Francisco De la Cruz

DevOps / Cloud Engineer · Ingeniero en Computación

Córdoba, Argentina (remoto) · franciscoo.delacruzz@gmail.com · linkedin.com/in/francisco-delacruz · github.com/FranciscoCross

---

PERFIL

Ingeniero DevOps / Cloud con ~4 años construyendo, migrando y operando plataformas **Kubernetes** productivas sobre **AWS** y **Azure** para fintech, insurtech, utilities y entornos regulados / **PCI**. Cubro todo el ciclo — IaC desde cero, GitOps, Kubernetes HA on-premise, observabilidad, seguridad cloud/SIEM y FinOps — entre nubes y bare-metal. **AWS Certified Solutions Architect – Professional.** Referente técnico interno y profesor universitario: ponente en conferencias, mentor y mantenedor de módulos de IaC.

> *Llevo plataformas Kubernetes de "frágiles y caras" a "aburridas y baratas" — entre nubes, on-premise y la red que está por debajo.*

HABILIDADES

- **Orquestación:** Kubernetes (EKS, EKS Auto Mode, on-prem kubeadm HA + etcd + kube-vip sobre vSphere), Helm, ArgoCD (GitOps/ApplicationSets), Karpenter, Cilium (CNI + Egress Gateway), Traefik, NGINX Ingress, KEDA, HPA, Longhorn (almacenamiento distribuido), Harbor (registry / pull-through cache de ECR)
- **AWS:** EKS, EC2, Lambda, API Gateway, RDS/Aurora, RDS Proxy, DynamoDB, ElastiCache, S3, EFS, ECR, SQS/SNS/EventBridge, Kinesis Firehose, MSK, CloudFront, Route 53, ACM, ALB/NLB, WAF, Cognito, OpenSearch, Control Tower, IAM Identity Center, IAM Roles Anywhere, GuardDuty/Security Hub/Inspector, Cost Explorer
- **Azure:** AKS, Azure PostgreSQL, ACR, Key Vault + Workload Identity, VNet, Application Gateway/AGIC + WAF, Front Door
- **IaC y CI/CD:** Terraform + Terragrunt (catálogo de módulos reusables), Atlantis (automatización de Terraform por PRs), CloudFormation; GitHub Actions (ARC self-hosted), GitLab CI, Bitbucket Pipelines (runners self-hosted)
- **Observabilidad:** Prometheus / kube-prometheus-stack, Grafana, Loki (+ MinIO), Mimir, Tempo, Thanos, Alloy, Datadog, New Relic, Honeycomb, OpenTelemetry
- **Datos y mensajería:** PostgreSQL, MySQL, MongoDB→DocumentDB, Kafka/MSK, RabbitMQ/Amazon MQ, OpenSearch/ElasticSearch, CDC (Debezium / Red Panda / Rising Wave / Iceberg), DMS
- **Seguridad y FinOps:** entornos PCI, SIEM sobre OpenSearch (evaluado vs Wazuh / Elastic / Datadog Cloud SIEM), IAM Roles Anywhere (X.509), Vault / External Secrets / Doppler, Kubecost, Savings Plans, Spot, reducción de ingesta de logs
- **Redes:** VPC/VNet, peering y failover multi-región, VPN IPSec / WireGuard / Pritunl, Cloudflare (Tunnel / Zero Trust Access), Private Link, HA de egress, MikroTik/RouterOS, fundamentos de BGP
- **Lenguajes/herramientas:** Python (boto3), Bash, PHP (modernización de legacy), Locust; LLM-ops (MCP, Claude API, Claude Code)

EXPERIENCIA

DevOps / Cloud Engineer — Consultora cloud (AWS Partner)

2022 – actualidad · Córdoba, Argentina (remoto)

Entregué infraestructura en más de 15 proyectos de cliente, como parte de squads DevOps dedicados y proyectos cloud end-to-end. Trabajo destacado (clientes anonimizados por industria):

Plataforma de trazabilidad fiscal y certificación digital — híbrida AWS + on-premise · Infra lead (2024–actualidad)

- Opero una plataforma de misión crítica (monolito PHP + microservicios) replicada en AWS (5 entornos) **y un datacenter**

on-premise con Kubernetes HA autogestionado (kubeadm, etcd, kube-vip).

- Construí la plataforma on-prem de punta a punta sobre **vSphere**: kubeadm HA + Cilium, almacenamiento de bloque distribuido **Longhorn** y un registry **Harbor** como pull-through cache de ECR; modernicé un componente legacy **CentOS 6 / PHP 5.4** con CI/CD containerizado y logging centralizado (Grafana Loki vía Alloy).
- Diseñé **HA del egress gateway sobre Cilium OSS** (sin licencia Enterprise): VIP flotante con kube-vip + un controller propio de label-sync que mantiene exactamente un nodo de egress vía leader-election — failover ~4–5s; diagnostiqué y resolví un cold-start de >30 min con pre-warming de IP.
- Depuré un DaemonSet CSI-SMB en **CrashLoop con ~21.000 reinicios**: dos releases de Helm del mismo driver colisionando en un puerto del host bajo `hostNetwork`.
- Adelgacé la observabilidad: Loki → MinIO, retiro de Thanos (liberé ~54 GiB de PVCs huérfanos); migraciones nginx→Traefik, ElastiCache→Redis in-cluster, DockerHub→ECR; reemplazo de keys estáticas por **IAM Roles Anywhere**.
- **FinOps:** cumplí un objetivo explícito de ~US$500/mes en dev con apagado nocturno, consolidación de NAT Gateways, NodePools Spot/On-Demand, EKS Auto Mode y Savings Plans.

Fintech de crédito al consumo y billetera digital — PCI (2024–2025)

- Ejecuté **5 upgrades de EKS in-place (1.28→1.32)** + Karpenter v0.34→v1.32 con un procedimiento repetible, validación de breaking changes y cero downtime.
- Unifiqué **~15 microservicios en 6 entornos en un único chart de Helm** y migré los despliegues a GitOps (ArgoCD ApplicationSets), eliminando el drift de configuración.
- Construí conectividad IPSec multi-túnel resiliente con entes reguladores; operé SIEM (OpenSearch) + remediación automática de GuardDuty; configuré retención de logs de 1 año para auditoría.

Fintech de emisión de tarjetas y loyalty — PCI, Azure→AWS (2025–2026)

- Tras comparar SIEM gestionados vs open-source (Datadog Cloud SIEM, Wazuh, Elastic), construí un **SIEM PCI sobre Amazon OpenSearch** (EventBridge→Firehose→S3→Lambda→OpenSearch, SSO con OKTA) ingiriendo CloudTrail, GuardDuty, VPC Flow Logs, EKS audit logs y más.
- Reemplacé Datadog por un stack propio Prometheus/Grafana/Mimir/Loki/Tempo en ~6 clústeres; recorté la **ingesta de VPC Flow Logs ~40–60%**.
- Migré Azure SQL → RDS (DMS) y armé un pipeline de CDC en streaming (Debezium→Red Panda→Rising Wave→Iceberg).

Fintech tax-tech (2022–2023) — ~25 microservicios en EKS + Lambda/API Gateway; migración **RDS→Aurora + RDS Proxy** en producción; trazas unificadas con **OpenTelemetry** (instrumentación manual + automática → Honeycomb); right-sizing FinOps.

SaaS de utilities/energía — multi-cloud (2025) — extendí una plataforma AWS/EKS+ArgoCD a **Azure** construyendo el catálogo de módulos Terraform de Azure desde cero (AKS, App Gateway, Key Vault + Workload Identity); reutilicé el mismo GitOps ArgoCD/Helm; reduje costo de ingress (AGIC→NGINX).

Otros: plataforma de cotización/insurtech de ~20 microservicios (migración a Karpenter, recuperación de caída de CI); SaaS de atención con **video Jitsi/Jibri en EKS** (Azure→AWS); apps de bienestar multi-región (EKS 1.24→1.27, IAM Identity Center); observabilidad insurtech (New Relic, EKS Auto Mode + Spot); GitOps de APIs bancarias; e-subastas govtech; migraciones de datos/BI (DMS, MongoDB→DocumentDB).

Interno y liderazgo

- Mantenedor del **Service Catalog de Terraform** de la empresa (módulos reusables, incl. EKS Auto Mode) publicados en el Terraform Registry.
- Trabajo de plataforma sobre un SaaS interno de automatización de infra: **GitHub Actions ARC** self-hosted en EKS con pool de Karpenter dedicado; lideré el post-mortem de una caída de producción.
- Redacté evidencia de **AWS Well-Architected / Service Delivery** (Graviton, API Gateway, RDS).
- Diseñé y mentoreé el **Trainee Program**; revisor de pruebas técnicas de contratación.
- **Enablement a clientes** — dicté capacitaciones prácticas (ej. Grafana) a equipos de ingeniería de clientes.
- Ponente en **Nerdearla 2025** — "Escalando apps en Kubernetes en base a requests HTTP/s"; charlas técnicas internas frecuentes.

Profesor universitario (part-time) — Diplomatura DevOps

2024 – actualidad · Córdoba, Argentina

- Dicto **Sistemas Operativos, Bases de Datos y Microservicios** en una Diplomatura DevOps profesional — fundamentos de SO (procesos, concurrencia, virtualización), contenedores y diseño de microservicios, redes y seguridad, y automatización con Bash/Python.

PROYECTOS PERSONALES DESTACADOS

Homelab self-hosted de dos nodos — Diseñé y opero un laboratorio de nivel productivo que refleja mi stack profesional: ingress **Traefik** con TLS Let's Encrypt automático (Cloudflare DNS-01) + **Authelia** SSO/2FA, DNS de red con **AdGuard**, stack completo de observabilidad **Grafana + Loki + Alloy + Prometheus** (más PCP y Scrutiny), NAS x86 con almacenamiento **RAID1 + btrfs** sobre SMB/NFS, tooling de **Kubernetes**, GitOps con GitHub Actions y malla **Tailscale** — todo declarado como IaC en Docker Compose. Expuesto públicamente con un **Cloudflare Tunnel** (ingress zero-trust, cero puertos de entrada) detrás de **Cloudflare Access** (SSO), con un edge endurecido (security headers HSTS/CSP, docker-socket-proxy read-only).

Observabilidad y seguridad de red de oficina 24/7 — Armé un stack de monitoreo completo (Grafana + VictoriaMetrics/Logs, 10 contenedores, 17 alertas → Slack) para una red MikroTik + UniFi sobre una Raspberry Pi, todo como IaC. **Mitigué un ataque de amplificación DNS en vivo** (~37× de amplificación, router usado como reflector), endurecí el firewall (anti-brute-force, drop por defecto en WAN, management fuera de Internet) y optimicé el WiFi (utilización de 2.4 GHz de 57%→29%).

CERTIFICACIONES Y FORMACIÓN

- **AWS Certified Solutions Architect – Professional** — verificable en Credly
- **AWS Academy Educator**
- Kubernetes y redes AWS (Black Belt)
- GenAI / LLM-ops (Anthropic): MCP, Claude API, Agent Skills, Claude Code — 2026

EDUCACIÓN

Ingeniería en Computación — Universidad Nacional de Córdoba (UNC-FCEFyN), 2017–2023

Proyecto integrador: *DevSecOps en entornos IoT* (nota 10/10).

IDIOMAS

Español (nativo) · Inglés (profesional)