# MATIAS ZAPF

matias@zapf.dev | linkedin.com/in/zapf | zapf.dev

## Profile

Software engineer working at the intersection of security, data, and machine learning — drawn to systems that detect fraud, vulnerabilities, and threats. Background in programming education; now focused on **cyberdefense**.

## What I'm building

Designing multi-agent systems and putting them to work — not as demos, but as pipelines that produce real output under hard verification.

- **ensamble** — a multi-agent SDLC orchestration framework where reliability is *architectural*, not prompted: the agent's output is treated as untrusted input. A fail-closed engine computes completion by re-running the project's real checks instead of believing the model, and a secret-scanning gate hard-blocks secrets in agent writes. Secure-by-default.
- **monitor** — a private, multi-source Python + Rust ingest service and Telegram bot running unattended 24/7. Strict TDD (+1k tests), architecture contracts that keep private data out of the broadcast path — enforced as a hard release gate — and a hardened secrets path: keys in the OS keyring, fail-loud, with adversarial leak-tests asserting no token reaches logs or sinks.
- **Knowledge graphs & technical writing** — I design knowledge systems and the pipelines that produce them. Privately, **apuntes.md** is an agentic pipeline (auditor□enricher loops, deterministic quality gates) that rebuilds my Cyberdefense coursework into curated, audited study material — theory, solved practice, and atomic notes — grounded in evidence-based pedagogy (Ausubel · Sweller · Mayer · Bloom · Matuschak). Publicly, I write long-form posts on my **blog** and maintain a **technical atlas** — a knowledge graph of security concepts as atomic, interlinked nodes, navigable as a D3 force-directed graph.

## Experience

### Programming Instructor — Silicon Misiones

*March 2023 - May 2025* · Remote · Cohorts of ~50 students with prior programming experience

Designed and delivered a 24-class hands-on curriculum across three progressive modules, taught live through interactive Google Colab notebooks where theory and exercises lived inline — authored with explicit pedagogical scaffolding (advance organizers, worked examples, retrieval prompts, error taxonomies).

- **Python foundations:** types and control flow, pattern matching, OOP and design patterns, error handling, modules, and file I/O — applied to ETL exercises on real-world datasets.
- **Intermediate / advanced Python:** generators and lazy evaluation, comprehensions, closures and decorators (timer, debug, memoize), regex-driven validation and extraction, ETL pipelines built around `@dataclass` and `match/case`.
- **Data Science & AI:** NumPy vectorization, REST API integration with caching, Pandas data wrangling, data visualization with Seaborn/matplotlib, SQL and SQLAlchemy (Core/ORM), applied transfer learning via Hugging Face pipelines, and a closing module on exploratory data analysis (EDA).

## Education

- **B.S. in Cyberdefense** — UNDEF · *2026 – 2029, in progress*
- **Online courses:** CS50 (Harvard), The Missing Semester (MIT), Python Programming MOOC (Helsinki)

## Technical Skills

- **Languages & systems:** Python, TypeScript, Rust, SQL, Bash, Linux
- **AI & agent systems:** multi-agent orchestration, LLM application development, agentic pipelines, RAG, prompt engineering, NLP (Transformers)
- **Backend & SaaS:** Python (Django, FastAPI, async, Pydantic), Rust (Axum, Tokio), PostgreSQL (multi-tenant RLS, SQLAlchemy), Next.js, REST APIs, web scraping & bot automation
- **Data analytics:** Power BI, Pandas, NumPy, Matplotlib, Seaborn, scikit-learn, Jupyter
- **Security engineering:** threat modeling (STRIDE), secrets management, secret-scanning, supply-chain & SAST hygiene, secure SDLC
- **Engineering practices:** TDD, hexagonal architecture (ports & adapters), architecture-as-lint, CI/CD gates
- **Knowledge engineering & technical writing:** knowledge graphs (D3 force-directed), atomic notes (Zettelkasten), agentic content pipelines, static-site generation (Astro, Quartz), MDX, technical documentation, evidence-based pedagogy
- **Cybersecurity (in study):** MITRE ATT&CK, NIST CSF, ISO 27001 fundamentals
- **Spoken languages:** Spanish (native), English (B2), Portuguese (basic)