Rafael Antonio Pérez Llorca

Ciberseguridad (Blue Team / Gestión de Incidentes)

Madrid, España · +34 673 571 559 · leafar1087@gmail.com · LinkedIn: https://www.linkedin.com/in/rperezll/

Disponibilidad: incorporación inmediata · Habilitado para trabajar (Visa de estudiante - 30 h/sem)

Perfil

Ingeniero Informático con sólida trayectoria en gestión de sistemas críticos, gobierno de datos y seguridad en el sector público (Policía Nacional del Perú). Actualmente cursando Máster en Ciberseguridad en CEU San Pablo. Especializado en estrategias Blue Team, cumplimiento normativo (RGPD/ISO 27001) y coordinación entre equipos técnicos y de negocio. Docente universitario de posgrado en Ciberseguridad. Busco aplicar mi experiencia en gestión de incidentes y *security by design* en el mercado español.

Formación académica

- Máster en Ciberseguridad (en curso) — Universidad CEU San Pablo, Madrid | Oct 2025 – Actualidad
- Maestría en Ingeniería de Sistemas (Gestión TIC) — Universidad César Vallejo, Perú
- Ingeniero en Ingeniería Informática y de Sistemas — Universidad Privada San Pedro, Perú

Experiencia profesional

POLICÍA NACIONAL DEL PERÚ (PNP) | Lima, Perú. *Organismo de alcance nacional. Gestión de sistemas críticos de orden interno y seguridad pública*

Jefe de Proyectos TIC | Ene. 2024 – Nov. 2025

- Incorporé requisitos de seguridad (autenticación, trazabilidad, segregación de funciones, cifrado en tránsito/descanso) en Gestión Documental, SERPOL y Mi Policía Digital.
- Planifiqué y ejecuté UAT/SIT con criterios de seguridad: perfiles/roles, pruebas de acceso, errores controlados y registro de evidencias.
- Cumplimiento RGPD: minimización, retención y revisión de contratos de datos/APIs; control de cambios con auditoría.
- Gestión de incidentes: clasificación/priorización, contención funcional y lecciones aprendidas para reducir la recurrencia.

Jefe de Sección – Base de Datos e Interoperabilidad | Ene. 2023 – Dic. 2023

- Gobierno de datos: elaboré políticas de acceso y calidad; revisión de permisos y uso legítimo (mínimo privilegio).
- Seguridad en integraciones: diseñé la estandarización de contratos, control de versionado y compatibilidad segura.
- Soporte a auditorías: gestioné evidencias y respuesta a hallazgos; acciones correctivas y documentación en Confluence.

Jefe de Sección – Desarrollo de Soluciones | Ene. 2019 – Dic. 2022

- Supervisión del ciclo de vida de desarrollo para servicios digitales nacionales (antecedentes digitales, denuncia virtual, personas desaparecidas)
- Definición de requisitos no funcionales (disponibilidad, integridad, confidencialidad).
- Revisión de integraciones: contratos, sanitización de entradas, manejo de errores y políticas de logging.
- Coordinación con QA/operaciones para pruebas de seguridad básicas y criterios de salida; documentación de evidencias.

Analista de Sistemas | Noviembre 2016 – Diciembre 2018

- Levantamiento de requisitos de seguridad y privacidad; casos de uso con controles y perfiles/roles (RBAC).
- SQL para verificación funcional y validación de integridad de datos en reportes.

Experiencia docente

UNIVERSIDAD CÉSAR VALLEJO | Lima, Peru

Docente Posgrado | Septiembre 2025 - actualidad

- Asignado a las cátedras de "Mitigación y Contención de Ciberataques" e "Ingeniería Forense". Formación de nuevos especialistas en respuesta a incidentes.

Certificaciones y formación continua

- **Cloudflare Application Services & Zero Trust** | *Seguridad perimetral y acceso*
- **Análisis Forense Digital y Respuesta a Incidentes** | *Gestión de evidencias*
- **Desarrollo Backend con Python y FastAPI** | *Creación de APIs seguras*
- **Inteligencia Artificial Generativa: Chatbots en Azure** | *Integración de IA en servicios*
- **Diplomado en Telecomunicaciones, Big Data e IoT** | *Infraestructura crítica*
- **ITIL (introducción, concepción, estrategia, operación)** | *Estrategia, diseño y operación del servicio*

Competencias y herramientas

- **Ciberseguridad (Blue Team):** Gestión de incidentes (NIST/ISO), MITRE ATT&CK, Cyber Kill Chain, Hardening, Planes de respuesta (Playbooks).
- **Redes y Perímetro:** Fortinet (FortiGate, FortiAnalyzer), Cloudflare (WAF, Zero Trust), VPN (IPsec/SSL).
- **Monitorización, EDR y Forense:** Wazuh (SIEM/EDR), Wireshark (análisis de tráfico), Volatility.
- **Desarrollo y Datos:** SQL Server, PostgreSQL, Postman (APIs), Git.
- **Gestión y Normativa:** ISO 27001/27035, Protección de Datos Personales, ITIL, Jira, Confluence.
- **Inteligencia Artificial:** Uso de LLMs para clasificación de incidencias y automatización de código (Python).