

**CVDex**

# **INSTRUCTIONS**

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

November 10, 2025

## 1 Project Operating Instructions (Finanzas SD - API & UI)

### 1.1 Roles

- **Backend Lead:** owns /services/finanzas-api (SAM, handlers, DDB, API Gateway).
- **FE Lead:** owns /src (UI). No backend logic in FE.
- **SRE:** owns workflows, alarms, canaries, OIDC integrity.

### 1.2 Guardrails (non-negotiable)

- **OIDC-only** AWS auth. No static AWS keys in workflows.
- Region **us-east-2**.
- Do NOT change /finanzas/\* CloudFront behavior or any acta-ui resources.
- Every new route returns **501** until implemented and is covered by tests.
- Single Node pkg per service (services/finanzas-api/package.json).

### 1.3 Required repository settings (Actions → Variables / Secrets)

#### Variables

- AWS\_REGION=us-east-2
- FINZ\_API\_STACK=finanzas-sd-api-dev
- FINZ\_API\_STAGE=dev
- COGNITO\_USER\_POOL\_ID=<your user pool id>
- COGNITO\_USER\_POOL\_ARN=<your user pool arn>

#### Secret

- OIDC\_AWS\_ROLE\_ARN=<arn:aws:iam::703...:role/ProjectplaceLambdaRole>

### 1.4 QA Gates (must pass before merge)

- 1) **Unit tests:** npm test in /services/finanzas-api (pro-rata, coverage math).
- 2) **SAM local smoke:** /health and /catalog/rubros → 200.
- 3) **Deploy OIDC:** aws sts get-caller-identity must succeed; no static fallback.
- 4) **Deployment summary:** API URL + working curl commands written to \$GITHUB\_STEP\_SUMMARY

### 1.5 Failure policy

- If OIDC fails, **stop** the job with a helpful error. Never fall back to static creds.
- If any required variable is empty, **stop** with a clear message.

## 1.6 Best practices

- Keep SAM authorizer issuer param from COGNITO\_USER\_POOL\_ID.
- Add handlers incrementally; stubs return **501** and are asserted in tests.
- One package.json per service; no nested Node projects.