PROPUESTA EJERCICIO PRACTICO

PROPUESTA DE TECNICA

Preparado por:

Christian Yépez
christyepez@gmail.com

TABLA DE CONTENIDO

ANTECEDENTES

Consideraciones para el entregable:

- Cree un documento PDF donde se detallen las respuestas téoricas y el caso práctico.
- El documento debe estar bien organizado y ser fácil de leer. Asegúrese de añadir cualquier texto explicativo que considere necesario.
- Suba el documento como respuesta a este ejercicio. Asegúrese de subirlo dentro del tiempo de resolución.
- **Adicional, crear un repositorio público en Github y subir el PDF a ese repositorio. Colocar la URL al repositorio en los comentarios de este ejercicio.**

Preguntas teóricas:

1. ¿Cuál es la diferencia entre nube pública, privada e hibrida?
2. Describa tres prácticas de seguridad en la nube.
3. ¿Qué es la IaC, y cuáles son sus principales beneficios?, mencione 2 herramientas de iaC y sus principales características.
4. ¿Qué métricas considera esenciales para el monitoreo de soluciones en la nube?
5. ¿Qué es Docker y cuáles son sus componentes principales?
6. Caso práctico

Caso práctico

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

- Frontend: Una aplicación web que los clientes utilizarán para navegación.
- Backend: Servicios que se comunican 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 o GCP) y sustente su selección.
- Diseñe una arquitectura de nube. Incluya diagramas que representen la arquitectura y justifique sus decisiones de diseño (Utilice https://app.diagrams.net/).

PREGUNTAS TEÓRICAS

Cual es la diferencia entre uebe publica, privada e hibrida?

Diferencias:

- ***Nube publica***: es disponble para todo el mundo, pueden acceder a ella cualquier persona (ejemplo los servicios que ofrece Azure)
- ***Nube privada***: infraestrucutructura administrada por una empresa, esta disponible para las personas que tienen permisos de acceso a los servicios de la compania (ejemplo sarepoint corporativo de la empresa, aplicaciones propias)
- ***Nube hibrida***: es una combinacion mix de nube privada con nube publica.

Describa tres practicas de segurdad en la nube

- ***Gestion de identidades***: IAM, MFA a nivel de tenanat de cliente, controlar los accesos y permisos
- ***Cifrado de datos***: Control de los accesos no autorizados.
- ***Monitoreo***: Llevar la trazabilidad de los registros, transacciones que aydue a realizar el seguimiento de la infomracion, que ayude a identifiacar anomalias en la información.

Que es la Iac, y cuales son sis principales beneficios, mencionoe 4 herramientas de iaC, y sus principales caracateristicas

IaC, es la abreviacion de Infraestrucutra como codigo, esta permiste gestionar los recursos de manera automatica dentro de la organización.

Beneficion:

- Reducir el error humano
- Permite replicar la infraestrucutra y controlar los recursos.
- Se puede aprovicinar de manera rapida
- Se tiene trazabilidad de las acciones para el manejod e recursos.

Herramientas:

- Se puede utilizar **Terraform** es multinube
- **Ansible**, por medio de YAML es muy facil configurar
- CloudFormatio, es de AWS y puede manejar YAML o Json

Que meticas considera escenciales para el monitoreo de soluciones en la nube.

- **Uso de CPU, memoria y disco**: Indica el rendimiento y la salud de los servicios.
- **Tiempos de respuesta y latencia**: Clave para la experiencia del usuario.
- **Disponibilidad**: Medir la continuidad operativa.
- **Errores de aplicación**: Detecta fallos o mal uso.
- **Costos**: Control de gastos y eficiencia.

Que es docker y cuales son sus componente principales

Permite encapsular una solucion en un contenedor que dispone de toso los componentes para que sea operativo, estos son ligeros y funcionan de manera aislada

Componentes:

- **Docker File**, archivo de configuracion para el contenedor
- **Imagen**: Plantillas que utilizar para crear los contenedores
- **Contenedores**: Ejecutan las imágenes
- **Docker Engine**: Motor que ejecuta los contenedores

EJERCICIO PRÁCTICO DE ARQUITECTURA

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

- FronEnd: Una aplicación web que los clientes utilizaran para la navegacion.
- Backend: Servicios que se comunican con la base de datos y el frontend
- Base de datos: Un sistema de gestion de base de datos que almacene informacion
- Almacenamiento de objetos: para gestionar imágenes y contenido estatico

1. JUSTIFICACION ARQUITECTURA

Frontend

- **SPA (Single Page Application)**: Se recomienda el uso de **Angular** o **React** debido a su capacidad de manejar interfaces dinámicas, modularidad y reutilización de componentes.

