

**Ikusi**

## **Security & IAM - CVDex**

Finanzas SD Documentation / Documentación de Finanzas SD

**Finanzas SD Documentation  
Documentación de Finanzas SD**

Ikusi  
November 10, 2025

Confidential - Internal Use Only

# 1 Security & IAM - CVdex

## Security and Identity Access Management Guidelines Directrices de Seguridad y Gestión de Acceso de Identidad

---

### 1.1 EN: Overview

This document defines security and IAM practices for Finanzas SD, ensuring compliance with guardrails and industry best practices.

### 1.2 ES: Descripción General

Este documento define prácticas de seguridad e IAM para Finanzas SD, asegurando cumplimiento con barreras de seguridad y mejores prácticas de la industria.

---

### 1.3 EN: Authentication & Authorization

#### 1.3.1 OIDC-Only CI/CD

- **No Static Keys:** Never store AWS access keys in code or environment variables
- **GitHub OIDC:** Use OpenID Connect for GitHub Actions authentication
- **Short-Lived Tokens:** Tokens automatically expire after workflow execution
- **Least Privilege:** IAM roles have minimal required permissions

#### 1.3.2 Cognito Groups

- **SDT** (Service Delivery Team): Full system access, administrative functions
- **PM** (Project Manager): Project management, pre-factura creation, budget oversight
- **FIN** (Finance): Financial approval, budget management, reporting
- **AUD** (Audit): Read-only access, audit trail review, compliance reporting

#### 1.3.3 JWT Middleware

- All API handlers validate JWT tokens
- Token expiration enforced
- Invalid tokens return 401 Unauthorized
- Token refresh managed by Cognito

### 1.4 ES: Autenticación y Autorización

#### 1.4.1 Solo OIDC en CI/CD

- **Sin Claves Estáticas:** Nunca almacenar claves de acceso AWS en código o variables de entorno
- **OIDC de GitHub:** Usar OpenID Connect para autenticación de GitHub Actions
- **Tokens de Corta Duración:** Tokens expiran automáticamente después de ejecución del flujo
- **Privilegio Mínimo:** Roles IAM tienen permisos mínimos requeridos

#### 1.4.2 Grupos Cognito

- **SDT** (Equipo de Entrega de Servicios): Acceso completo al sistema, funciones administrativas
- **PM** (Gerente de Proyecto): Gestión de proyectos, creación de pre-facturas, supervisión presupuestaria
- **FIN** (Finanzas): Aprobación financiera, gestión presupuestaria, reportes
- **AUD** (Auditoría): Acceso solo lectura, revisión de registro de auditoría, reportes de cumplimiento

#### 1.4.3 Middleware JWT

- Todos los manejadores API validan tokens JWT
- Expiración de token aplicada
- Tokens inválidos devuelven 401 No Autorizado
- Actualización de token gestionada por Cognito

---

### 1.5 EN: Data Security

#### 1.5.1 Encryption at Rest

- **DynamoDB**: Server-side encryption (SSE) with AWS managed keys
- **S3**: AES-256 encryption for all objects
- **Secrets Manager**: Encrypted configuration values

#### 1.5.2 Encryption in Transit

- **TLS 1.2+**: Required for all communications
- **HTTPS Only**: No HTTP endpoints exposed
- **Certificate Management**: AWS Certificate Manager for CloudFront

#### 1.5.3 CORS Policy

- **Restricted Origins**: Only CloudFront distribution allowed
- **No Wildcards**: Explicit origin whitelist
- **Credentials Allowed**: Support for JWT in headers

### 1.6 ES: Seguridad de Datos

#### 1.6.1 Encriptación en Reposo

- **DynamoDB**: Encriptación del lado del servidor (SSE) con claves gestionadas por AWS
- **S3**: Encriptación AES-256 para todos los objetos
- **Secrets Manager**: Valores de configuración encriptados

#### 1.6.2 Encriptación en Tránsito

- **TLS 1.2+**: Requerido para todas las comunicaciones
- **Solo HTTPS**: Sin endpoints HTTP expuestos
- **Gestión de Certificados**: AWS Certificate Manager para CloudFront

### 1.6.3 Política CORS

- **Orígenes Restringidos:** Solo distribución CloudFront permitida
  - **Sin Comodines:** Lista blanca de origen explícita
  - **Credenciales Permitidas:** Soporte para JWT en encabezados
- 

## 1.7 EN: Evidence Pack Requirements

Before any production merge, the following evidence must be collected:

### 1.7.1 Required Documents

#### 1. Test Results

- Unit test coverage report (>80%)
- API contract validation (Newman)
- Integration test results

#### 2. Security Scans

- CodeQL analysis (0 critical alerts)
- Dependency vulnerability scan (0 high/critical)
- OWASP Top 10 checklist

#### 3. Performance Tests

- Load test results (target: 100 req/s)
- Latency metrics (p95 < 200ms)
- Database performance (query times)

