RESOLUCIÓN DE RETO TÉCNICO – INGENIERO CLOUD

APLICANTE: MARIO FERNANDO VILLACRES MALDONADO

FECHA: 2026/01/03

PREGUNTAS TEÓRICAS:

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

   Nube pública, se refiere a modelo informático donde los proveedores de servicios en la nube ponen los servicios y recursos a disposición de las organizaciones a través del internet público

   Nube privada, se refiere al conjunto de componentes que conforman un entorno de computación dedicado a una sola organización.

   Nube Híbrida, hace referencia a un diseño de infraestructura que integra los recursos internos de una empresa (on-premise) con los servicios de proveedores de nube.

2. **Describa tres prácticas de seguridad en la nube**

   - Principio de mínimo privilegio en el acceso y autorización a los recursos, se basa en la práctica de otorgar solamente los permisos necesarios a los usuarios para la actividad o rol específico que tienen designado.
   - Mantener la encriptación de información, tanto en reposo como en tránsito, al mantener cifrada la información se agrega un nivel de seguridad para que en caso de que alguien intente acceder o interceptarla no pueda ser interpretable.
   - Identificación de amenazas de seguridad en tiempo real, manteniendo observación adecuada de estos eventos se puede tomar acción inmediata para mitigar, controlar y solucionar amenazas de seguridad.

3. **¿Qué es la IaC y cuáles son sus principales beneficios?, mencione 2 herramientas de IaC y sus principales características**

   Son las iniciales asociadas a la gestión de Infraestructura como código, usada para el aprovisionamiento y respaldo de la infraestructura, mediante el manejo de archivos con configuraciones logrando optimización de tiempo, reutilización de configuraciones y reducción de errores.

   - **AWS CloudFormation:** Se caracteriza por ser propio de AWS de uso gratuito, usa código JSON o YAML para la descripción de recursos y configuraciones de los componentes de la infraestructura, se puede integrar con el servicio IAM de AWS para autorizar la gestión de los recursos de infraestructura involucrados

- **Terraform:** Se consideara una solución multi nube para la gestión de los recursos de infraestructura como código, para los principales proveedores de servicios en la nube, usa lenguaje HCL, maneja planes de ejecución (pipelines) con gestión de estado para mapear el código con la infraestructura real.

4. **¿Qué métricas considera esenciales para el monitoreo de soluciones en la nube?**

   Rendimiento: Hace relación al consumo de recursos como procesamiento, memoria, latencia, etc.

   Disponibilidad: Cantidad de peticiones, tasa de códigos de respuesta, encolamientos, rechazo de peticiones por exceso de umbrales.

   Costos: La medición y análisis continuo de los costos involucrados para identificación de posibles optimizaciones del uso

   Seguridad: Identificación de actividades o cambios sospechosos que podrían estar relacionados a amenazas se seguridad.

5. **¿Qué es Docker y cuáles son sus componentes principales?**

   Es una plataforma que se basa en un sistema operativo para contenedores con la capacidad de virtualizar el hardware del servidor, los contenedores son paquetes de software livianos e independientes que contienen todo lo necesario para su ejecución actuando como máquinas virtuales portables.

   Dentro de los componentes principales se encuentran:

   - Consola de línea de comandos
   - El proceso dockerd que gestiona las imágenes, contenedores
   - Imágenes Docker
   - Contenedores
   - Repositorios Docker
   - Redes Docker
   - Volúmenes
   - Docker compose

6. CASO PRÁCTICO:

JUSTIFICACIÓN DE SELECCIÓN DE AWS COMO PROVEEDOR DE SERVICIOS EN LA NUBE:

El proveedor de nube seleccionado es AWS debido a la antigüedad en el mercado y en consecuencia mayor cantidad de casos de éxitos para entornos productivos para clientes a todo nivel como de documentación disponible.

DESCRIPCIÓN DE LA ARQUITECTURA PROPUESTA:

La arquitectura propuesta la nube de AWS está conformada por una Región (US-EAST1) y considerando una VPC en dos zonas de disponibilidad, dentro de las cuales se implementan instancias EC2 con auto escalado en grupo de 2 instancias tanto para la pareja de servidores front end como los servidores de Backend con su respectivo tier.

Conformando dos líneas de servicios en distintas zonas de disponibilidad balanceadas a través de Application Load Balancer, a las cuales, los clientes acceden usando la resolución de dominio Route 53, como mejora de seguridad se incorpora un WAF (Web Application Firewall) para mayor control de posibles ataques como inyecciones SQL, Cross-Site Scripting, DDoS.

Para la gestión de imágenes y contenido estático se usa Amazon S2 y para mejorar los tiempos de entrega de este contenido se incorpora AWS CloudFront.

Para el manejo de certificados digitales TLS, con el fin de mantener cifrada la información en tránsito se usa AWS Certificate Manager.

Las instancias EC2 de servidores web se comunican con las instancias EC2 de servidores de aplicación a través de application load balancer que permite el balanceo automático entre los nodos que se encuentren activos.

Las instancias EC2 de backend se integran al servicio RDS de Base de datos principal, y se implementa un segundo RDS en la 2da zona de disponibilidad como standby.

Se propone el uso de Amazon Cognito con user pool del servicio para autenticación de los usuarios o con la autenticación de usuarios federados mediante el User Identitty.

Para la observabilidad / monitore se usa CloudWatch como servicio nativo de AWS

Para el almacenamiento de información sensible como credenciales para autenticación de los servicios se propone AWS Secrets Manager y AWS Key Management Service para almacenamiento de claves de encriptación de datos sensibles en reposo

DIAGRAMA - ARQUITECTURA DE NUBE PROPUESTA: