Finanzas SD Infra Audit (us-east-2)

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

December 17, 2025

[ARCHIVED] Superseded by docs/finanzas/overview.md on 2025-12-05 # Finanzas SD Infra Audit (us-east-2)

0.1 Summary

- Verified that Finanzas SD AWS resources exist in account 703671891952 (dev stage) and align with the SAM template defaults for Cognito, DynamoDB tables, and CloudFront origin domain.
- Confirmed the expected Lambda fleet for the HTTP API is deployed in `us-east-2` with dev-staged function names that match the SAM template naming pattern.
- DynamoDB tables for the Finanzas domain exist with the expected pk/sk composite keys and on-demand billing.
- CloudFront distribution EPQU7PVDLQXUA routes `/finanzas/*` to the `ukusi-ui-finanzas-prod` S3 origin. A manifest mismatch between deployed and local Finanzas builds (JS hash drift) was identified; the deploy workflow now performs a post-upload manifest diff and will fail fast if drift remains.
- API Gateway HTTP API `finanzas-sd-api-dev` exposes the full route set with JWT authorizer pointing to Cognito pool `us-east-2_FyHLt0hiY` and client dshos5iou44tuach7ta3ic

0.2 AWS Inventory

- **Template defaults**: Cognito pool/client IDs, CloudFront domain, and table prefixes declared in `services/finanzas-api/template.yaml` guide expected resource names and origins.【F:services/finanzas-api/template.yaml†L4-L120】
- **Lambda functions discovered**: Dev-stage functions exist for allocations, alerts, line items, providers, close-month, forecast, adjustments, rubros, invoices, recon, allocations, health, catalog, prefacturas, baseline, billing, handoff, plan, alerts PEP3, upload, payroll, and projects.【668cf0†L1-L22】
- **DynamoDB tables present**: `finz_projects`, `finz_rubros`, `finz_allocations`, `finz_payroll_actuals`, `finz_adjustments`, `finz_alerts`, `finz_providers`, `finz_audit_log` (plus docs/prefacturas) exist in `us-east-2`.【564a6a†L1-L17】
- **CloudFront**: Distribution `d7t9x3j66yd8k.cloudfront.net` with origin `ukusi-ui-finanzas-p` and path behaviors for `/finanzas*`.【f05cd1†L1-L17】【f56339†L1-L31】
- **API Gateway**: HTTP API `finanzas-sd-api-dev` (ID pyorjw6lbe) with dev stage auto-deploying and Cognito JWT authorizer (pool `us-east-2_FyHLt0hiY`, client dshos5iou44tuach7ta3ici5m).【c195ba†L1-L12】【c4f2b9†L1-L17】

0.3 Lambda Audit

- All expected Finanzas SD Lambda functions are deployed under the dev stage naming convention (e.g., `finanzas-sd-api-dev-ProjectsFn-...`).【668cf0†L1-

L22】

- API routes are fully mapped to Lambda integrations via AWS_PROXY integrations; each route key resolves to a Finanzas Lambda function ARN, confirming connectivity between API Gateway and Lambda backends.【0b9af3†L1-L77】【bf0315†L1-L77】
- No log or health anomalies were observed in this pass (log sampling not requested); recommend periodic `aws logs tail` checks per runbook.

0.4 DynamoDB Audit

- Required domain tables exist with pk/sk composite keys and PAY_PER_REQUEST billing, matching the SAM definitions for projects, rubros, allocations, payroll_actuals, adjustments, alerts, providers, and audit_log.【4f8aa9†L1-L21】【49e190†L1-L21】【13596a†L1-L21】【cffaba†L1-L11】
- Table naming aligns with the `finz_` prefix from the SAM template parameters, ensuring Lambdas referencing TABLE_* env vars resolve to existing tables.【F:services/finanzas-api/template.yaml†L46-L78】

0.5 S3 + CloudFront Audit

- CloudFront distribution `d7t9x3j66yd8k.cloudfront.net` routes `/finanzas`, `/finanzas/`, and `/finanzas/*` to the `ukusi-ui-finanzas-prod` S3 origin with HTTPS redirects, confirming the correct SPA behavior is configured at the edge.【f05cd1†L1-L17】【f56339†L1-L18】
- Current bucket manifest (key prefix `finanzas/`) shows SPA entrypoints (`finanzas/index.html`, `finanzas/auth/callback.html`) plus assets and docs, with JS bundle `finanzas/assets/index` L38】
- Local `npm run build:finanzas` (with VITE_API_BASE_URL set) produces bundle `dist-finanzas/assets/index-ppTbD_1B.js` alongside matching HTML and assets.【d46f88†L2-L23】 The JS hash mismatch indicates deployed UI drift from the latest build; CloudFront currently serves the older bundle despite matching HTML filenames.【225404†L33-L38】
- Sample `curl -I` against `/finanzas/` returns HTTP 200 from CloudFront, confirming edge availability but not bundle freshness.【deb1e8†L1-L16】
- S3 object metadata for `finanzas/index.html` correctly reports `text/html` Content-Type and SSE enabled.【9ddfa6†L1-L10】

0.6 API + Auth Audit

- API Gateway HTTP API exposes expected Finanzas routes (projects, rubros, providers, allocations, payroll, adjustments, prefacturas, handoff, close-month, baseline,

plan, forecast, recon, health).【0b9af3†L1-L77】
- Each route integrates to the corresponding Lambda via AWS_PROXY with no missing integrations observed.【bf0315†L1-L77】
- JWT authorizer uses Cognito pool us-east-2_FyHLt0hiY and client dshos5iou44tuach7ta3ici matching the SAM defaults referenced by the UI and API.【c4f2b9†L1-L17】【F:services/finanzas-api/template.yaml†L5-L35】

0.7 Gaps & Recommended Fixes

- **S3/UI drift (Critical → Mitigated by CI guard):** Deployed JS bundle finanzas/assets/index does not match the latest local build (index-ppTbD_1B.js). The UI deploy workflow now runs a post-upload manifest comparison (local build vs. finanzas/ prefix) and fails on mismatch so drift cannot persist; rerun Deploy Finanzas UI to sync the current bundle and invalidate CloudFront.【d46f88†L9-L23】【225404†L33-L38】
- **Build-time env guardrail (Implemented):** CI now computes and exports VITE_API_BASE_UR before build and verifies the value is embedded in the bundle, preventing silent misconfiguration. Keep repo variables (FINZ_API_ID, FINZ_API_STAGE_*, DEV_API_URL) aligned with the intended stage before triggering deployments.【F:.github/workflows/deploy-ui.yml†L70-L193】
- **Ongoing health checks:** Keep periodic log/metrics validation for each Lambda (CloudWatch logs + lambda get-function-configuration) and S3 object content-type sampling in CI, following the runbook to catch drift before deployment.