#### 4. Smoke Tests

- Health endpoint verification
- Key user flows tested
- Error handling validated

#### 5. Rollback Plan

- Step-by-step rollback procedure
- Database migration rollback (if applicable)
- Estimated rollback time

### 1.7.2 Evidence Pack Format

- PDF compilation of all documents
- Signed by QA lead and DevOps lead
- Uploaded to deployment workflow
- Archived in evidence repository

## 1.8 ES: Requisitos de Paquete de Evidencia

Antes de cualquier fusión a producción, se debe recopilar la siguiente evidencia:

### 1.8.1 Documentos Requeridos

#### 1. Resultados de Pruebas

- Reporte de cobertura de pruebas unitarias (>80%)
- Validación de contrato API (Newman)
- Resultados de pruebas de integración

#### 2. Escaneos de Seguridad

- Análisis CodeQL (0 alertas críticas)
- Escaneo de vulnerabilidades de dependencias (0 alta/crítica)
- Lista de verificación OWASP Top 10

#### 3. Pruebas de Rendimiento

- Resultados de prueba de carga (objetivo: 100 req/s)
- Métricas de latencia (p95 < 200ms)
- Rendimiento de base de datos (tiempos de consulta)

#### 4. Smoke Tests

- Verificación de endpoint de salud
- Flujos clave de usuario probados
- Manejo de errores validado

#### 5. Plan de Rollback

- Procedimiento de rollback paso a paso
- Rollback de migración de base de datos (si aplica)
- Tiempo estimado de rollback

### 1.8.2 Formato de Paquete de Evidencia

- Compilación PDF de todos los documentos
- Firmado por líder QA y líder DevOps
- Cargado a flujo de despliegue
- Archivado en repositorio de evidencia

---

## 1.9 EN: Guardrails Checklist

Before any deployment:

- [ ] No static AWS credentials in code
- [ ] OIDC configured for CI/CD
- [ ] All API routes have JWT validation
- [ ] CORS restricted to CloudFront only
- [ ] Encryption at rest enabled (DDB, S3)
- [ ] TLS 1.2+ enforced
- [ ] Evidence pack complete and approved
- [ ] CodeQL scan passed (0 critical)
- [ ] Dependency scan passed (0 high/critical)
- [ ] No production impacts on unrelated systems

## 1.10 ES: Lista de Verificación de Barreras de Seguridad

Antes de cualquier despliegue:

- [ ] Sin credenciales estáticas AWS en código
- [ ] OIDC configurado para CI/CD
- [ ] Todas las rutas API tienen validación JWT
- [ ] CORS restringido solo a CloudFront
- [ ] Encriptación en reposo habilitada (DDB, S3)
- [ ] TLS 1.2+ aplicado
- [ ] Paquete de evidencia completo y aprobado
- [ ] Escaneo CodeQL pasado (0 crítico)
- [ ] Escaneo de dependencias pasado (0 alta/crítica)
- [ ] Sin impactos de producción en sistemas no relacionados

---

## 1.11 EN: Incident Response

### 1.11.1 Security Incident Procedure

1. **Detect:** CloudWatch alarms, user reports, monitoring
2. **Contain:** Disable affected functionality, rotate credentials
3. **Investigate:** Review audit logs, CloudWatch logs, access patterns
4. **Remediate:** Apply fixes, deploy patches, update policies
5. **Document:** Incident report, lessons learned, preventive measures

### 1.11.2 Credential Compromise

- Immediately disable affected IAM role
- Rotate all potentially exposed credentials
- Review CloudTrail for unauthorized access
- Notify security team and stakeholders

### 1.11.3 Data Breach

- Follow data breach response plan
- Notify affected users within 72 hours
- Document scope and impact
- Implement additional controls

## 1.12 ES: Respuesta a Incidentes

### 1.12.1 Procedimiento de Incidente de Seguridad

1. **Detectar:** Alertas CloudWatch, informes de usuarios, monitoreo
2. **Contener:** Deshabilitar funcionalidad afectada, rotar credenciales
3. **Investigar:** Revisar logs de auditoría, logs CloudWatch, patrones de acceso
4. **Remediar:** Aplicar correcciones, desplegar parches, actualizar políticas
5. **Documentar:** Reporte de incidente, lecciones aprendidas, medidas preventivas

### 1.12.2 Compromiso de Credenciales

- Deshabilitar inmediatamente rol IAM afectado
- Rotar todas las credenciales potencialmente expuestas
- Revisar CloudTrail para acceso no autorizado
- Notificar a equipo de seguridad y partes interesadas

### 1.12.3 Violación de Datos

- Seguir plan de respuesta a violación de datos
  - Notificar a usuarios afectados dentro de 72 horas
  - Documentar alcance e impacto
  - Implementar controles adicionales
- 

**Document Version:** 1.0

**Effective Date:** November 2024

**Review Date:** May 2025

**Owner:** Security Team / Equipo de Seguridad

**Status:** Active / Activo