Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 10**

1. Temas: **Getting started with databases, Cyber Security, Securing the cloud**

Integrante:

José Angel Quispe Meza
Matrícula: 390007
a390007@uach.mx

1. Resumen Tema "getting started with databases"

En el laboratorio Getting Started with Databases, aprendí sobre el uso y administración de servicios de bases de datos en AWS, destacando Amazon RDS (Relational Database Service). Este servicio facilita la configuración, operación y escalabilidad de bases de datos relacionales, como MySQL, PostgreSQL y SQL Server, sin necesidad de preocuparse por el mantenimiento de hardware o parches de software.

Otro punto importante fue la introducción a Amazon DynamoDB, una base de datos NoSQL completamente gestionada. Aprendí a configurar tablas para almacenar datos no estructurados, asegurando una alta disponibilidad y escalabilidad para aplicaciones modernas, como análisis en tiempo real o aplicaciones móviles. También se exploraron los beneficios de Amazon Aurora, que ofrece un rendimiento superior a los motores tradicionales, ideal para aplicaciones empresariales críticas.

El laboratorio incluyó ejercicios prácticos para comprender cómo conectar aplicaciones con bases de datos y cómo realizar consultas usando SQL y API compatibles. Además, se destacó la importancia de la automatización en la creación de copias de seguridad y la recuperación ante desastres, conceptos esenciales para mantener la integridad de los datos.

2. Resumen Tema "cyber security"

En los cursos breves de Cyber Security, adquirí conocimientos esenciales sobre las amenazas digitales más comunes y las mejores prácticas para proteger sistemas y datos. Aprendí sobre los conceptos básicos de ataques como phishing, ransomware y malware, así como estrategias de mitigación. También se destacó la importancia de la autenticación multifactorial (MFA) y el cifrado como barreras efectivas para salvaguardar la información confidencial.

El curso más extenso se enfocó en la implementación de controles de seguridad en sistemas empresariales. Se exploraron herramientas como AWS Identity and Access Management (IAM) para gestionar permisos de acceso y garantizar que solo usuarios autorizados puedan acceder a recursos específicos. Además, se resaltó el uso de la

arquitectura Zero Trust, que opera bajo el principio de "nunca confiar, siempre verificar", como una base sólida para la seguridad en entornos corporativos.

3. Resumen Tema “securing the cloud”

El curso Securing the Cloud se centró en las mejores prácticas para proteger entornos en la nube. Aprendí a implementar políticas de seguridad utilizando servicios como AWS CloudTrail, que permite registrar todas las actividades en una cuenta de AWS, y AWS Config, que monitorea cambios en los recursos y asegura el cumplimiento de normativas.

Otro tema clave fue la protección contra ataques DDoS (denegación de servicio distribuida) mediante AWS Shield y AWS WAF (Web Application Firewall). Estas herramientas ayudan a detectar y mitigar intentos de saturar sistemas y aplicaciones en la nube. Además, se destacó la importancia de establecer una red segura mediante Amazon VPC (Virtual Private Cloud), que proporciona aislamiento y control total sobre los recursos.

Un aspecto valioso fue la implementación de medidas proactivas, como la realización de auditorías de seguridad y la capacitación continua del personal. También se discutieron los beneficios del cifrado de datos en reposo y en tránsito, asegurando que la información esté protegida en todo momento.