Nadia Arellano G.
Ingeniera en Informática

Resumen Módulo 3 - Seguridad en Infraestructura Cloud

Este documento forma parte del portafolio profesional de Nadia Arellano, participante del Bootcamp "Seguridad Cloud" otorgado por Talento Digital y SENCE, impartido por OTEC EDUTECNO.

Objetivos del módulo 3:

- Configurar componentes de seguridad esenciales en la infraestructura cloud usando servicios de AWS como Route 53, Shield, WAF, ACM y VPN.
- Implementar mecanismos de protección frente a amenazas como DDoS, spoofing, MITM y accesos no autorizados.
- Diseñar una arquitectura segura para el acceso remoto y la conexión de redes locales con la nube.

Contenidos clave:

- Seguridad en DNS con Route 53 y DNSSEC.
- Protección contra ataques DDoS y spoofing con AWS Shield y WAF.
- Uso de certificados SSL/TLS y HSTS para prevenir ataques MITM.
- Configuración de túneles IPSEC VPN y Client VPN en AWS.
- Protocolos de cifrado (AES, SHA-256) y autenticación (Radius, Active Directory).
- Monitoreo y alertas con CloudWatch y análisis de registros con Athena y CloudTrail.

Evidencias incluidas en este módulo:

- Actividades resueltas de las seis sesiones del módulo.
- Evaluación final con respuestas justificadas.
- Este mismo resumen, que incluye una reflexión sobre el impacto del módulo en el desarrollo profesional.

Reflexión personal:

El módulo 3 me permitió aplicar directamente conceptos de seguridad en entornos cloud, usando herramientas de AWS. Aprendí a configurar mecanismos de defensa eficaces como AWS WAF y Shield, lo cual me dio una visión más concreta sobre cómo proteger aplicaciones web. Además, la integración de VPNs y certificados SSL reforzó la importancia de una arquitectura robusta, especialmente en contextos de trabajo remoto o híbrido.