

JOHAN DAVID RODRIGUEZ CASTRO

Bucaramanga, Santander, Colombia | +57 313 878 4948 | johan.rc2020@gmail.com
github.com/Yoyagm | linkedin.com/in/johan-rodriguez-97bb29323 | johanrodriguez.is-a.dev

PERFIL PROFESIONAL

Estudiante de último semestre de Ingeniería de Sistemas y Software (UPB Bucaramanga), en la intersección entre ingeniería de seguridad y machine learning aplicado. Entrego herramientas, no informes: un escáner de cadena de suministro de código abierto, un clasificador de phishing que auditó su propio benchmark y publicó la cifra honesta en lugar de la que favorecía, y un dashboard de priorización de vulnerabilidades que desmontó midiendo la ventaja que venía a demostrar. Inglés C2 verificado (EF SET 80/100).

COMPETENCIAS TÉCNICAS

Seguridad y Detección: Seguridad de la cadena de suministro de software (slopsquatting), detection-as-code, mapeo a MITRE ATT&CK, priorización de vulnerabilidades basada en riesgo (CISA KEV / EPSS / CVSS), análisis de phishing y URLs, 2FA TOTP, SDLC seguro y gates de seguridad en CI

Datos, ML e IA: LightGBM, XGBoost, scikit-learn; detección de fugas de datos y diseño de evaluaciones honestas; explicabilidad con SHAP; validación agrupada, temporal y walk-forward; calibración de probabilidades; NLP con FinBERT; orquestación multiagente con CrewAI; RAG con ChromaDB; pandas / NumPy

Cloud y DevOps: AWS (IAM, VPC, EC2, Auto Scaling, ALB, RDS Multi-AZ, ECR, CloudWatch), Terraform (IaC), Docker, CI/CD con GitHub Actions, pruebas de carga con k6, Google Cloud (BigQuery ML, Cloud Storage, DLP)

Programación: Python, TypeScript / JavaScript, C#, SQL, VBA, Dart, HCL, LaTeX

Bases de Datos: PostgreSQL, MySQL, SQLite, DuckDB, ChromaDB; arquitecturas híbridas SQL / NoSQL

Métodos y Herramientas: Ágil / Scrum, desarrollo dirigido por especificación, pytest, Playwright, mypy strict, modelado UML, Git

EXPERIENCIA

Desarrollador / Soporte Técnico

GOATGuard: github.com/Yoyagm/goatguard-app | Ene 2026 – Actualidad | Pontificia Universidad Bolivariana

- Diseñé y construí GOATGuard, una plataforma full-stack de monitoreo de seguridad de red (FastAPI + PostgreSQL + Flutter), para cerrar la brecha de movilidad de los administradores que gestionan activos tecnológicos distribuidos.
- Construí un motor de clasificación automática de activos de red (routers, impresoras, cámaras) con monitoreo en tiempo real y dashboards de KPIs, y detección proactiva de port scans e intentos de intrusión, aplicando principios de Blue Team y detection engineering.

Scrum Master

Jun 2025 – Nov 2025 | Pontificia Universidad Bolivariana

- Gestioné el ciclo de vida de desarrollo bajo Scrum, facilitando las ceremonias y optimizando el Product Backlog para asegurar entrega incremental de valor.
- Contribuí al diseño de una infraestructura de alta disponibilidad orientada a 100.000 usuarios concurrentes con objetivo de latencia por debajo de 500 ms, sobre arquitecturas de datos híbridas SQL / NoSQL / en memoria.

PROYECTOS TÉCNICOS DESTACADOS

SlopGuard — Escáner de Cadena de Suministro de Código Abierto

github.com/Yoyagm/sloguard | 2026 | Independiente

- Construí un guardián de pre-instalación que puntúa dependencias de PyPI y npm frente a nombres alucinados, typosquatted y maliciosos *antes* de que se ejecute código alguno, con un motor de detección de cinco capas y cero dependencias en tiempo de ejecución.
- Aseguré la corrección con un gate de CI al ≥ 90 % de cobertura global (≥ 95 % en rutas críticas) y ocho contratos de arquitectura con import-linter, y entregué cuatro puntos de integración desde un solo núcleo: CLI, hook de pre-commit, GitHub Action y SaaS auto-hospedable.

Detector de Phishing por URL — Detección Explicable y Auditoría de Fugas

yoyagm.github.io/phishing-url-detector | 2026 | Independiente

- Audité PhiUSIIL (UCI id 967, 235.795 URLs) antes de entrenar y medí dos fugas de etiqueta independientes: una regla de una línea alcanza 99,67 % de exactitud, y features léxicas hechas a mano sobre la URL cruda el arreglo obvio siguen dando 99,51 % sin medir nada.
- Reentrené solo sobre nombres de host canonicalizados y publiqué el resultado honesto: ROC-AUC 0,937 y 70,5 % de recall con 1 % de falsos positivos, contra phishing enviado dos años después de recolectar los datos de entrenamiento.
- Lo entregué: TreeSHAP exacto reimplementado en JavaScript sin dependencias (paridad verificada a $1e-12$ contra la referencia de Python), 113 tests incluyendo guardianes de fugas con controles negativos, y un servicio FastAPI containerizado.

Dashboard de Priorización de Vulnerabilidades — CISA KEV + EPSS + NVD

github.com/Yoyagm/vuln-prioritization-dashboard | 2026 | Independiente

- Construí una tubería de ingesta reproducible sobre tres feeds públicos que ordena 359.399 CVEs vivos, con contratos de datos versionados y tests de esquema que rompen la build cuando un feed cambia de forma.
- Reproduce la afirmación de la industria de que EPSS es $6,1\times$ más eficiente que CVSS, y luego demostré con puntuaciones congeladas en cinco cortes que la mayor parte es artefacto de evaluación: EPSS gana la cabeza de la cola ($1,2-1,8\times$) y pierde la cola larga ($0,5-0,7\times$).

Además: infraestructura AWS de tres capas en alta disponibilidad con Terraform + GitHub Actions ([eval-final-dgiti](#)) | tubería autónoma de ML y agentes para mercados, 505 tests | GreenPulse, plataforma agronómica offline-first. Casos de estudio completos: johanrodriguez.is-a.dev/proyectos.

FORMACIÓN

Ingeniería de Sistemas y Software

Feb 2023 – Actualidad | Pontificia Universidad Bolivariana

- Último semestre. Cursos avanzados de arquitectura de software y diseño de sistemas; labs 1–6 de AWS Academy Cloud Foundations (IAM, VPC, EC2, EBS, Auto Scaling, balanceo).

CERTIFICACIONES

Google Cloud (2026) — 7 skill badges: Secure Lakehouse Data • Protect Sensitive Data with Data Loss Prevention • Create ML Models with BigQuery ML • Use APIs to Work with Cloud Storage • Gemini Enterprise (flujos multiagente, primera aplicación) • Vibe Coding and MCP. Google (2026) — DeepMind: Train A Small Language Model.

Cisco Networking Academy (2026) — Introduction to Cybersecurity. Hugging Face (2026) — AI Agents Course. freeCodeCamp (2026) — Machine Learning with Python • Data Analysis with Python • Scientific Computing with Python • Data Visualization • JavaScript Algorithms and Data Structures.

Idiomas: Español — Nativo • Inglés — C2 Competente (EF SET 80/100, verificado). Todas verificables públicamente en linkedin.com/in/johan-rodriguez-97bb29323.