



# Alonso Veliz García

Ingeniero Informático + ADE — Ciberseguridad

📍 Valencia, España | 📩 [avelgar@outlook.com](mailto:avelgar@outlook.com) | ☎ +34 640 26 89 72 | [in Alonso Veliz Garcia](#) | [github alonsoveliz1](#)

## Sobre Mí

Reciente graduado en **Ingeniería Informática y ADE** por la Universitat Politècnica de València. Poseo experiencia práctica en la elaboración de sistemas de detección de amenazas (IDS) y en seguridad de redes. Busco forjar una carrera en el ámbito de la ciberseguridad, aunque también tengo interés en la programación, y soy competente en lenguajes como **Python** y **Rust**. Todo ello me llevó, como cúlmen del doble grado al diseño e implementación de un **IDS** para detección de tráfico malicioso basado en algoritmos de **Machine Learning**. Mi formación en ADE complementa mi perfil técnico con capacidad de documentación estructurada y resolución de problemas.

## Habilidades Técnicas

**Seguridad y Monitorización:** IDS/IPS, Análisis de Tráfico de Red, Análisis de Logs, Wireshark, TCP/IP, fundamentos SIEM.

**Programación:** Python (scripting, automatización), Rust, Bash, SQL.

**ML para Seguridad:** Scikit-learn, Pandas, ONNX Runtime, Detección de Anomalías, Clasificación de Amenazas.

**Sistemas y Herramientas:** Linux (CLI, administración), Docker, Git, Windows.

## Educación

### Doble Grado en Ingeniería Informática y ADE

Sept 2019 – Dic 2025

Universitat Politècnica de València (UPV)

- **TFG:** Layton - Sistema de Detección de Intrusiones – **Matrícula de Honor (10/10)**.

- **Asignaturas relevantes:** Redes de Computadores, Sistemas Operativos, Sistemas Distribuidos.

## Proyectos

### Layton – Sistema de Detección de Intrusiones (IDS)

[github/Layton](#)

- Desarrollé sistema de detección de amenazas en tiempo real con **98% de precisión** en flujos TCP maliciosos.
- Integración de modelos ML mediante **ONNX Runtime** para inferencia asíncrona y clasificación de amenazas.
- Implementé análisis de logs y dashboard de alertas para monitorización de seguridad en tiempo real.
- **Stack:** Rust, Tauri, ONNX Runtime, Wireshark, Docker, React, TypeScript.

### Pipeline ML para Detección de Ciberataques

[Layton-models](#)

- Desarrollé modelos de clasificación (Random Forest, XGBoost) para detección de anomalías en red.
- Optimizado para **alto recall** minimizando falsos negativos – crítico en operaciones de seguridad.
- Procesamiento del dataset CICIDS: ingeniería de features, limpieza y análisis.
- **Stack:** Python, Scikit-learn, XGBoost, Pandas, Optuna.

## Idiomas

**Español:** Nativo    **Catalán:** Nativo    **Inglés:** B2/C1 (Cambridge FCE – Grade A)    **Francés:** A2