Backend

- **Tecnologías sugeridas:** Net Core, Java (Spring Boot)
- **Contenerización:** Docker + Kubernetes (EKS, AKS, GKE)
- **Exposición de API:** API Gateway (Azure API Management)
- **Seguridad**: Autenticación JWT, validación de roles, WAF (Web Application Firewall)

Base de Datos

- **Opciones SQL:** Azure SQL Database, Postgress
- **Alta disponibilidad:** Multi-AZ / replicación automática
- **Backups** automáticos y encriptación en reposo y en tránsito

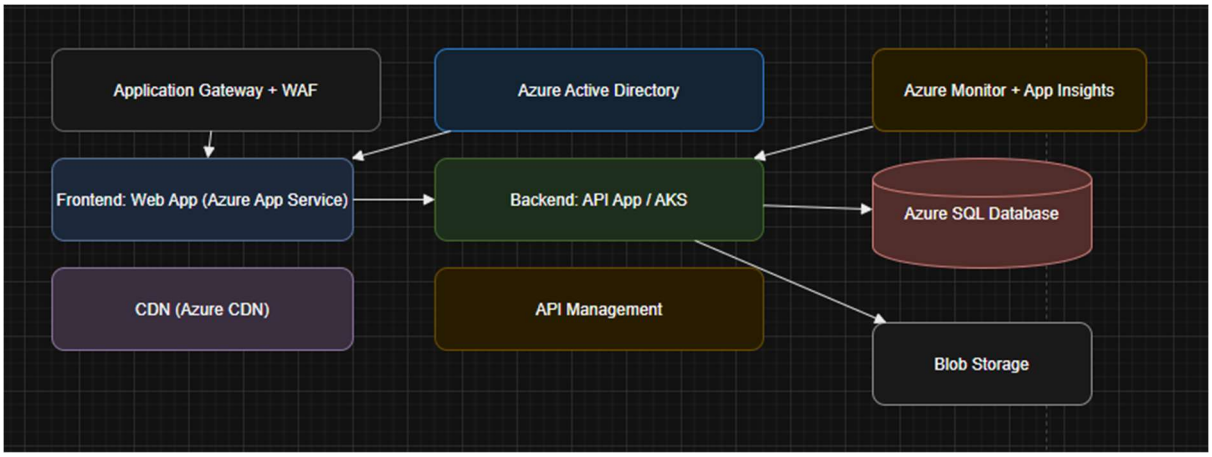
Almacenamiento de Objetos

- **Azure Blob Storage:** Para el manejo de imágenes, archivos estáticos del frontend, backups, etc**.**

Comunicación y Seguridad

- Azure Application Gateway + WAF, distribuye el tráfico de forma segura.
- Azure Active Directory B2C (si hay autenticación de usuarios)
- Azure Monitor + Application Insights: Para observabilidad, métricas y trazabilidad.

2. Diseño arquitectura



3. Autenticación y Autorización

- **OAuth 2.0 con OpenID Connect**
- Flujo recomendado: **Authorization Code Flow con PKCE** para garantizar máxima seguridad, evitando exposición de credenciales en el cliente.
- Onboarding con reconocimiento facial utilizando **Azure Face API** o **Face++**, con integración a un sistema de identidad gestionado.
- Métodos de acceso adicionales: **Huella digital, Face ID y autenticación multifactor (MFA)** con **Microsoft Authenticator**.

4. Persistencia de Información para Clientes Frecuentes

Se aplicará el **patrón Cache-aside**, donde los datos de clientes frecuentes se almacenarán en **Redis**, **herramientas Azure** mejorando tiempos de respuesta y reduciendo carga en la base de datos principal.

5. Notificaciones

- **Twilio**: Para envío de SMS y WhatsApp con mayor confiabilidad en mercados globales.
- **Firebase Cloud Messaging (FCM)**: Ideal para notificaciones en dispositivos móviles.

6. Infraestructura y Alta Disponibilidad

- **Despliegue en la nube**: Se recomienda **Azure** por su capacidad de escalabilidad global y cumplimiento de normativas.
- **Balanceadores de carga**: **Azure Load Balancer** o **NGINX** para distribución del tráfico.

- **Base de datos distribuida**: Uso de **Azure SQL Managed Instance** para alta disponibilidad.
- **Microservicios desacoplados** mediante colas de mensajes **RabbitMQ**, **Amazon SQS**, **Azure Service Bus** o **Apache Kafka**.

7. Seguridad y Normativas

- **Cifrado de datos en tránsito y en reposo** usando **TLS 1.3, AES-256**.
- **Cumplimiento de normativas**:
  - **ISO 27001**: Gestión de Seguridad de la Información.
  - **PCI DSS**: Protección de datos de tarjetas.
  - **GDPR y Ley de Protección de Datos Personales**: Protección de información personal.
  - **SOX**: Auditoría de transacciones financieras.
  - **OWASP Top 10**: Protección contra vulnerabilidades web.

8. Monitoreo y Recuperación ante Desastres

- **Logs centralizados** con **ELK (Elasticsearch, Logstash, Kibana)**, **Splunk** o **Datadog** para trazabilidad.
- **Alertas y monitoreo** con **Prometheus, Grafana o New Relic**.
- **Backups** automáticos y replicación en múltiples regiones con **Azure Backup**
- **Auto-healing** con **Kubernetes**, **Azure Scale Sets**.

9. Beneficios de la Arquitectura Propuesta

- **Escalabilidad**: Microservicios desacoplados permiten crecimiento modular.
- **Seguridad**: Autenticación robusta y cifrado.
- **Alta disponibilidad**: Balanceadores de carga, bases de datos distribuidas y monitoreo.
- **Baja latencia**: Uso de caché y servicios optimizados en la nube.

Esta arquitectura garantiza una solución segura, escalable y eficiente para la banca por internet de BP.