Irving García Mendoza

IT Controls & Compliance · Information Security & Infrastructure Manager

Remote — Mexico • hola@irving.bio • 15+ years · IT risk, security & cloud

PROFESSIONAL SUMMARY

Information Security and Infrastructure leader with 15+ years across IT risk, security consulting, and cloud operations — currently Infrastructure & Information Security Manager at **Clara**, a pre-IPO LATAM fintech. Owns the IT control environment protecting financial operations across Mexico, Brazil, and Colombia: design and operation of IT General Controls (logical access, change management, security operations) over a 70-account, two-region AWS Organization with a ~USD $2.9M annual cloud and SaaS footprint. Combines hands-on cloud security engineering with audit-evidence discipline (Sprinto, Prowler, Steampipe/Turbot) and a production AI platform practice — security-bounded LLM agents on AWS Bedrock. Earlier career delivering regulatory and information-security consulting to banks, insurers, and government on fintech frameworks and Latin-American data-protection law. An ownership mindset suited to building an IT controls function ahead of an IPO, not merely maintaining one.

CAREER HIGHLIGHTS

- Led and completed the migration of a full-mesh VPC Peering estate (80+ connections) to **AWS Transit Gateway** across two regions with atomic route cutover and instant-rollback design — zero service disruption.
- Deployed AWS GuardDuty and centralized security alerting across **70 accounts** in two regions; drove fleet-wide CVE remediation including SSH elimination on 174 EC2 instances and continuous compliance monitoring.
- Designed and operates a production fleet of **five security-bounded LLM agents** on AWS Bedrock under a four-layer read-only enforcement model, automating infrastructure operations and FinOps reporting organization-wide.
- Brought **740+ Kafka topics** to high-availability standards with zero downtime across an 8-cluster MSK estate; raised OpenSearch lifecycle-policy coverage from 18.5% to 98.6% across a 1,703-index security-logging cluster.
- Produced the container-platform business case identifying **~31% run-rate savings**; administers an 11-product AWS Marketplace portfolio and executed an observability vendor migration contract-to-contract.

CORE COMPETENCIES

IT Risk & Compliance

- IT General Controls (ITGC) and IT Application Controls (ITAC) over financial data flows
- Risk identification, control-gap assessment, remediation, and findings management
- Audit support and evidence collection for internal and external auditors
- SOX (IT component); SOC 2, ISO 27001, PCI DSS, NIST CSF awareness
- Compliance automation (Sprinto) and continuous control monitoring

Information Security

- Identity lifecycle (joiner/mover/leaver), least privilege, segregation of duties
- Organization-scale vulnerability/CVE remediation and configuration hardening
- Threat detection & logging: GuardDuty, CloudTrail, Security Lake, Inspector, SIEM
- Posture management (Prowler), cross-account governance (Steampipe/Turbot)
- Zero Trust (Cloudflare WARP/Gateway), WAF, KMS, secrets, SPF/DKIM/DMARC

Cloud Infrastructure, FinOps & Resilience

- AWS multi-account Organizations (70 accounts), SCPs, StackSets, multi-region ops
- IaC: Terraform, Terragrunt, CloudFormation; Python/Bash/TypeScript automation
- Cost decomposition, anomaly root-cause, platform business cases, vendor administration
- Backup/recovery and BCP/DRP controls across jurisdictions

AI Platform Engineering & Automation

- Production LLM agents on AWS Bedrock (Anthropic Claude) with read-only enforcement
- RAG architectures: Bedrock Knowledge Bases, Aurora pgvector, OpenSearch
- Serverless automation on Cloudflare Workers (Workflows, Durable Objects, D1, AI Gateway)
- Workflow automation (n8n), MCP server development, AI governance and spend tiering

PROFESSIONAL EXPERIENCE

Clara — Infrastructure & Information Security Manager

2020 – Present

Pre-IPO fintech (corporate cards & spend management), LATAM — Mexico, Brazil, Colombia

Owns the IT control environment and cloud security posture for a regulated, pre-IPO fintech operating a 70-account AWS Organization across three countries and two AWS regions.

IT General Controls — Logical Access

- Operates the engineering identity lifecycle — 60+ documented offboardings enforcing timely revocation, least privilege, and segregation of duties across AWS, Okta/Auth0, and SaaS.
- Led an organization-wide IAM Identity Center security audit (65 accounts, 165 SSO users, 52 permission sets), remediating dormant users, over-privileged assignments, and offboarding gaps; runs a recurring credential-hygiene program (87 user/key remediations, org-wide credential reporting).
- Migrated 240 users from legacy OpenVPN to Cloudflare Zero Trust (WARP/Gateway) via a phased, MDM-driven rollout across three countries, then decommissioned the VPN estate.

IT General Controls — Change & Configuration Management

- Governs infrastructure change through an auditable ticketed workflow — 400+ completed change/security tickets and 40+ projects led through a staged pipeline (change approval, functionality test, proof of success, rollback verification).
- Builds hardened Amazon Linux 2023 golden AMIs on a quarterly cadence for all accounts and regions; directed lifecycle programs spanning DocumentDB engine upgrades (7 clusters), OpenSearch engine upgrades, EOL Lambda runtime remediation (78 functions), and EC2 Image Builder standardization.

Security Operations & Vulnerability Management

- Led the organization-wide AWS GuardDuty deployment — 70 accounts, two regions, delegated administration, StackSet auto-enrollment, KMS-encrypted publishing — with centralized EventBridge alerting of high-severity findings to Slack.
- Drove fleet-wide remediation: critical CVEs patched across all accounts, SSH disabled on 174 EC2 instances, vulnerable kernel module removed across 13 accounts via SSM, followed by continuous SSH compliance monitoring with daily org-wide reporting.
- Ran the email anti-spoofing program: 31 corporate domains audited, authentication driven to 96% compliance across 18 AWS SES sending domains (SPF hard-fail, DKIM, DMARC enforcement).
- Conducted an organization-wide WAFv2 effectiveness review (21 Web ACLs protecting 65 load balancers) and operates container-image scanning with automated triage to Slack.

Network Segmentation & Resilience

- Led and completed the VPC Peering to AWS Transit Gateway migration (80+ connections, multi-region, cross-account) with atomic route cutover and instant-rollback design.
- Redesigned 6 partner site-to-site IPSec VPNs across 6 accounts from static routing to BGP dynamic routing with hardened cryptography (IKEv2-only) and automatic failover, validated on a staging canary before production cutover.
- Manages backup/recovery and BCP/DRP controls (AWS Backup, snapshot policies, cross-account backup account) across multiple operating jurisdictions.

Data Platform Controls & Operations

- Remediated high-availability risk across an 8-cluster Amazon MSK (Kafka) estate — 740+ topics brought to replication and MinISR standards with zero downtime, including response to an AWS Health high-risk event on a production payments cluster; re-architected Kafka observability onto Amazon Managed Prometheus and Grafana.
- Raised OpenSearch lifecycle (ISM) coverage from 18.5% to 98.6% across a 1,703-index security-logging cluster; remediated write-saturation and shard-distribution incidents on production search clusters.
- Supports data-integrity controls over financial pipelines: AWS DMS change-data-capture (13 replication instances, 213 tasks) with latency alerting, encryption at rest/in transit, and access controls over an estate of 86 Aurora PostgreSQL clusters, DocumentDB, OpenSearch, MSK, Databricks, MWAA (Airflow), and QuickSight.

AI Platform Engineering

- Designed and operates five autonomous LLM agents on AWS Bedrock (Anthropic Claude) serving infrastructure operations over Slack — conversational diagnostics, ECS operations, Kafka alarm triage, FinOps reporting — under a four-layer read-only security model (IAM boundaries, pre-execution guard hooks, toolset restriction, prompt contracts).
- Built an LLM-driven support-intake bot on Cloudflare Workers (Workflows, Durable Objects, D1, AI Gateway) converting Slack requests into structured, tracked tickets; replaced third-party SaaS automations with auditable Workers.
- Deployed a self-hosted agent memory platform on ECS and a compliance-documentation RAG architecture (Bedrock Knowledge Bases on Aurora pgvector) supporting a PCI DSS environment; operates an n8n automation platform with 13+ production alerting workflows; governs organization Bedrock access and AI spend through inventory audits and model-tiering analysis.

FinOps, Vendor & Audit Governance

- Stewards the ~USD $2.9M annual cloud and SaaS footprint: cost observability pipelines, monthly service-level decomposition, anomaly root-cause analysis, and centralized cross-account CloudWatch observability spanning 64 accounts.
- Administers the AWS Marketplace subscription portfolio (11 products — Databricks, Auth0/Okta, Red Hat OpenShift, LaunchDarkly, Splunk, Fortinet, Turbot, and observability platforms) including renewals, private offers, and a contract-to-contract observability vendor migration; produced the ROSA-versus-EKS business case identifying ~31% run-rate savings.
- Generates audit and control evidence via Sprinto; built and delivered a compliance knowledge base consolidating control documentation as a single source of truth.

Grow Mobility — Chief Security Officer & Infrastructure Manager

- Established and led the information-security function: web and mobile (iOS/Android) application security audits, API hardening, and infrastructure, database, and cloud security assessments.

- Built and administered the AWS environment with cloud-wide monitoring (New Relic).
- Designed and operated a data-lake platform (AWS Redshift, Glue, Athena) processing ~35 TB across 29 SQL databases and 270 DynamoDB tables for near-real-time analytics.

Advanced Solutions 2H Mexico — Solutions & Services Manager

- Designed and implemented client information-security solutions; managed medium- and long-term network re-engineering programs establishing foundations for control, administration, and performance-monitoring technologies.
- Evaluated and integrated security technologies: UTM appliances (ASIC/FPGA), on-the-fly and pre-boot encryption, token/software authentication, and SIEM/event-correlation platforms (ArcSight, NetIQ/Attachmate, Enterasys).
- Performed controlled real-attack product evaluations and contracted penetration testing.

Independent Information Security & Regulatory Consultant

- Delivered infrastructure and information-security consulting to financial-sector and government clients, including Banjército (banking), ANA Seguros (insurance), Alsis Funds, Solutrust (fiduciary services), Secretaría de Relaciones Exteriores, Secretaría del Trabajo y Previsión Social, SEDESOL/DICONSA, SKY/Novavisión, Universidad Latina (UNILA), Grupo THEOS, ITERA, McAfee, and Fortinet.
- Advised on fintech regulatory frameworks and Latin-American data-protection law (Mexico, Brazil, Chile, Colombia, Peru).
- Specialized in database query-filtering and record-transfer controls, network-anomaly detection, data-loss prevention (DLP), and IPv6 hardening for DNS, DHCP, and mail services.

Early Career — Systems Administration

- **Universidad y Escuela Internacional, S.C.** — Designed Active Directory with ACL-based segregation across administrative, academic, and student populations; administered ISA Server clusters with content filtering; integrated SUSE Linux and Informix/ADABAS-D systems.
- **EJE Technologies, S.A. de C.V.** — Remote administration of email, web hosting, and monitoring (Nagios/Cacti) on FreeBSD across SPARC and Intel x86 architectures.

TECHNICAL SKILLS

Cloud & Platforms	AWS (Organizations, IAM/SSO, EC2, VPC/Transit Gateway, RDS/Aurora PostgreSQL, DocumentDB, S3, MSK/Kafka, OpenSearch, DMS, ECS/EKS, Lambda, MWAA/Airflow, CloudFront, API Gateway, QuickSight, Bedrock, Image Builder, Transfer Family), Red Hat OpenShift (ROSA), Databricks, Cloudflare (DNS at scale, Zero Trust, Workers)
Security & Compliance	GuardDuty, CloudTrail, Security Lake, Inspector, AWS Config, KMS, Secrets Manager, WAF (AWS / Fortinet), Cloudflare Zero Trust, Okta/Auth0, Prowler, Sprinto, Steampipe/Turbot, SIEM/event correlation, vulnerability management, hardening, SPF/DKIM/DMARC, network forensics (Wireshark/tshark), penetration-testing tooling
AI & Automation	AWS Bedrock (Anthropic Claude, multi-model), LLM agent architecture and security, RAG (Bedrock Knowledge Bases, pgvector), MCP server development, n8n, Cloudflare Workers (Workflows, Durable Objects, D1, KV, AI Gateway)

Resilience & Data	AWS Backup, snapshot/lifecycle policies, BCP/DRP, DMS/CDC data integrity, Kafka replication and MinISR standards, encryption at rest & in transit
Observability	Dynatrace, Tsuga, Splunk, Amazon Managed Prometheus, Managed Grafana, OpenTelemetry, CloudWatch (cross-account OAM), Vector.dev, pgBadger
IaC & Languages	Terraform, Terragrunt, CloudFormation (StackSets), Python, Bash, PowerShell, Ruby, TypeScript/Node.js, Git
Frameworks	SOX (IT component) / ITGC / ITAC, SOC 2, ISO 27001, PCI DSS, NIST CSF, LGPD / LATAM data-protection law (working knowledge)

CERTIFICATIONS

- **In progress:** CISA, CRISC, ISO 27001 Lead Implementer/Auditor
- Contributor to b:Secure information-security magazine
- Speaker at industry events including b:Secure Conference and the Congreso de Seguridad y Software Libre

LANGUAGES & EDUCATION

- **Spanish** — Native
- **English** — Professional working proficiency (B2+)
- **Business Administration** — degree studies

ADDITIONAL

Independent work in financial markets: development of technical indicators (TradingView) and an algorithmic trading bot for automated order execution (Python, CCXT, Deribit).