Seguridad y Cumplimiento

Cumplimiento PCI DSS Level 1

Requisito	Implementación	Tecnología AWS	Estado
Req 1: Firewall	VPC + Security Groups	VPC, Security Groups, NACLs	✅
Req 2: Configuración Segura	Hardening de sistemas	AMI, Container Security	✅
Req 3: Protección de Datos	Cifrado en reposo	KMS, HSM	✅
Req 4: Cifrado en Tránsito	TLS 1.3	Certificate Manager	✅
Req 5: Anti-malware	Protección contra virus	GuardDuty, Inspector	✅
Req 6: Sistemas Seguros	Gestión de vulnerabilidades	Code Scanning, Inspector	✅
Req 7: Control de Acceso	RBAC + ABAC	IAM, Cognito	✅
Req 8: Autenticación	MFA + Contraseñas fuertes	Cognito, KMS	✅
Req 9: Acceso Físico	Seguridad del centro de datos	AWS Compliance	✅
Req 10: Monitoreo	Logging + Monitoreo	CloudTrail, CloudWatch	✅
Req 11: Pruebas de Seguridad	Penetration Testing	Automated Scanning	✅
Req 12: Política de Seguridad	Seguridad de la información	Documentación + Training	✅

Seguridad y Cumplimiento

Controles de Seguridad Implementados:

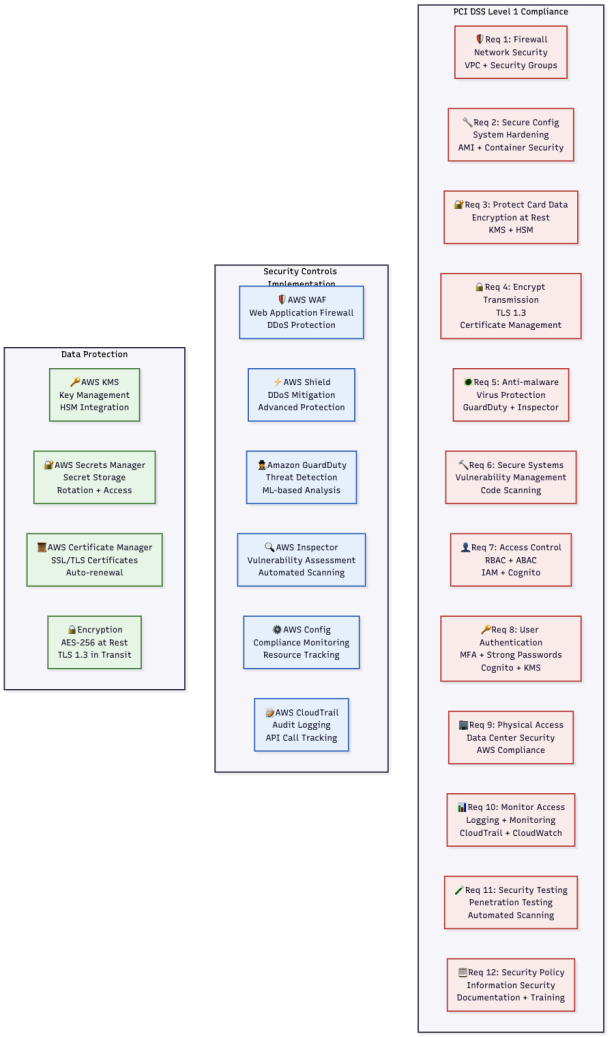
- AWS WAF: Web Application Firewall con protección DDoS
- AWS Shield: Mitigación avanzada de DDoS
- Amazon GuardDuty: Detección de amenazas basada en ML
- AWS Inspector: Evaluación automatizada de vulnerabilidades
- AWS Config: Monitoreo de cumplimiento y tracking de recursos
- AWS CloudTrail: Logging de auditoría y tracking de llamadas API

Identity and Access Management (IAM)

IAM robusto es fundamental para controlar el acceso a recursos críticos y cumplir con regulaciones bancarias.

Arquitectura IAM:

- Amazon Cognito: Identity Provider centralizado
- Multi-Factor Authentication: SMS + TOTP + Biometric
- Single Sign-On: SAML + OpenID Connect
- AWS IAM: Gestión de identidades y permisos
- RBAC + ABAC: Control de acceso basado en roles y atributos



Seguridad y Cumplimiento

Cumplimiento

- PCI DSS Level 1: Cumplimiento completo para procesamiento de pagos
- GDPR/LOPD: Protección de datos personales
- Basel III: Requisitos de capital bancario
- ISO 27001: Gestión de seguridad de la información

Protección

- Cifrado End-to-End: Protección completa de datos
- Detección de Amenazas: Identificación proactiva de riesgos
- Monitoreo Continuo: Vigilancia 24/7
- Respuesta Automática: Mitigación automática de amenazas

Auditoría

- Logging Completo: Registro de todas las actividades
- Trazabilidad Total: Seguimiento completo de transacciones
- Reportes Automáticos: Generación automática de reportes
- Evidencia de Cumplimiento: Documentación para auditorías

Resiliencia

- Tolerancia a Fallos: Continuidad ante fallos de seguridad
- Recuperación Rápida: Restauración rápida de servicios
- Continuidad del Negocio: Operación ininterrumpida
- Planes de Contingencia: Procedimientos de emergencia