Juan Rodríguez Castellano

Sistemas · Cloud · Ciberseguridad (Blue Team → Red Team)

CONTACTO

juanrodcas98@gmail.com
+34 640 103 050
Córdoba, España
reiderer.dev
/in/juan-rodriguez-castellano
github.com/juanrc98

FORTALEZAS CLAVE

- Sistemas Microsoft (AD, Entra ID, Intune)
- Operaciones SOC y SIEM (Blue Team)
- Cloud Azure y automatización
- Gestión de vulnerabilidades (CVSS)
- Virtualización y alta disponibilidad
- Autoaprendizaje y documentación

HERRAMIENTAS Y TECNOLOGÍAS

Microsoft 365 · Entra ID · Intune · Autopilot · Azure · Microsoft Sentinel (KQL) · Defender XDR · Splunk · Wazuh · LogPoint · MITRE ATT&CK · Nessus · OpenVAS · Windows Server · Linux · Active Directory · Proxmox · VMware · Pacemaker/Corosync · SQL Server · TCP/IP · PowerShell · Python · Bash

CERTIFICACIONES

- ✓ CompTIA Security+ SY0-701 (activa)
- ✓ eJPTv2 — Jr Penetration Tester (INE)
- ✓ Google Cybersecurity Professional
- ✓ Microsoft MD-102 — en preparación

Horizonte: AZ-104, AZ-500, OSCP

IDIOMAS

Español: Nativo
Inglés: B2 — competencia profesional

DISPONIBILIDAD

Inmediata · remoto e híbrido
Movilidad nacional · turnos 24/7
Carnet: clase B

"Entiendo cómo se monta la infraestructura y cómo se defiende: ese contexto completo es mi mayor ventaja."

PERFIL PROFESIONAL

Técnico que se mueve entre los sistemas y la ciberseguridad. Base sólida en administración de entornos Microsoft híbridos (Active Directory, Entra ID, Intune, Microsoft 365, Azure) y experiencia real en operaciones SOC 24/7: monitorización SIEM, triaje de alertas, gestión de vulnerabilidades y análisis de amenazas con MITRE ATT&CK. Perfil profundamente autodidacta, con un portfolio activo de laboratorios y un blog técnico propio (reiderer.dev). Orientado a Blue Team con progresión hacia Red Team.

EXPERIENCIA PROFESIONAL

Técnico de Soporte TI — Migración Microsoft 365

Ecointegral Ingeniería (vía GI Group) — Grupo Bureau Veritas · Córdoba · Mar 2026 – May 2026

- Despliegue y migración de más de 230 endpoints Windows a Microsoft 365 con Windows Autopilot.
- Administración de identidades en Entra ID, políticas de cumplimiento en Intune y soporte N1 a usuarios.

Técnico Informático

Fersoft Informática · Córdoba (presencial y remoto) · Oct 2025 – Dic 2025

- Instalación y configuración de SQL Server, virtualización VMware y configuración de red (VLANs, switching).
- Soporte técnico N1 presencial y remoto; diagnóstico y resolución de incidencias de software y hardware.

Analista de Ciberseguridad — SOC N1 (Prácticas)

IaaS365 · Córdoba (híbrido, turnos 24/7) · Mar 2025 – Jun 2025

- Monitorización 24/7 de eventos en SIEM (Splunk, LogPoint, Wazuh) y EDR/XDR; triaje y escalado de incidentes.
- Gestión de vulnerabilidades (Nessus, OpenVAS) con priorización CVSS; análisis de IOCs y TTPs con MITRE ATT&CK.
- Auditorías ENS, phishing simulado (GoPhish) y automatización con Python y Bash.

PROYECTOS Y LABORATORIOS

- **Microsoft Sentinel Lab (Azure):** reglas KQL mapeadas a MITRE ATT&CK, playbook SOAR con Logic Apps y hunting de abuso de OAuth.
- **Wazuh SIEM Lab:** endpoint comprometido con reglas personalizadas, FIM, VirusTotal y gestión de 22 CVEs con CVSS.
- **Clúster de Alta Disponibilidad:** Pacemaker y Corosync sobre Linux con balanceo MariaDB y failover automático.
- **Red Team — CTF & write-ups:** DarkHole y Psycho: SQLi, LFI y escalada de privilegios vía SUID. Homelab con Proxmox y AD.

FORMACIÓN

CFGS — Administración de Sistemas Informáticos en Red (ASIR)

CES Lope de Vega · Córdoba · Sep 2023 – Jun 2025

Formación Especializada en Ciberseguridad (80 h)

The Bridge · Andalucía Emplea+ · Sep 2025