RAFAEL M. **PÉREZ**

Analista de Ciberseguridad | Blue Team | Soc |SysAdmin
Ubicación: España - Sevilla (disponibilidad remota o híbrida)
rmp.blueteam@proton.me · **rafaelmperez.com** · **www.linkedin.com/in/rafaelmperez**

Analista de Ciberseguridad (**Security Analyst**) y Administrador de Sistemas en formación continua, con enfoque en **bastionado (hardening)**, **monitorización (monitoring)** y **respuesta a incidentes (incident response)**.
Combino conocimientos en Linux, Windows Server y seguridad operativa con experiencia práctica aplicando estándares **NIST, OWASP, ISO 27001 y CIS Benchmarks**.

Certificado por **Cisco (CCST Cybersecurity, CCST Networking, Ethical Hacker)** y **Google Cybersecurity Certificate**, aplico metodologías estructuradas en entornos híbridos (on-premise y cloud).
Fluido en **francés (C1)**, colaboro eficazmente en entornos internacionales.

Mi objetivo es integrarme en un **SOC / Blue Team** donde pueda aplicar habilidades en **detección, hardening, gestión de vulnerabilidades, disaster recovery y automatización defensiva**.

CERTIFICACIONES

- **CCST Cybersecurity** – Cisco (2025)
- **CCST Networking** – Cisco (2025)
- **Google Cybersecurity Certificate** (2025)
- **Ethical Hacker** – Cisco (2025)
- **IFCD072PO** – Ciberseguridad y Hacking Ético (SEPE) – 300 h
- **IFCT013** – Prevención, Análisis y Respuesta a Incidentes (SEPE) – 49 h
- **IFCM026PO** – Seguridad Informática y Firma Digital (SEPE) – 50 h

EXPERIENCIA

(2022 - 2025)

HELP DESK / SOPORTE TÉCNICO - REVEX FRANCE

Windows | Active Directory | Networking | Atención al usuario

- Brindé soporte técnico de primer nivel a usuarios en entornos Windows y Office 365.
- Diagnostiqué y resolví incidencias de hardware, red y software.
- Administré cuentas en Active Directory y gestioné accesos a recursos compartidos.
- Colaboré con técnicos de segundo nivel en la resolución de incidencias complejas.
- Desarrollé habilidades de comunicación y documentación técnica bilingüe (FR/ES).

(2006 – 2022)

OTRA EXPERIENCIA PROFESIONAL

- Desempeñé diversos roles no relacionados con IT, desarrollando competencias en gestión operativa, trabajo en equipo y resolución de problemas en entornos exigentes.
- Estas experiencias fortalecieron mi adaptabilidad, disciplina y enfoque en resultados, cualidades que aplico en mi actual trayectoria en ciberseguridad.

PROYECTOS

(TODOS LOS PROYECTOS ESTÁN DOCUMENTADOS EN MI PORTAFOLIO)

Bastionado de sistemas Ubuntu 24.04 LTS

Ubuntu | Lynis | Auditd | PAM | UFW | CIS Benchmarks

- Implementé un proceso completo de **hardening Linux**, reforzando seguridad en kernel, autenticación, servicios y red.
- Apliqué controles CIS y NIST, mejorando la puntuación de auditoría de 68 a 87 puntos con Lynis.
- Configuré Auditd, USBGuard y PAM para fortalecer la trazabilidad y control de acceso.

Bastionamiento de sitio web y seguridad perimetral

Cloudflare | OWASP ZAP | Nikto | Nmap | SSLyze

- Realicé **vulnerability testing** y reforcé la seguridad web según **OWASP Top 10**.
- Configuré Cloudflare y firewall perimetral para mitigar ataques DoS y escaneos externos.
- Documenté métricas de vulnerabilidad antes y después del bastionado, reduciendo riesgos significativamente.

Firewall dinámico con GeoIP

iptables | GeoIP | Bash | SSH | Auth.log

- Desarrollé un script automatizado que analiza logs SSH y bloquea IPs foráneas con iptables.
- Mejoré la detección temprana de accesos no autorizados y reduje incidentes de fuerza bruta un 40 %.

Sistema de detección de intrusos e integración con Grafana

Suricata | Grafana | Fail2Ban | Node Exporter | Ubuntu

- Implementé un **IDS/IPS** con monitorización en tiempo real y alertas automatizadas.
- Visualicé eventos de red y SOC mediante paneles personalizados en Grafana.

Laboratorio de pentesting local con máquinas vulnerables

Kali Linux | Metasploitable | VirtualBox | OWASP Juice Shop

- Desplegué un entorno virtual para ejercicios de pentesting y ciberdefensa.
- Analicé vectores de ataque y apliqué contramedidas de hardening para servicios críticos.

Pipeline en Bash para informes técnicos automatizados

Bash | Pandoc | IA local Gemma 2B | Markdown

- Diseñé un pipeline modular para generar informes técnicos automatizados desde terminal, mejorando trazabilidad y documentación de auditorías.

EDUCACIÓN

SEPTIEMBRE 2025 - ACTUALIDAD

TÉCNICO SUPERIOR EN ADMINISTRACIÓN DE SISTEMAS EN RED (ASIR), ILERNA

- Enfocado en administración segura, virtualización, redes y servicios.

SEPTIEMBRE 2024 - FINALIZADO

TÉCNICO EN SISTEMAS MICROINFORMÁTICOS Y REDES (SMIX), ILERNA

- Formación en mantenimiento de equipos, soporte técnico, redes LAN/WAN y seguridad básica.

HABILIDADES (SKILLS)

- Administración de sistemas **Linux y Windows Server**
- Hardening y aplicación de estándares **CIS, NIST, OWASP, ISO 27001**
- **Information Security**, **Vulnerability Testing**, **Disaster Recovery**, **Security Policies**
- **Respuesta a incidentes** (SIEM básico, Suricata, Fail2Ban)
- **Automatización defensiva** con Bash y Ansible
- Gestión básica de entornos **AWS y Azure (Cloud Security)**
- **Analytical Skills, Problem-Solving y Communication** técnica bilingüe (FR/ES)

COMPETENCIAS TÉCNICAS

Linux, Ubuntu, Kali Linux, Windows Server, Bash, Ansible, Suricata, Grafana, Fail2Ban, UFW, PAM, Auditd, USBGuard, Lynis, iptables, GeoIP, OWASP ZAP, Nmap, Nikto, SSLyze, Metasploit, VirtualBox, Cloudflare, SIEM, IDS/IPS, Threat Detection, Vulnerability Management, Incident Response, SOC Monitoring, Log Analysis, Syslog, Cloud Security, AWS, Azure, Security Automation, Network Defense, Forensics, CIS Benchmarks, NIST, ISO 27001, OWASP Top 10, Python (básico), GitHub, Markdown, Pandoc, IA Local, Documentation, Ethical Hacking, Blue Team, Red Team Fundamentals.

AVISO LEGAL

*Este currículum forma parte del **portafolio profesional de Rafael M. Pérez** y se publica exclusivamente con fines **informativos y de presentación profesional**.*
*Queda **prohibida su reproducción, modificación o uso con fines comerciales o no autorizados**.*

Todos los proyectos, certificaciones y experiencias reflejados son **reales y verificables**, disponibles para consulta en **rafaelmperez.com**
