

# VALENTINA RAMÍREZ

*Fullstack Developer (Django + React) · Seguridad en aplicaciones · Bilingüe ES/EN*

wavival.dev@luminaw.co · +573116865766 · linkedin.com/in/wavival · github.com/wavival · wavival.dev

## PERFIL PROFESIONAL

Desarrolladora fullstack con más de dos años construyendo productos digitales reales con Django REST Framework, PostgreSQL y React. Fundadora de Lúmina W. Integro IA funcional mediante la API de Claude y aplico criterio de seguridad desde el diseño. Bilingüe español/inglés B2.

## HABILIDADES TÉCNICAS

**Backend:** Python · Django · Django REST Framework · PostgreSQL · JWT · APIs REST

**Frontend:** React · TypeScript · JavaScript · Tailwind CSS · Astro

**Seguridad:** OWASP · MITRE ATT&CK; · PTES · Pentesting · Desarrollo seguro

**IA & Tools:** Claude API · Prompt Engineering · n8n · Git · Linux · Postman · CI/CD

## EXPERIENCIA LABORAL

**Lógica — Frontend Developer & UI Tester** Oct 2025 – Dic 2025 · Medellín, Colombia · Remoto

- Desarrollé componentes reutilizables con React e integré APIs REST en productos reales.
- Ejecuté pruebas de UI y funcionales sobre Be Kind Network, Newo y Lógica, documentando más de 50 bugs e inconsistencias.

**Amazon — Agente Bilingüe** Sep 2024 – Feb 2025 · Medellín, Colombia · Remoto

- Atendí clientes en inglés y español en entornos de alto volumen, desarrollando comunicación técnica clara bajo presión.

## PROYECTOS TÉCNICOS

**TerraCore [Live]** — terracoreapp.co · app.terracoreapp.co

*Python · Django REST Framework · PostgreSQL · JWT · React · TypeScript · Tailwind CSS*

- SaaS B2B para digitalizar operaciones agropecuarias en Colombia, sector con brecha tecnológica crítica.
- Arquitectura multitenancy: cada empresa accede a sus datos de forma aislada sobre una sola instancia.
- Módulos en desarrollo: inventario de insumos con rotación automática, producción por lote, salud animal y dashboard en tiempo real.
- API REST con autenticación JWT, endpoints protegidos por rol y serialización con DRF.
- Frontend en React + TypeScript consumiendo la API propia; diseño responsivo con Tailwind CSS.
- Modelado relacional complejo: productos, lotes, animales, usuarios y organizaciones en PostgreSQL.

### **NullBreach [Live]** — [wavival.dev/nullbreach](https://wavival.dev/nullbreach) · [github.com/wavival/nullbreach-api](https://github.com/wavival/nullbreach-api)

*Python · Django REST Framework · PostgreSQL · JWT · Claude API · React · TypeScript · Astro*

- Aplicación fullstack de seguridad con autenticación JWT y gestión de sesiones.
- Motor de análisis de fragmentos de código contra OWASP Top 10: detecta vulnerabilidades comunes como inyección SQL, XSS, hardcoded secrets y manejo inseguro de errores.
- Chat de IA integrado vía Claude API con contexto persistente de conversación e historial por usuario en base de datos.
- Backend desacoplado en Django REST Framework; frontend en Astro + React con TypeScript.
- Endpoints protegidos por autenticación; respuestas paginadas y caché de consultas frecuentes.

### **Root [Live]** — [wavival.dev/root](https://wavival.dev/root)

*Python · Django REST Framework · PostgreSQL · React · Claude API*

- PWA para personas con restricciones alimentarias (celiaquía, diabetes tipo 2, intolerancia a la lactosa).
- Scanner de etiquetas nutricionales por IA: el usuario fotografía un producto y Claude analiza ingredientes contra su perfil de restricciones.
- Sistema de recetas curadas con filtrado estricto por múltiples condiciones simultáneas.
- Diario de consumo offline-first con sincronización posterior al backend.
- Perfil de salud persistente que personaliza todas las respuestas del modelo.

### **Forgotten Portal [Laboratorio]** — [github.com/wavival/forgotten-portal-writeup](https://github.com/wavival/forgotten-portal-writeup)

*Nmap · Gobuster · Netcat · Python · MITRE ATT&CK; · PTES · Linux · DockerLabs*

- Ejercicio completo de pentesting ofensivo sobre máquina virtual en DockerLabs.
- **Fases:** reconocimiento con Nmap y Gobuster, explotación de upload PHP sin validación, reverse shell con Netcat, escalada de privilegios a root.
- Vulnerabilidades identificadas y clasificadas: CWE-615 (info en comentarios), CWE-434 (upload sin restricción), CWE-312 (credenciales en claro), CWE-321 (clave hardcodeda), CWE-269 (privilegios excesivos).
- Documentado con metodología PTES y TTPs mapeados a MITRE ATT&CK.; Writeup publicado.

## **EDUCACIÓN**

### **Universidad EAFIT** | *Nodo Nov 2025 – Abr 2026*

- *Diplomado en Ciberseguridad (Operaciones SOC)*

### **SENA** | *Oct 2025 – Dic 2027*

- *Tecnología en Análisis y Desarrollo de Software (ADSO) · En curso*

### **Platzi** | *Jun 2025 – Presente*

- *Django · React · Desarrollo con IA · En curso*

### **Universidad de San Buenaventura** | *Ago 2023 – Nov 2027*

- *Profesional en Lengua Inglesa · En curso*