JUAN RODRÍGUEZ CASTELLANO

Analista Junior de Ciberseguridad · SOC & Microsoft Security

juanrodcas98@gmail.com · +34 640 103 050 · Córdoba, España · Movilidad geográfica nacional · Disponibilidad turnos 24/7

linkedin.com/in/juan-rodriguez-castellano · juanrc98.github.io

PERFIL PROFESIONAL

Analista junior de ciberseguridad formado en ASIR, con experiencia en operaciones SOC 24/7 y en despliegue de infraestructura Microsoft en entorno corporativo. Monitorización y triaje de alertas con SIEM (LogPoint, Wazuh) y EDR/XDR (Trend Micro, Cynet), aplicando MITRE ATT&CK para el análisis y escalado de incidentes. Experiencia complementaria en despliegue masivo de endpoints con Windows Autopilot y gestión de identidades en Microsoft Entra ID. Certificado CompTIA Security+ y eJPTv2, actualmente preparando Microsoft SC-200 (Security Operations Analyst). Inglés B2 profesional.

EXPERIENCIA PROFESIONAL

Técnico de Soporte TI — Proyecto migración Microsoft 365

ECOINTEGRAL INGENIERÍA, SL (vía GI Group) · Contrato temporal · Marzo 2026 – actualidad · Córdoba, presencial

Entorno: Windows 11 · Windows Autopilot · Microsoft Entra ID · Microsoft 365 · Políticas de cumplimiento

- Despliegue y migración de más de 230 endpoints Windows al entorno corporativo Microsoft 365 en el marco de la integración de Ecointegral en el grupo Bureau Veritas.
- Preparación de equipos y enrolamiento automatizado mediante Windows Autopilot.
- Gestión de identidades en Microsoft Entra ID y verificación de políticas de cumplimiento.
- Resolución de incidencias de despliegue y soporte a usuarios finales.
- Documentación técnica de procedimientos e incidencias.

Analista de Ciberseguridad — SOC N1 (prácticas)

IaaS365 · Contrato de prácticas · Marzo 2025 – Junio 2025 · Córdoba, híbrido · Turnos 24/7

Entorno: LogPoint · Wazuh · Trend Micro Vision One · Cynet · Nessus · OpenVAS · MITRE ATT&CK · ENS

- Monitorización de consolas SIEM, EDR/XDR, firewalls e IDS/IPS en turnos rotativos 24/7, gestionando alertas de múltiples clientes.
- Triaje y clasificación de alertas por criticidad, validación de eventos y descarte de falsos positivos.
- Identificación de IOCs en entornos Windows/Linux y clasificación mediante MITRE ATT&CK.
- Documentación y escalado de incidentes a N2 con análisis de causa raíz.
- Ejecución de escaneos de vulnerabilidades con Nessus y OpenVAS, priorización CVSS y seguimiento de remediación.
- Colaboración en campañas de phishing simulado con GoPhish y auditorías conforme al Esquema Nacional de Seguridad (ENS).
- Automatización de tareas de análisis de logs mediante scripting en Bash.

Técnico Informático

Fersoft Informática · Jornada completa · Octubre 2025 – Diciembre 2025 · Córdoba, presencial

Entorno: Windows · SQL Server · Software de gestión contable · Soporte remoto

- Soporte técnico e implantación de software de gestión empresarial en pymes, en el marco del despliegue nacional de Verifactu (posteriormente aplazado por el Gobierno).
- Instalación y configuración de SQL Server, creación y vinculación de bases de datos.
- Integración de software de facturación y adaptación a requisitos de Verifactu.
- Soporte presencial y remoto a usuarios finales, diagnóstico y resolución de incidencias de software y periféricos.

PROYECTOS Y LABORATORIOS

Laboratorio Wazuh SIEM — Preparación técnica para proyecto freelance (Marzo 2026)

- Preparación técnica para un proyecto de tuning de SIEM propuesto por un tercero, finalmente no ejecutado por cancelación del cliente.

- Despliegue de Wazuh en entorno de laboratorio y estudio de agentes, decoders y reglas personalizadas.
- Configuración de File Integrity Monitoring (FIM), integración con VirusTotal y mapeo de reglas a MITRE ATT&CK.

Portfolio adicional disponible en juanrc98.github.io

COMPETENCIAS TÉCNICAS

SIEM	LogPoint · Wazuh (reglas, decoders, FIM) · Splunk (nociones SPL)
EDR / XDR	Trend Micro Vision One · Cynet
Microsoft Security	Microsoft Sentinel (en desarrollo) · Microsoft Entra ID · Windows Autopilot · Defender (fundamentos)
Vulnerabilidades	Nessus · OpenVAS · priorización CVSS
Detección / Threat Intel	MITRE ATT&CK; · IOCs · VirusTotal · Cyber Kill Chain
Sistemas	Linux (Debian, Ubuntu) · Windows Server · Active Directory
Scripting	Bash · Python (básico) · PowerShell (básico)
Frameworks	MITRE ATT&CK; · NIST CSF · ISO 27001 · ENS · OWASP Top 10

CERTIFICACIONES

- **CompTIA Security+ SY0-701** — Nov 2025 / Nov 2028
- **eJPTv2 — Junior Penetration Tester** (INE Security) — Dic 2025 / Dic 2028
- **Google Cybersecurity Professional Certificate**
- **Microsoft SC-200** — Security Operations Analyst — *En preparación (examen previsto junio 2026)*

FORMACIÓN ACADÉMICA

CFGS Administración de Sistemas Informáticos en Red (ASIR)
CES Lope de Vega · Septiembre 2023 – Junio 2025

Formación especializada en Ciberseguridad
The Bridge · Programa Andalucía Emplea+ (Servicio Andaluz de Empleo) · Septiembre 2025 · 80 horas

IDIOMAS

Español: Nativo · **Inglés:** B2 — Competencia profesional