CVDex

controls-and-audit

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

November 10, 2025

1 Controls and Audit Framework

Controls and Audit Framework for Finanzas SD
Marco de Controles y Auditoría para Finanzas SD

1.1 EN: Overview

This document defines the controls and audit framework for Finanzas SD, ensuring financial accuracy, security compliance, and operational integrity.

1.2 ES: Descripción General

Este documento define el marco de controles y auditoría para Finanzas SD, asegurando precisión financiera, cumplimiento de seguridad e integridad operacional.

1.3 EN: Control Categories

1.3.1 Preventive Controls

- **Access Control**: Cognito groups enforce RBAC
- **Input Validation**: All forms validate data before submission
- **Budget Limits**: System prevents over-budget allocations
- **Dual Approval**: High-value items require two approvers
- **Encryption**: Data encrypted at rest and in transit

1.3.2 Detective Controls

- **Audit Logging**: All actions logged with actor and timestamp
- **CloudWatch Alarms**: Automated alerts for anomalies
- **Deviation Reports**: Monthly variance analysis
- **Access Reviews**: Quarterly user access audits
- **Security Scans**: Automated CodeQL and dependency checks

1.3.3 Corrective Controls

- **Adjustment Workflow**: Structured process for corrections
- **Incident Response**: Defined procedures for issues
- **Rollback Capability**: Ability to revert deployments
- **Backup and Recovery**: Regular backups with tested restore

1.4 ES: Categorías de Control

1.4.1 Controles Preventivos

- **Control de Acceso**: Grupos Cognito aplican RBAC
- **Validación de Entrada**: Todos los formularios validan datos antes de envío
- **Límites Presupuestarios**: Sistema previene asignaciones sobre presupuesto
- **Aprobación Dual**: Elementos de alto valor requieren dos aprobadores
- **Encriptación**: Datos encriptados en reposo y en tránsito

1.4.2 Controles Detectivos

- **Registro de Auditoría**: Todas las acciones registradas con actor y marca de tiempo
- **Alarmas CloudWatch**: Alertas automatizadas para anomalías
- **Reportes de Desviación**: Análisis de varianza mensual
- **Revisiones de Acceso**: Auditorías trimestrales de acceso de usuarios
- **Escaneos de Seguridad**: Verificaciones automatizadas CodeQL y dependencias

1.4.3 Controles Correctivos

- **Flujo de Ajuste**: Proceso estructurado para correcciones
- **Respuesta a Incidentes**: Procedimientos definidos para problemas
- **Capacidad de Rollback**: Habilidad para revertir despliegues
- **Respaldo y Recuperación**: Respaldos regulares con restauración probada

---

1.5 EN: Audit Trail Requirements

1.5.1 Logged Events

Every system action must log:

- **Actor**: user_id and email
- **Timestamp**: ISO 8601 format with timezone
- **Action**: create, read, update, delete, approve, reject
- **Entity**: affected resource (project, pre-factura, allocation)
- **Entity ID**: unique identifier
- **Before/After**: state change details (for updates)
- **Metadata**: additional context (IP address, user agent, etc.)

1.5.2 Retention Policy

- **DynamoDB Audit Log**: 7 years minimum
- **CloudWatch Logs**: 90 days (exported to S3 for long-term)
- **S3 Archived Logs**: 7 years with Glacier transition after 1 year

1.5.3 Tamper Protection

- Audit logs are append-only
- No deletion or modification allowed
- Write-only IAM permissions for log writers
- Read permissions restricted to audit team

1.6 ES: Requisitos de Registro de Auditoría

1.6.1 Eventos Registrados

Cada acción del sistema debe registrar:

- **Actor**: user_id y email
- **Marca de Tiempo**: Formato ISO 8601 con zona horaria
- **Acción**: crear, leer, actualizar, eliminar, aprobar, rechazar
- **Entidad**: recurso afectado (proyecto, pre-factura, asignación)
- **ID de Entidad**: identificador único
- **Antes/Después**: detalles de cambio de estado (para actualizaciones)
- **Metadatos**: contexto adicional (dirección IP, agente de usuario, etc.)

