Evaluación del módulo 9

Consigna del proyecto👨‍💻

alkemy

Evaluación del módulo

Proyecto: Cloud Secure

Situación inicial 📍

Unidad solicitante: Equipo de Seguridad de la fintech “Blue Wave”

Blue Wave migró su core bancario a AWS Academy Learner Lab (cuenta educativa sin costo). Tras una auditoría preliminar, el CISO detectó configuraciones débiles de identidad, carencia de protecciones contra DDoS y ausencia de evidencias para marcos como ISO 27001 o PCI DSS.
El reto consiste en **diseñar y ejecutar una auditoría de seguridad integral**, aplicar controles de cumplimiento normativo y desplegar servicios gestionados (IAM, Cognito, WAF, Shield, Config, GuardDuty, Macie) que mitiguen los riesgos hallados.

Nuestro objetivo 📋

Aplicar principios de seguridad cloud mediante el análisis de amenazas, cumplimiento normativo y uso de servicios especializados, entregando:

- Una **arquitectura segura** documentada.
- **Configuraciones** de identidad, red y aplicación alineadas a buenas prácticas.
- **Evidencias** de cumplimiento generadas con AWS Config, CloudWatch y CloudTrail.
- **Informe de auditoría** con hallazgos y plan de remediación.
- Estimación de **costos** de los servicios habilitados.

Requerimientos 🤝

Dimensión	Requisito mínimo
Identidad	Roles IAM con *mínimo privilegio*, MFA y políticas separadas por entorno (Dev/Test/Prod).
Aplicación	Protección capa 7 con AWS WAF y capa 3/4 con AWS Shield Standard.
Datos	Buckets S3 cifrados y escaneados por Macie; KMS habilitado.
Cumplimiento	Reglas AWS Config para CIS v1.4; plantilla ISO 27001 en Audit Manager.
Monitoreo	CloudWatch Logs + métricas; alarmas de alta severidad a SNS.
Evidencias	CloudTrail habilitado en todas las regiones; Security Hub centralizando hallazgos.

Métricas generales 🔢

Métrica	Mín.	Máx.
Controles CIS implementados	10	20
Hallazgos críticos remediados	5	10
Evidencias Audit Manager adjuntas	8	16
Reglas WAF configuradas	3	5
Roles IAM creados	4	6
Pruebas RED-GREEN (tdd-security scripts)*	6	12
Automatizaciones (Lambda/EventBridge)	2	4
Diagramas de arquitectura actualizados	1	1

* Scripts Bash/Python que validan (RED) y luego confirman (GREEN) la existencia de controles (p.ej., bucket cifrado).

Paso a paso 👣

Módulo: Fundamentos de Seguridad Cloud
Etapas (lecciones): 6 — cada una basada en uno de los manuales teóricos.

> Dedica tiempo asincrónico en AWS Academy Learner Lab; en clase en vivo resolveremos dudas y revisaremos avances.

Lección 1 – Principios de Seguridad en la Nube

📌 **Objetivo:** Comprender responsabilidad compartida, cifrado, mínimo privilegio y monitoreo continuo.
📍 **Tareas:**

1. Leer el manual #1.
2. Crear diagrama de responsabilidad compartida para Blue Wave.
3. Activar CloudTrail (todas las regiones) y configurar bucket S3 cifrado para logs.
4. Script TDD-Security: verificar que CloudTrail esté encendido (RED-GREEN).

Lección 2 – Normas Internacionales

📌 **Objetivo:** Mapear controles ISO 27001, GDPR y PCI DSS a la arquitectura.
📍 **Tareas:**

1. Completar plantilla ISO 27001 en AWS Audit Manager.
2. Habilitar AWS Config y reglas CIS predefinidas.
3. Documentar brecha ↔ control pendiente (matriz de trazabilidad).

Lección 3 – Modelo de Compliance y Seguridad Automatizada

📌 **Objetivo:** Automatizar detección y remediación de desviaciones.
📍 **Tareas:**

1. Crear reglas AWS Config para cifrado S3 y rotación KMS.

2. Vincular remediación automática (SSM Automation) para buckets sin cifrar.

3. Habilitar GuardDuty y Macie en cuenta de seguridad central.

Lección 4 – Seguridad de Aplicativo

📌 **Objetivo:** Proteger capa 3/4 y 7 con Shield y WAF; distribuir contenido seguro con CloudFront.

