



# #Roadmap

## Cronología de mi Hoja de Ruta Profesional

No sigo solo un plan de estudios, sigo un plan de acción. Aprendo investigando y creando, proyecto tras proyecto. Cada avance está respaldado por práctica real, documentación técnica y mejora continua.

### 2024–2025 | Fundamentos consolidados

*Primeros dos años (ya logrado)*

- Formación sólida en sistemas operativos, redes, seguridad y administración Linux.
- Desarrollo de proyectos prácticos de **bastionado web**, **automatización con Bash** y **auditorías técnicas**.
- Creación y publicación de mi **portafolio técnico profesional** (rafaelmperez.com).
- Obtención del título de **Sistemas Microinformáticos y Redes (SMR)**.
- Obtención de certificaciones **Cisco CCST Cybersecurity**, **Cisco Ethical Hacker** y **Google Cybersecurity certificate**.

### 2025–2026 | Expansión técnica y certificaciones

*Próximos pasos (6–12 meses)*

- Profundizar en **seguridad ofensiva y defensiva**, combinando práctica con simulaciones reales.
- Obtener certificaciones base: **CompTIA Security+**, **LPIC-1** y **Cisco CCNA**
- Montar un **laboratorio propio de ciberseguridad** para pruebas controladas de bastionado, ataques y respuesta a incidentes.
- Iniciar desarrollo de **scripts y pipelines de seguridad automatizada** para entornos Linux y web.

[sysadminweb@proton.me](mailto:sysadminweb@proton.me) – Rafael M. Pérez (2025)

Portafolio técnico - [rafaelmperez.com](https://rafaelmperez.com)





## 2026–2028 | Profesionalización y especialización

*Meta a medio plazo (1–3 años)*

- Participar en **proyectos profesionales o colaborativos** de ciberseguridad y automatización.
- Contribuir a la comunidad mediante **repositorios open source**, artículos técnicos y documentación pública.
- Completar el título de **Administración de Sistemas Informáticos en Red (ASIR)**.
- Preparar certificaciones avanzadas como **CompTIA CySA+**, **eJPT/eCPPT**, o **IRCP (Incident Response Certified Professional)**.
- Consolidar una metodología propia de **hardening automatizado y respuesta a incidentes** basada en estándares (OWASP, CIS, NIST).

## 2028 en adelante | Consolidación profesional

*Meta a largo plazo (3–5 años en adelante)*

- Consolidarme como **especialista en ciberseguridad ofensiva y defensiva**, con enfoque en bastionado, detección y automatización.
- Liderar **proyectos de protección de infraestructuras críticas y entornos corporativos**.
- Mantener una formación continua en **DevSecOps, análisis forense y seguridad en la nube**.
- Compartir conocimiento mediante **mentoring, cursos técnicos y documentación profesional**.

**Nota:** Esta hoja de ruta es dinámica y evoluciona según mis avances, intereses y los desafíos que voy enfrentando.

[sysadminweb@proton.me](mailto:sysadminweb@proton.me) – Rafael M. Pérez (2025)

Portafolio técnico - [rafaelperez.com](https://rafaelperez.com)





## #ROADMAP DE CERTIFICACIONES EN CIBERSEGURIDAD

### Entry Level:



1° (Completado)



2° (Completado)



3° (En curso)



4° (Planeado)

### Nivel intermedio (Especialización Blue Team):



5° (2026)



6° (2026)

#### Complementarias:

TryHackMe Blue Team Path

LetDefend SOC Analyst Labs

### Nivel Experto Blue Team:

SC-900 Microsoft



7° (2027-2028)



8° (2027-2028)

[sysadminweb@proton.me](mailto:sysadminweb@proton.me) – Rafael M. Pérez (2025)

Portafolio técnico - [rafaelmperez.com](https://rafaelmperez.com)