1.6.2 Política de Retención

- **Registro de Auditoría DynamoDB**: 7 años mínimo
- **Registros CloudWatch**: 90 días (exportados a S3 para largo plazo)
- **Registros Archivados S3**: 7 años con transición a Glacier después de 1 año

1.6.3 Protección contra Manipulación

- Registros de auditoría son solo anexar
- Sin eliminación o modificación permitida
- Permisos IAM solo escritura para escritores de log
- Permisos de lectura restringidos a equipo de auditoría

1.7 EN: Compliance Requirements

1.7.1 Financial Controls

- **Segregation of Duties**: Requestor ≠ Approver
- **Dual Authorization**: Amounts > threshold require two approvals
- **Budget Enforcement**: System blocks over-budget transactions
- **Reconciliation**: Monthly comparison of plan vs actual

1.7.2 Security Controls

- **Authentication**: MFA required for all users
- **Authorization**: Role-based access via Cognito groups
- **Encryption**: TLS 1.2+ and AES-256
- **Vulnerability Management**: Regular security scans

1.7.3 Operational Controls

- **Change Management**: All production changes require evidence pack
- **Backup and Recovery**: Daily backups, tested restore procedures
- **Monitoring**: 24/7 CloudWatch alarms and canaries
- **Incident Management**: Defined response procedures

1.8 ES: Requisitos de Cumplimiento

1.8.1 Controles Financieros

- **Segregación de Deberes**: Solicitante ≠ Aprobador
- **Autorización Dual**: Montos > umbral requieren dos aprobaciones
- **Aplicación Presupuestaria**: Sistema bloquea transacciones sobre presupuesto
- **Reconciliación**: Comparación mensual de plan vs real

1.8.2 Controles de Seguridad

- **Autenticación**: MFA requerido para todos los usuarios
- **Autorización**: Acceso basado en roles vía grupos Cognito
- **Encriptación**: TLS 1.2+ y AES-256
- **Gestión de Vulnerabilidades**: Escaneos de seguridad regulares

1.8.3 Controles Operacionales

- **Gestión de Cambios**: Todos los cambios de producción requieren paquete de evidencia

- **Respaldo y Recuperación**: Respaldos diarios, procedimientos de restauración probados
- **Monitoreo**: Alarmas y canaries CloudWatch 24/7
- **Gestión de Incidentes**: Procedimientos de respuesta definidos

---

1.9 EN: Audit Schedule

1.9.1 Monthly Audits

- Budget execution vs plan
- Pre-factura approval queue aging
- Access control review (new users)
- System error rates

1.9.2 Quarterly Audits

- Complete user access review
- Segregation of duties compliance
- Audit log integrity check
- Control effectiveness assessment

1.9.3 Annual Audits

- Comprehensive financial audit
- Security posture assessment
- Business continuity plan test
- Third-party penetration test

1.10 ES: Cronograma de Auditoría

1.10.1 Auditorías Mensuales

- Ejecución presupuestaria vs plan
- Antigüedad de cola de aprobación de pre-facturas
- Revisión de control de acceso (nuevos usuarios)
- Tasas de error del sistema

1.10.2 Auditorías Trimestrales

- Revisión completa de acceso de usuarios
- Cumplimiento de segregación de deberes
- Verificación de integridad de registro de auditoría
- Evaluación de efectividad de controles

1.10.3 Auditorías Anuales

- Auditoría financiera comprensiva
- Evaluación de postura de seguridad
- Prueba de plan de continuidad de negocio
- Prueba de penetración de terceros

1.11 EN: Reporting

1.11.1 Audit Reports Generated

1. **Monthly Control Report**
    - Control testing results
    - Exceptions identified
    - Remediation status
2. **Quarterly Compliance Report**
    - Compliance status summary
    - Key risk indicators
    - Trend analysis
3. **Annual Audit Report**
    - Overall control environment
    - Material findings
    - Management responses
    - Recommendations

1.11.2 Report Distribution

- **Executive Summary**: Board and executives
- **Detailed Report**: Audit committee
- **Findings**: Management for remediation
- **Trends**: Risk management team

1.12 ES: Reportes

1.12.1 Reportes de Auditoría Generados

1. **Reporte de Control Mensual**

- Resultados de prueba de controles
- Excepciones identificadas
- Estado de remediación

2. **Reporte de Cumplimiento Trimestral**

   - Resumen de estado de cumplimiento
   - Indicadores clave de riesgo
   - Análisis de tendencias

3. **Reporte de Auditoría Anual**

   - Ambiente de control general
   - Hallazgos materiales
   - Respuestas de gerencia
   - Recomendaciones

1.12.2 Distribución de Reportes

- **Resumen Ejecutivo**: Junta y ejecutivos
- **Reporte Detallado**: Comité de auditoría
- **Hallazgos**: Gerencia para remediación
- **Tendencias**: Equipo de gestión de riesgos

Document Version: 1.0
Effective Date: November 2024
Review Date: Quarterly / Trimestral
Owner: Audit Team / Equipo de Auditoría
Status: Active / Activo