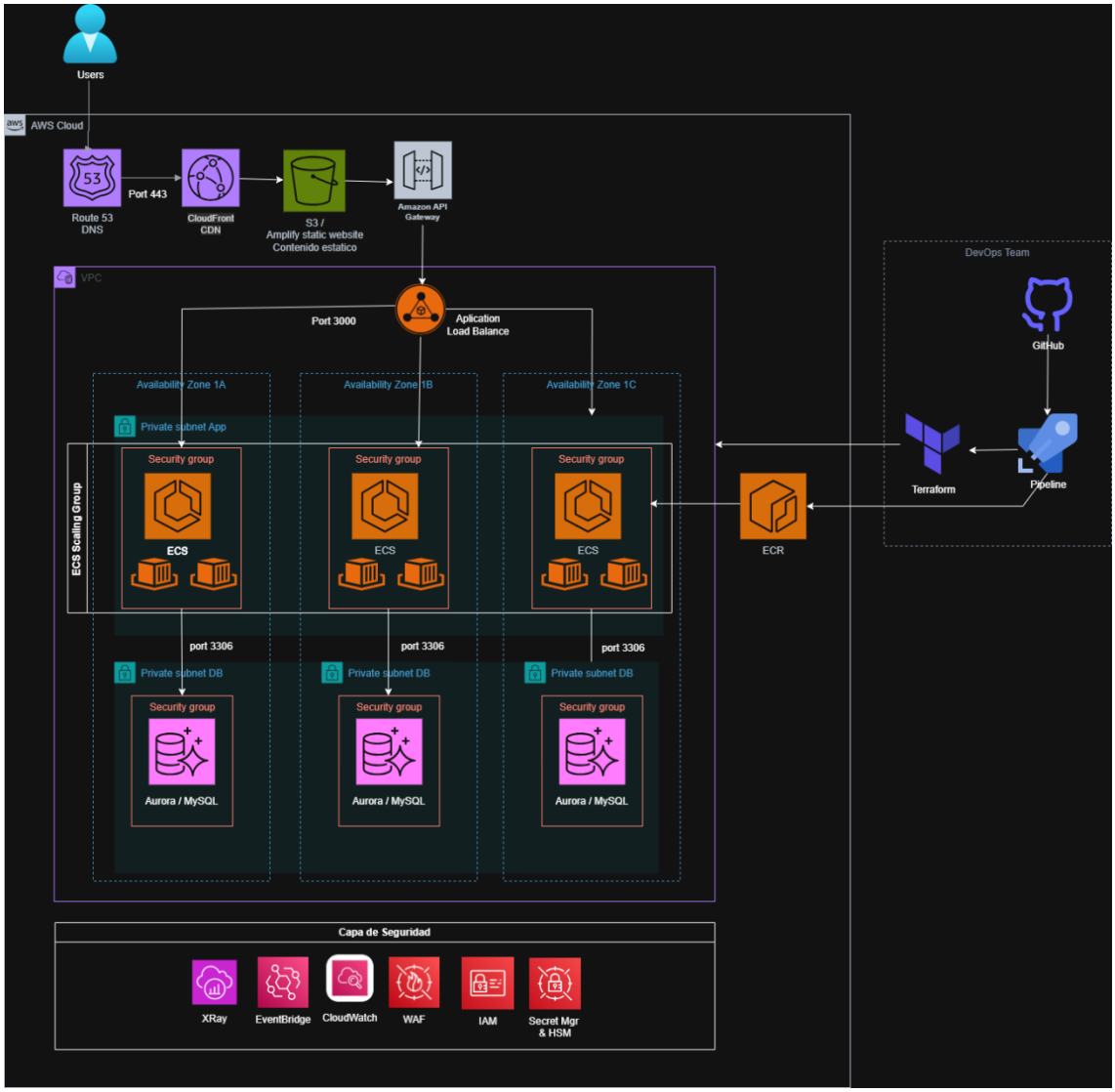
Grupo de seguridad en backend y DB permitiendo tráfico solo desde el ALB y limitar el acceso a la DB solo desde el Backend, Se han segmentado las subnet y los grupos de seguridad de las App y las DB de manera que haya segmentación por tipo de servicios.

Secret Manager y HSM para el almacenamiento seguro de credenciales y la encriptación de la DB

Monitoreo:

CloudWatch y X-Ray para el análisis de métricas y logs

Event Bridge para la automatización de acciones según los logs de la aplicación.


Users
AWS Cloud
Route 53
DNS
Port 443
CloudFront
CDN
S3 /
Amplify static website
Contenido estatico
Amazon API
Gateway
VPC
Port 3000
Aplication
Load Balance
Availability Zone 1A
Availability Zone 1B
Availability Zone 1C
Private subnet App
ECS Scaling Group
Security group
ECS
port 3306
Private subnet DB
Aurora / MySQL
ECR
DevOps Team
GitHub
Terraform
Pipeline
Capa de Seguridad
XRay
EventBridge
CloudWatch
WAF
IAM
Secret Mgr
& HSM