COLOMBIA POTENCIA DE LA VIDA

TIC

BOOTCAMP ARQUITECTURA EN LA NUBE

EXPLORADOR- Módulo 2

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Contextualización de mis aprendizajes

En el mundo actual, donde la tecnología desempeña un papel fundamental en la mayoría de las operaciones comerciales y empresariales, la seguridad de los datos y la eficiencia en la gestión de recursos son aspectos críticos. En este contexto, Amazon Web Services (AWS) emerge como un líder indiscutible en la provisión de servicios en la nube, ofreciendo una amplia gama de soluciones que abarcan desde almacenamiento hasta computación y más allá.

El propósito del módulo 2 es sumergirse en el amplio espectro de servicios que ofrece AWS en las áreas de seguridad, redes e informática. Estos aspectos no solo son esenciales para comprender cómo funcionan los servicios en la nube de AWS, sino que también son fundamentales para garantizar la integridad, confidencialidad y disponibilidad de los datos en entornos en la nube.

Objetivo general

UNIDAD 1

- Reconocer el modelo de responsabilidad compartida
- Identificar la responsabilidad del cliente y de AWS
- Reconocer usuarios, grupos y roles de IAM
- Describir los diferentes tipos de credenciales de seguridad en IAM
- Identificar los pasos para proteger una nueva cuenta de AWS
- Explorar los usuarios y los grupos de IAM
- Reconocer cómo proteger los datos de AWS
- Reconocer los programas de conformidad de AWS

Competencias a desarrollar

- Comprender los conceptos fundamentales del modelo de responsabilidad compartida de AWS.
- Identificar las áreas de responsabilidad del proveedor (AWS) y del cliente (usuario).
- Distinguir claramente las responsabilidades que recaen en el cliente y en AWS en el contexto del modelo de responsabilidad compartida.
- Identificar y comprender el propósito de los usuarios, grupos y roles en AWS Identity and Access Management (IAM).

Competencias a desarrollar

- Comprender cómo se utilizan estos tipos de credenciales en diferentes contextos de autenticación y autorización en AWS.
- Reconocer los pasos y las mejores prácticas para proteger una nueva cuenta de AWS desde el momento de su creación.
- Identificar medidas de seguridad básicas, como la configuración de políticas de IAM, la activación de la autenticación multifactor (MFA), la configuración de alertas de seguridad, entre otros.
- Explorar y comprender cómo se gestionan usuarios y grupos en IAM a través de la consola de administración de AWS.
- Reconocer las medidas de seguridad disponibles en AWS para proteger los datos, como el cifrado, la gestión de claves, el control de acceso, etc.
- Identificar las mejores prácticas para proteger los datos en reposo y en tránsito en entornos de AWS.

Activación de saberes previos

TIEMPO DE EJECUCIÓN: 12 HORAS

PLANTEAMIENTO DE LA SESIÓN	MATERIALES
Lección 1 Introducción al Modelo de Responsabilidad Compartida de AWS Objetivo de Aprendizaje: Comprender los conceptos básicos del Modelo de Responsabilidad Compartida de AWS y su importancia en la seguridad de los servicios en la nube. Actividad: El mentor proporcionará una introducción al Modelo de Responsabilidad Compartida de AWS, explicando los roles y responsabilidades tanto del proveedor (AWS) como del cliente (usuario). Se discutirán ejemplos concretos de cómo se aplica este modelo en la práctica y cómo afecta a la seguridad y gestión de los servicios en la nube. **Lección 2 Definición de IAM y Demostración de IAM en AWS** Objetivo de Aprendizaje: Familiarizarse con el servicio IAM de AWS y comprender cómo se utiliza para gestionar identidades y accesos de forma segura en la plataforma. Actividad: Demostración grabada. Los estudiantes verán una demostración grabada que muestra cómo navegar por la consola de administración de AWS y configurar políticas de IAM. Se destacarán las características clave de IAM, como la creación de usuarios, grupos, roles y políticas, así como la asignación de permisos. Laboratorio Práctico: Configuración de IAM en la Consola de Administración de AWS Objetivo de Aprendizaje: Aplicar los conocimientos adquiridos sobre IAM en un entorno práctico mediante la configuración de usuarios, grupos, roles y políticas en la consola de administración de AWS. Actividad: Laboratorio práctico. Los estudiantes completarán una serie de tareas guiadas en la consola de administración de AWS para configurar IAM. Esto incluirá la creación de usuarios, la asignación de políticas, la creación de grupos y la asignación de usuarios a grupos, así como la configuración de roles.	• Simulador de políticas de IAM • Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2. • Demostración de IAM • Tareas que requieren credenciales de usuario raíz - AWS Identity and Access Management (amazon.com) • Configuración de IAM - AWS Identity and Access Management (amazon.com) • Configuración del acceso a una API protegido por MFA - AWS Identity and Access Management (amazon.com) • Integraciones y servicios admitidos de CloudTrail - AWS CloudTrail (amazon.com) • Creación de informes de costes y uso - Informes AWS Cost and Usage Reports (amazon.com) • Habilitar todas las características en la organización - AWS Organizations (amazon.com)

PLANTEAMIENTO DE LA SESIÓN	MATERIALES
Lección 3 Protección de Datos en AWS y Trabajo para Garantizar la Conformidad Objetivo de Aprendizaje: Comprender cómo se protegen los datos en AWS y cómo se trabaja para garantizar la conformidad con los estándares de seguridad y regulaciones. Actividad: Presentación y discusión en grupo. Se presentarán las medidas de seguridad y las mejores prácticas para proteger los datos en AWS, como el cifrado, la gestión de claves, y el cumplimiento de normativas. Se discutirán los desafíos y estrategias para garantizar la conformidad con estándares como GDPR, HIPAA, PCI-DSS, entre otros. **Lección 4 Servicios y Recursos de Seguridad Adicionales en AWS** Objetivo de Aprendizaje: Explorar los servicios y recursos de seguridad adicionales disponibles en AWS para reforzar la protección de los datos y los sistemas. Actividad: Presentación y estudio de caso. Se presentarán servicios adicionales de seguridad en AWS, como AWS WAF (Web Application Firewall), AWS Shield, AWS Security Hub, entre otros. Se analizarán casos de uso y ejemplos de cómo estos servicios pueden ser utilizados para mejorar la seguridad en la nube. **Revisión de Conocimientos:** Objetivo de Aprendizaje: Evaluar la comprensión de los conceptos clave abordados en la unidad. Actividad: Cuestionario o Evaluación. Los estudiantes completarán un cuestionario o evaluación que cubra los temas discutidos en el módulo, incluyendo el Modelo de Responsabilidad Compartida, IAM, protección de datos, conformidad y servicios de seguridad adicionales. Esto ayudará a consolidar el aprendizaje y a identificar áreas de mejora o conceptos que requieren mayor clarificación.	• Administración de políticas en AWS Organizations - AWS Organizations (amazon.com) • Características | AWS Key Management Service (KMS) | Amazon Web Services (AWS) • Conformidad con HIPAA – Amazon Web Services (AWS) • Documentación de AWS WAF (amazon.com) • Cómo los servicios de AWS usan AWS KMS - AWS Key Management Service (amazon.com) • Cifrado de datos en tránsito - Cifrado de datos de archivos con Amazon Elastic File System • Programas de conformidad – Amazon Web Services (AWS) • Servicios en el ámbito: Amazon Web Services (AWS) • RGPD – Amazon Web Services (AWS)

COLOMBIA POTENCIA DE LA VIDA

TIC

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira