

Gabo Rodriguez

rol Application Security · DevSecOps · Pentesting · AI Security
ubicación Buenos Aires, AR
github  GitHub (<https://github.com/y3rb1t4>)
linkedin  LinkedIn (<https://www.linkedin.com/in/grodriguezsec/>)

Ingeniero de application security y DevSecOps, con recorrido previo como pentester. Meto seguridad dentro del pipeline de entrega —threat modeling, SAST y DAST, secure SDLC— y pasé años del lado ofensivo, testeando aplicaciones web, móviles y cloud. En la parte de nube trabajo con IAM en AWS y Azure, apoyado en credenciales de vida corta en lugar de secretos estáticos, para que el acceso quede auditable.

Últimamente vengo trabajando en la seguridad de sistemas de agentes de IA: colmena, mi trust firewall open source, aplica política determinística por agente a cada tool call que hace un agente de código, sin ningún modelo en el camino crítico.

EXPERIENCIA

Senior Application Security Engineer @ Cashea 2026-02 — actualidad

AppSec Research Engineer @ Baufest 2025-05 — 2026-02

- Impulsé iniciativas de application security en varios equipos de producto.
- Ejecuté evaluaciones de seguridad con SAST, DAST y análisis mobile y cloud.
- Diseñé prácticas de secure SDLC, integrando herramientas de seguridad en los pipelines de CI/CD.

Senior Application Security Analyst @ ITTI Digital 2023-10 — 2025-04

HTB Ambassador, Argentina @ Hack The Box 2024-02 — 2025-04

Rol comunitario: referente y sostén de la comunidad argentina de Hack The Box.

Security Consultant — Application Security @ IBM 2022-06 — 2023-12

Cloud security advocate en el CoE de Cybersecurity, sobre la cuenta Banco Supervielle.

Pentester @ Just Mobile Security 2022-05 — 2023-10

Red Team @ Xelere 2022-03 — 2022-06

ETL Developer @ Charles Taylor 2021-08 — 2022-06

Tutor de entorno virtual @ Argentina Programa 2021-09 — 2023-01

Proyectista y supervisor de obra @ Ingeniería eléctrica

2010-06 — 2021-09

Once años en ingeniería eléctrica y termomecánica antes de pasar a seguridad — UTN Buenos Aires (becario y proyectista eléctrico), Galileo Technologies, Planeta Frío y Brignone. Proyecto, presupuesto y supervisión de obra.

SKILLS

application security	Threat modeling · SAST · DAST · Secure SDLC · Seguridad en aplicaciones web · Seguridad mobile · Revisión segura de código
devsecops	Seguridad en pipelines de CI/CD · Gates de seguridad automatizados · Policy as code · Infrastructure as Code · Gestión de secretos · GitLab
seguridad ofensiva	Pentesting · Red team · Pentesting web y de APIs · Pentesting mobile · Pentesting cloud
seguridad en ia	Gobernanza de agentes de IA · Política sobre tool calls de LLMs · Defensa ante prompt injection · Límites de confianza multiagente · MCP · Threat modeling de sistemas de IA
cloud & iam	AWS IAM · Azure · STS / credenciales de vida corta · Mínimo privilegio · Modelos de madurez de IAM
lenguajes	Rust · Python · Bash · TypeScript

CERTIFICACIONES

GitLab DevSecOps Sales Specialty — GitLab
DevSecOps Essentials
Blockchain Essentials

FORMACIÓN

Ingeniería — Ingeniería Eléctrica — Universidad Tecnológica Nacional

2011-01 — 2020-07

IDIOMAS

español	Nativo
inglés	Competencia profesional (B2)
alemán	Básico