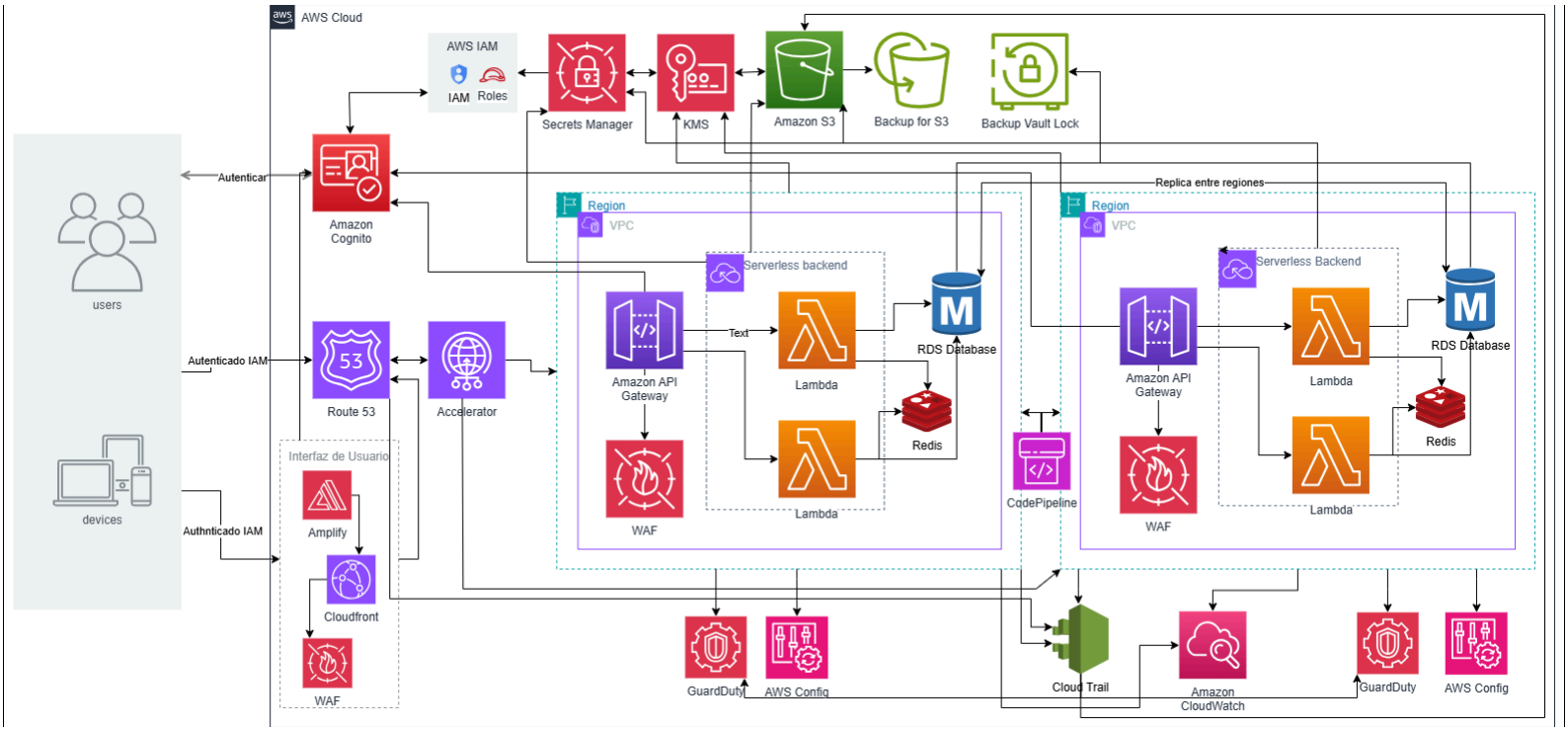
Tarea - Elementos de seguridad en empresa: On premise y Cloud

Henri Daniel Peña Dequero - Z3540462P

Diseño de Arquitectura de Seguridad en la Nube

Propuesta de arquitectura de seguridad en la nube orientada a un sistema empresarial de reservas de vuelos. Dado que la aplicación maneja información sensible —incluyendo datos personales de pasajeros y procesos de pago— el diseño se centra en proteger los tres principios fundamentales de la seguridad: **confidencialidad**, **integridad** y **disponibilidad**. La arquitectura se ha implementado siguiendo buenas prácticas reconocidas en AWS y adoptando un enfoque multi región para asegurar la disponibilidad ante fallos regionales.

1. Diagrama



2. Riesgos de seguridad principales

El sistema está expuesto a numerosos riesgos entre los que podemos encontrar:

- **Ataques de denegación de servicio (DDoS)** que puedan saturar los puntos de entrada y provocar indisponibilidad del servicio.
- **Filtración de datos sensibles** tanto por accesos no autorizados, robos de credenciales o exposición involuntaria de información almacenada.
- **Escalada de privilegios** donde un usuario con permisos limitados puede obtener acceso a recursos críticos del sistema.
- **Inyección de sql, código y ataques a nivel de aplicación**, especialmente contra las API expuestas públicamente.
- **Compromiso de claves o secretos** permitiendo accesos indebidos a bases de datos o servicios internos.
- **Fallos regionales** que pueden afectar la disponibilidad completa de una zona o región de AWS si no existe redundancia geográfica.
- **Modificación malintencionada de registros o acciones no auditadas**, afectando la integridad operativa del sistema.

