

Finanzas SD - Security & compliance

Finanzas SD - Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

December 13, 2025

1 Finanzas SD – Security & compliance

Last updated: 2025-12-06

Audience: Audit, Security, PMO, SDMT

Purpose: Security controls and compliance guidelines

Executive perspective: security leans on Cognito, scoped IAM roles, and auditable storage so every approval, upload, and reconciliation is provable. / Perspectiva ejecutiva: la seguridad se apoya en Cognito, roles IAM acotados y almacenamiento auditable para que cada aprobación, carga y conciliación sea comprobable.

1.1 Access control

- Autenticación: Cognito Hosted UI + JWT; API Gateway authorizer verifica firma y grupos (PMO, FIN, SDMT, AUDIT, EXEC_R0).
- Autorización por dominio: handlers validan grupo requerido; rechazan llamadas sin rol o sin projectId asociado.
- Principle of least privilege: sin llaves estáticas; despliegues usan roles OIDC de GitHub.

1.2 Data protection

- **Storage:** DynamoDB cifrado por defecto; S3 con claves segregadas por proyecto y sin objetos públicos.
- **Transit:** HTTPS obligatorio en UI y API base `https://pyorjw6lbe.execute-api.us-east-2.amazonaws.com`.
- **Retention:** evidencias versionadas; cambios de baseline y facturas incluyen trazabilidad (updated_by, timestamp).

1.3 Operational controls

- **Health:** /health revisa dependencias críticas antes de releases.
- **Logging:** CloudWatch con contexto (endpoint, projectId, operación). No incluir PII innecesaria ni tokens.
- **Alerts:** /alerts expone desviaciones y aprobaciones; utilice para revisión PMO/Auditoría.

1.4 Compliance guidance

- Separar ambientes (dev/stg/prod) y no mezclar artefactos de Acta/Prefactura.
- Evidencias deben guardarse con metadatos mínimos: projectId, module, lineItemId o invoiceId, uploader.
- Revisar RACI en `pmo-handbook.md` para responsabilidades de aprobación.