

Finanzas SD - Arquitectura técnica / Technical architecture

Finanzas SD - Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

December 5, 2025

1 Finanzas SD - Arquitectura técnica / Technical architecture

Executive perspective: Finanzas SD runs as a secure, decoupled stack where Cognito, API Gateway, and domain Lambdas enforce access while DynamoDB and S3 keep evidence auditable. / Perspectiva ejecutiva: Finanzas SD opera como una pila desacoplada y segura donde Cognito, API Gateway y Lambdas por dominio aplican controles de acceso mientras DynamoDB y S3 mantienen evidencia auditable.

1.1 Component map

- **Frontend (Finanzas UI):** rutas /finanzas/**, React + Cognito Hosted UI, despliegue en S3 + CloudFront.
- **API Gateway finanzas-sd-api:** proxy único con rutas por dominio (projects, rubros, allocations, invoices, uploads, health).
- **Lambdas por dominio** (carpeta services/finanzas-api/src/handlers): validan JWT Cognito y aplican lógica de negocio.
- **Almacenamiento:**
 - **DynamoDB:** tablas de proyectos, baselines, rubros, line items, allocation rules, invoices y alerts/changes.
 - **S3:** bucket estático para UI (ukusi-ui-finanzas-*) y prefix de evidencias para uploads/docs.
- **Observabilidad:** logs estructurados en CloudWatch; endpoints /health y /alerts.
- **Seguridad:** Cognito groups (PM0, FIN, SDMT, AUDIT, EXEC_R0) aplicados en UI y API authorizer.

Ver diagrama `diagrams/finanzas-architecture.svg` para flujos de solicitud y almacenamiento.

1.2 Request flow (end-to-end)

1. Usuario ingresa vía Hosted UI Cognito y obtiene JWT con grupos.
2. Finanzas UI envía llamadas firmadas con JWT hacia API Gateway.
3. Authorizer valida grupos y enruta a la Lambda correspondiente.
4. Lambda opera sobre DynamoDB (lectura/escritura), puede publicar alertas y retorna respuesta JSON.
5. Para cargas de evidencia, la Lambda genera la clave S3 y registra metadatos vinculados a proyecto/line item/invoice.

1.3 Deployment/runtime

- Región us-east-2; infraestructura descrita en `services/finanzas-api/template.yaml` (SAM).

- Promoción por etapas (dev/stg/prod) sin mezclar Acta/Prefactura artefactos.
- Pipelines existentes reutilizan diagnósticos (finanzas-aws-diagnostic) y health checks profundos.

1.4 Data protection controls (resumen)

- JWT verificado en API Gateway; Lambdas niegan acceso si falta grupo requerido.
- Evidencia en S3 con claves segregadas por proyecto y sin llaves estáticas.
- Registros de auditoría para cambios de baseline, handoff y facturas.