COLOMBIA POTENCIA DE LA VIDA

TIC

BOOTCAMP ARQUITECTURA EN LA NUBE

INTEGRADOR- MÓDULO 2

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Contextualización de mis aprendizajes

Aquí se explican diversos aspectos relacionados con la protección de la infraestructura en entornos informáticos. Se abordan conceptos fundamentales de seguridad de la información tales como la identificación de amenazas, la evaluación de riesgos y la implementación de medidas de seguridad adecuadas.

Además, se abordan, específicamente, los desafíos y las soluciones relacionadas con la seguridad en la nube; a medida que las organizaciones migran sus servicios y datos a entornos de nube pública, privada o híbrida, surgen nuevas consideraciones de seguridad que deben ser comprendidas y atendidas de manera efectiva. En estas lecciones se exploran las mejores prácticas, herramientas y técnicas para fortalecer la seguridad en los entornos informáticos, garantizando así la integridad, confidencialidad y disponibilidad de los recursos.

Al finalizar este módulo, los participantes estarán mejor preparados para enfrentar los desafíos de seguridad en la infraestructura informática, adquiriendo un enfoque proactivo y centrado en la prevención; podrá implementar y mantener un entorno seguro que proteja los activos digitales de una organización y garantice su continuidad operativa en un mundo cada vez más interconectado y amenazante.

Objetivo general

UNIDAD 1

- Definir los componentes de una nube virtual privada (VPC).
- Reconocer los límites de la cuenta.
- Describir los servicios de Amazon Web Services (AWS) disponibles para proteger su red y sus recursos.

Competencias a desarrollar

- Comprensión conceptual: explica de manera clara y concisa qué es una nube virtual privada (VPC) y cómo funciona.
- Identificación de componentes: reconoce y describe los elementos fundamentales que constituyen una VPC, como subredes, tablas de enrutamiento, grupos de seguridad y gateways.
- Diseño de VPC: diseña y configura una VPC según los requisitos específicos de una organización, teniendo en cuenta aspectos como la conectividad, la seguridad y la escalabilidad.
- Conocimiento de los límites: se familiariza con los límites establecidos por los proveedores de servicios en la nube, como AWS, en términos de recursos y servicios disponibles para cada cuenta.

Competencias a desarrollar

- Monitoreo y gestión: identifica y monitorea los límites de la cuenta para evitar posibles interrupciones en el servicio debido a la superación de estos límites.
- Planificación y optimización: desarrolla habilidades para planificar y optimizar el uso de los recursos dentro de los límites de la cuenta, maximizando la eficiencia y minimizando los costos.
- Conocimiento de los límites: entiende los límites establecidos por los proveedores de servicios en la nube, como AWS, en términos de recursos y servicios disponibles para cada cuenta.
- Monitoreo y gestión: identifica y monitorea los límites de la cuenta para evitar posibles interrupciones en el servicio debido a la superación de estos límites.
- Planificación y optimización: desarrolla habilidades para planificar y optimizar el uso de los recursos dentro de los límites de la cuenta, maximizando la eficiencia y minimizando los costos.

Activación de saberes previos

Tiempo de Ejecución: 20 horas

PLANTEAMIENTO DE LA SESIÓN	MATERIALES
Lección 1: Introducción a la protección de la infraestructura Objetivo: Comprender la importancia de la protección de la infraestructura en entornos informáticos y familiarizarse con los conceptos básicos de seguridad de la información Lección 2: Estructura de una aplicación web de tres niveles y Uso de una VPC Objetivo: Comprender la estructura básica de una aplicación web de tres niveles y cómo se divide en capas de presentación, lógica de negocios y datos.	¿Qué es Amazon VCP? https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html. Conexión a internet mediante una puerta de enlace de internet Conexión a Internet mediante una puerta de enlace de Internet - Amazon Virtual Private Cloud Puertas de enlace NAT Gateways NAT - Amazon Virtual Private Cloud

Activación de saberes previos

PLANTEAMIENTO DE LA SESIÓN	MATERIALES
Actividades: Lectura y discusión de materiales que describen los conceptos de capas en una aplicación web. Análisis de ejemplos de arquitecturas de aplicaciones web de tres niveles. Ejercicio práctico: Diseño de la arquitectura de una aplicación web de tres niveles, identificando los componentes de cada capa. Objetivo: Acercar al participante al concepto de Virtual Private Cloud (VPC) y comprender cómo se utiliza para aislar recursos en la nube.	Instancias de NAT Instancias NAT - Amazon Virtual Private Cloud Comparar las puertas enlace NAT con instancias NAT https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html Dimensionamiento de VPC Nubes virtuales privadas (VPC) - Amazon Virtual Private Cloud

Activación de saberes previos

PLANTEAMIENTO DE LA SESIÓN	MATERIALES
Actividades: Presentación de conceptos básicos de VPC, incluyendo subredes, tablas de rutas y gateways. Demostración de la creación y configuración de una VPC en AWS. Ejercicio práctico: Creación de una VPC personalizada, configurando subredes públicas y privadas. Lección 3: Configuración de subredes públicas y privadas y protocolos de Internet Objetivo: Aprender a configurar subredes públicas y privadas dentro de una VPC y comprender cómo funcionan los protocolos de Internet en este contexto.	Direccionamiento IP Direccionamiento IP para VPC y subredes - Amazon Virtual Private Cloud Direcciones Elásticas Asociar direcciones IP elásticas con recursos en la VPC - Amazon Virtual Private Cloud Configurar tablas de enrutamiento Configurar tablas de enrutamiento - Amazon Virtual Private Cloud

Activación de saberes previos

PLANTEAMIENTO DE LA SESIÓN	MATERIALES
Actividades: Explicación de la diferencia entre subredes públicas y privadas y su importancia en la seguridad de la red. Ejercicio práctico: Configuración de subredes públicas y privadas en una VPC, asignación de direcciones IP y configuración de tablas de rutas. Discusión sobre los protocolos de Internet utilizados en subredes públicas y privadas, como HTTP, HTTPS y SSH. Lección 4: Uso de grupos de seguridad de AWS y Uso de ACL de red de AWS Objetivo: Comprender cómo se utilizan los grupos de seguridad de AWS para controlar el tráfico de red hacia y desde instancias de EC2 dentro de una VPC.	Controlas el trafico hacia los recursos de AWS mediante grupos de seguridad Controlar el tráfico hacia los recursos de AWS mediante grupos de seguridad - Amazon Virtual Private Cloud Registro del trafico de IP con registro de flujo de la VPC https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html. ¿Qué es Elastic Load Balancing? ¿Qué es Elastic Load Balancing? - Elastic Load Balancing (amazon.com)

Activación de saberes previos

PLANTEAMIENTO DE LA SESIÓN	MATERIALES
Actividades: Introducción a los grupos de seguridad de AWS y su función en la seguridad de la red. Ejercicio práctico: Creación y configuración de grupos de seguridad en AWS, estableciendo reglas de entrada y salida. Estudio de casos: Análisis de escenarios de seguridad y cómo los grupos de seguridad pueden ayudar a mitigar riesgos. Objetivo: Aprender a utilizar las Listas de Control de Acceso (ACL) de red de AWS para controlar el tráfico de red a nivel de subred dentro de una VPC.	Protección de datos en Elastic Load Balancing Protección de datos en Elastic Load Balancing - Elastic Load Balancing (amazon.com) Amazon Inspector https://aws.amazon.com/inspector.

Activación de saberes previos

PLANTEAMIENTO DE LA SESIÓN

Actividades:
Explicación de los conceptos básicos de las ACL de red y cómo difieren de los grupos de seguridad.
Ejercicio práctico: Configuración de ACL de red en una VPC de AWS para permitir o denegar tráfico específico.
Comparación entre grupos de seguridad y ACL de red: Discusión sobre cuándo usar cada uno y cómo complementarse mutuamente.

Lección 5: Uso de equilibradores de carga de AWS, Resumen global y Protección de los recursos de cómputo
Objetivo: Comprender cómo funcionan los equilibradores de carga de AWS y cómo se utilizan para distribuir el tráfico entre múltiples instancias de EC2.
Actividades:
Introducción a los equilibradores de carga de AWS y sus diferentes tipos (clásico, de red, de aplicación).
Ejercicio práctico: Creación y configuración de un equilibrador de carga en AWS, distribuyendo el tráfico entre instancias de EC2.

Activación de saberes previos

PLANTEAMIENTO DE LA SESIÓN

Objetivo: Repasar los conceptos clave aprendidos en el módulo y discutir estrategias para proteger los recursos de cómputo en una infraestructura en la nube.
Actividades:
Revisión de los conceptos clave del módulo, incluyendo VPC, grupos de seguridad, ACL de red y equilibradores de carga.
Debate sobre mejores prácticas para proteger instancias de EC2 y otros recursos de cómputo en la nube.

Ejercicio práctico: Implementación de medidas de seguridad adicionales en instancias de EC2, como la configuración de software de seguridad y la gestión de actualizaciones.
Laboratorio: Protección de los recursos de la VPC mediante grupos de seguridad

Objetivo: Aplicar los conocimientos adquiridos en el módulo mediante la configuración práctica de grupos de seguridad para proteger los recursos dentro de una VPC.

Activación de saberes previos

PLANTEAMIENTO DE LA SESIÓN

Actividades:
Laboratorio práctico guiado: Configuración de grupos de seguridad en una VPC de AWS según un escenario específico.
Evaluación del cumplimiento de los requisitos de seguridad y solución de problemas.
Discusión sobre las lecciones aprendidas y posibles mejoras en la configuración de seguridad.

Evaluación de conocimientos

COLOMBIA POTENCIA DE LA VIDA

TIC

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira