Roberto Aguirre Guardia

Senior AI Engineer · IA Generativa y agéntica en producción (LLMs, RAG, agentes de IA) · Evals, Shadow Mode, observabilidad y guardrails · Secure by Design (OWASP LLM, IAM, prompt injection) · Banca y entornos regulados · APIs y microservicios · Inglés C1

Bogotá, Colombia · Remoto · aguirrerjg@gmail.com · +57 317 675 0419 · linkedin.com/in/roberto-javier-aguirre-guardia

RESUMEN

Senior AI Engineer que lleva soluciones de IA Generativa y agéntica a producción de punta a punta: del entendimiento del negocio y el diseño técnico a la integración, evaluación, despliegue y monitoreo. Construye y opera una plataforma **multiagente en producción** (Agent Squad) con **LLMs, RAG, agentes de IA y prompt engineering**. Domina las prácticas que el rol exige: **Shadow Mode**, evaluación de LLMs, **logging, trazabilidad, observabilidad y monitoreo** (LangFuse, Arize Phoenix), y **guardrails y seguridad aplicada a IA** (OWASP para LLM, IAM y mínimo privilegio, mitigación de prompt injection y fuga de datos, monitoreo de alucinaciones y sesgos). Desarrolla **APIs, microservicios y sistemas distribuidos** sobre su stack principal (TypeScript/Node) y un **framework de agentes propio**; usa Python para tooling y automatización. Experiencia en **banca y entornos regulados** (originación de crédito). Bajo su liderazgo, **DigitalHubAssist** alcanzó el estatus de **Registered Partner en el programa de partners de Anthropic**. Español nativo, inglés C1.

EXPERIENCIA

Head of AI, Innovación & Producto · **DigitalHubAssist** — Oct 2024 · Presente

EE. UU. (LLC) · Remoto · IA Generativa y agéntica en producción · Programa de partners de Anthropic

- **Diseña y desarrolla soluciones GenAI y agénticas de extremo a extremo** (Agent Squad): LLMs, RAG, agentes de IA y orquestación, integradas con APIs, microservicios y sistemas empresariales. Optimiza **pipelines de inferencia** (latencia, costos, escalabilidad y confiabilidad).
- Lleva soluciones a **producción** con **Shadow Mode** y estrategias de despliegue seguras, más **evaluación de calidad**, logging, trazabilidad, **observabilidad y monitoreo** (LangFuse, Arize Phoenix), y **guardrails, Secure by Design, IAM y mitigación de prompt injection y fuga de datos** (OWASP para LLM).
- Trabaja con **Producto, Datos, Arquitectura y Seguridad**; promueve reutilización de componentes y buenas prácticas. Bajo su liderazgo, **DigitalHubAssist** alcanzó **Registered Partner en el programa de partners de Anthropic**.

Gerente de Consultoría / Delivery Técnico · **NTT DATA** — Abr 2021 · Oct 2024

Multinacional (GSI Tier 1) · Banca (Grupo AVAL) · Entorno regulado

- **Soluciones en banca y entornos regulados**: dirigió **CrediCore** (originación de crédito digital), con **integración a sistemas empresariales**, paso a **producción** y trazabilidad, traduciendo requerimientos de negocio en soluciones técnicas, con equipos multidisciplinarios de hasta 50 y coordinación hasta la presidencia del banco.

Delivery e Integración de Plataformas · **VASS · GlobalHitss · Tecnocom** — 2012 · 2021

Banca · Pensiones · Seguros · Salud

- **Integración de plataformas y canales digitales** con sistemas core (Porvenir, **premio LATAMDIGITAL 2019**), APIs y migración a la nube (Azure), con foco en confiabilidad y niveles de servicio, bajo metodologías ágiles.

COMPETENCIAS

IA Generativa y agéntica: LLMs, RAG, agentes de IA y orquestación, prompt engineering, evaluación de soluciones basadas en LLMs, pipelines de inferencia (latencia, costos, escalabilidad, confiabilidad), arquitectura de soluciones de IA

Producción y despliegue: Shadow Mode, Canary, A/B y rollback, logging, trazabilidad, observabilidad y monitoreo (LangFuse, Arize Phoenix), MLOps / LLMOps, CI/CD, Docker

Seguridad aplicada a IA: guardrails, Secure by Design, IAM y mínimo privilegio, mitigación de prompt injection y fuga de datos, OWASP para LLM, monitoreo de alucinaciones, sesgos y fairness

Ingeniería y datos: APIs, microservicios y sistemas distribuidos; TypeScript / Node.js (stack principal) y framework de agentes propio; Python para tooling y automatización; PostgreSQL, pgvector, Redis; nube (Azure); modelos vía API (Anthropic Claude, OpenAI)

Dominio e idiomas: banca y entornos regulados (originación de crédito) · Ingeniería de Sistemas (U. de Lima) + MBA (Tec de Monterrey) · español nativo · inglés C1