📍 **Tareas:**

1. Asociar AWS WAF (reglas administradas + rate-based) a un CloudFront distro.

2. Habilitar AWS Shield Standard (automático) y revisar métricas DDoS.

3. Script TDD-Security: simular petición maliciosa → esperar bloqueo (RED-GREEN).

Lección 5 – Autenticación y Autorización en Cloud

📌 **Objetivo:** Implementar flujo de identidad con Cognito (User Pool + Identity Pool).

📍 **Tareas:**

1. Crear User Pool con políticas de contraseña fuertes y MFA obligatorio.

2. Configurar federación con Google OIDC.

3. Mapear grupo “Auditor” → rol IAM de solo-lectura.

4. Evidenciar inicio de sesión exitoso en CloudTrail.

Lección 6 – Auditorías Tradicionales y su Evolución al Cloud

📌 **Objetivo:** Ejecutar auditoría final, priorizar hallazgos y generar informe ejecutivo.

📍 **Tareas:**

1. Seguir las 6 etapas: Planeación, Descubrimiento, Evaluación, Pruebas, Análisis, Informe.

2. Usar Security Hub para consolidar hallazgos y exportar CSV.

3. Calcular KPI “% hallazgos críticos resueltos”.

4. Presentar plan de remediación a 30 días con costos estimados (AWS Pricing Calculator).

¿Qué vamos a validar? 🔍

Área	Criterios clave
Técnicos	Controles CIS habilitados, IAM con mínimo privilegio, WAF/Shield activos, logs centralizados.
Automatización	Reglas AWS Config + remediación, scripts TDD-Security con resultados RED-GREEN.
Cumplimiento	Evidencias ISO 27001, GDPR, PCI DSS en Audit Manager.
Documentación	Diagrama de arquitectura segura, matriz de trazabilidad, informe ejecutivo.
Performance	Alarmas CloudWatch configuradas, tiempo medio de remediación < 15 min (simulado).

Referencias 🦺

AWS Well-Architected Framework – Security Pillar
https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/

CIS AWS Foundations Benchmark v1.4
https://www.cisecurity.org/benchmark/amazon_web_services

AWS Foundational Security Best Practices Standard (Security Hub)
https://docs.aws.amazon.com/securityhub/latest/userguide/fsbp-standard.html

ISO/IEC 27001 – Controles mapeados a AWS
https://aws.amazon.com/compliance/iso-27001-faqs/

AWS Workshop: WAF & Shield
https://catalog.workshops.aws/waf-shield/en-US

AWS Workshop: Automating Compliance with AWS Config
https://catalog.workshops.aws/config/en-US

AWS Workshop: Amazon Cognito Fundamentals
https://catalog.workshops.aws/cognito/en-US

Recursos 🎁

- **AWS Academy Learner Lab** – Cuenta educativa sin costo.
- Blog "AWS Security Blog" – Ejemplos de IaC y remediación automática.
- Repositorio Git: *tdd-security-scripts* (Bash/Python) para pruebas RED-GREEN.
- Vídeo corto "Cómo usar Audit Manager" (YouTube, 10 min).

Entregables ✅

1. **Repositorio Git** con:
    - Carpeta iac/ (CloudFormation/Terraform).
    - Carpeta scripts/ (pruebas RED-GREEN).

    - Carpeta docs/ (diagrama, matriz, informe PDF).

2. **Export** de hallazgos Security Hub y evidencias Audit Manager.
3. **Presentación final** (10 diapositivas) con arquitectura segura y costos.
4. **Video demo** (≤ 5 min) mostrando bloqueo WAF y evento GuardDuty.

Portafolio 💼

Publica el repositorio en GitHub y enlázalo en tu portafolio.
Incluye capturas del dashboard Security Hub y el diagrama final. Destaca:

- Diseño de arquitectura segura.
- Automatización de cumplimiento.
- Métricas logradas (p.ej., 90 % hallazgos críticos resueltos).

Esto demostrará tu capacidad para **auditar, asegurar y documentar** entornos cloud de forma profesional.

¡Éxitos!

Nos vemos más adelante

alkemy