Teniendo esto en cuenta base, se procede a seleccionar los controles de seguridad representados en el diagrama.

3. Descripción de los componentes de seguridad

La arquitectura presentada se distribuye en **dos regiones**, cada una con su propia **VPC privada**, lo que permite aislar la infraestructura crítica del tráfico público. Dentro de cada VPC se ubican las funciones Lambda en una arquitectura de software serverless, las bases de datos RDS y el clúster Redis, todos ellos inaccesibles directamente desde Internet. Esta segmentación reduce significativamente la superficie de ataque.

La **autenticación y autorización** de usuarios se gestiona mediante **Amazon Cognito**, en conjunto con **IAM Roles**, que definen permisos precisos por recurso y operación. Esto garantiza que tanto los usuarios finales como los servicios internos interactúan únicamente con los componentes autorizados y mitiga la **escala de privilegios**.

Como mecanismo de seguridad perimetral, cada región incorpora un **AWS WAF**, encargado de analizar el tráfico entrante, bloquear **solicitudes maliciosas**, prevenir intentos de **inyección** y detectar patrones de ataque conocidos. Junto a este componente, **AWS Route 53** y **AWS Global Accelerator** permiten dirigir el tráfico a la región óptima según **disponibilidad y latencia**, además de actuar como mecanismo de resiliencia ante un **fallo regional completo**.

El backend se implementa mediante **AWS Lambda**, adoptando un enfoque **serverless**. Este modelo contribuye directamente a la disponibilidad, ya que AWS gestiona automáticamente el **escalado horizontal**, distribuye la carga según demanda y aplica **parches de seguridad** sin intervención manual.

En cuanto al almacenamiento, cada región mantiene su propia instancia de **Amazon RDS**, configurada con un proceso de **replicación entre regiones** que asegura consistencia en los datos. Como complemento, **Amazon ElastiCache (Redis)** mejora el rendimiento del backend reduciendo tiempos de acceso a datos frecuentes. Tanto las bases de datos como los buckets de **Amazon S3** cuentan con **AWS Backup**, junto con un **Backup Vault Lock** que garantiza tener una copia inmutable haciendo uso de la **regla 3-2-1-1-0**, evitando modificaciones o eliminaciones accidentales o maliciosas manteniendo siempre disponible una copia íntegra.

La arquitectura hace un uso de **AWS KMS**, que se encarga del **cifrado de datos** en reposo y en tránsito, así como de la gestión de claves criptográficas asociadas a S3, RDS y otros servicios. Para la gestión de secretos se utiliza **AWS Secrets Manager**, que permite **rotación automática y almacenamiento** seguro bajo políticas estrictas de IAM.

El monitoreo del sistema se implementa mediante **AWS CloudTrail**, encargado de registrar todas las acciones realizadas dentro de la cuenta, facilitando auditorías completas; **Amazon CloudWatch**, que supervisa métricas operativas, comportamiento de las funciones Lambda y estado de los componentes; y **GuardDuty**, que analiza patrones de seguridad, detecta **comportamientos anómalos** y alerta ante **accesos o actividades sospechosas.**

Finalmente, la interfaz de usuario se entrega mediante **AWS Amplify**, distribuida con **CloudFront** para proporcionar baja latencia y disponibilidad global. Este frontal se integra de forma nativa con Cognito para garantizar la **autenticación** antes de interactuar con los recursos backend; y con WAF protegiendo contra ataques como **SQL injection y XSS**

---

4. Relación entre riesgos y medidas de mitigación

Cada riesgo identificado se encuentra vinculado a uno o varios controles de la arquitectura:

- **DDoS y ataques externos:** mitigados por WAF, distribución de tráfico con Route 53 + Global Accelerator y aislamiento mediante API Gateway.
- **Pérdida o robo de datos:** mitigado mediante cifrado con KMS, uso de VPC privadas, IAM Roles restrictivos y secretos almacenados en Secrets Manager.
- **Fallos regionales:** abordados con la arquitectura multi región, la replicación entre bases de datos y distribución global del tráfico con Route 53 y Accelerator.
- **Inyección y ataques a la capa de aplicación:** protegidos por WAF, validación de identidad con Cognito y aislamiento del backend.
- **Escalada de privilegios:** controlada mediante IAM con privilegios mínimos y auditoría continua con CloudTrail.
- **Manipulación o eliminación de backups:** evitada mediante la replicación de los datos entre regiones, y con Backup Vault Lock, que garantiza su inmutabilidad.
- **Actividades maliciosas o no autorizadas:** detectadas con GuardDuty y registradas mediante CloudTrail y CloudWatch.