



Santiago Ruiz Cajilema

Técnico de Sistemas y Redes | Ciberseguridad IT/OT

Lugo, Galicia | Disponible para teletrabajo | 673 463 119 | santiago_14_rj@icloud.com

LinkedIn: [linkedin.com/in/santiago-ruiz-cajilema](https://www.linkedin.com/in/santiago-ruiz-cajilema) | Web y CV: santiagoruiz.es

EN CIFRAS

5+ años en hospitales
60+ hospitales
4 certificaciones oficiales
720 h formación ciber OT

COMPETENCIAS

Ciberseguridad

- ISA/IEC 62443, modelo Purdue
- Zonas y conductos, IDMZ, VPN
- Análisis forense industrial
- Kali Linux, Nmap, Wireshark
- Metasploit (básico), OWASP

Redes

- TCP/IP, DNS, DHCP, NAT
- VLAN, routing y switching
- VRRP, MRP/HRP

Sistemas

- Windows Server, Windows
- Linux (Ubuntu, Kali), Bash
- Active Directory, Azure AD / MFA
- Docker, VMware, VirtualBox

OT / Industrial

- SCALANCE, SINEMA RC, PROFINET
- PLC S7-1200, TIA Portal
- Node-RED, OPC UA, SCADA

Scripting

- Python, Bash, SQL, JSON

IDIOMAS

Español: nativo

Inglés: C1, fluido · bachillerato completo en Canadá (3 años) y formación técnica en Londres

Lengua de Signos Española: B1

PERFIL PROFESIONAL

Más de 5 años de trabajo técnico en hospitales, una infraestructura crítica; los últimos 3 implantando y dando soporte a software clínico sobre **redes hospitalarias de gran tamaño** en más de 60 centros de España.

Titulado en el **Curso de Especialización en Ciberseguridad en Entornos OT** (720 h) y certificado **Cisco CCST Cybersecurity, Cisco CCST Networking, IT Specialist - Cybersecurity y Network Security Support Technician**. Busco mi primer puesto dedicado a ciberseguridad: SOC, seguridad OT o sistemas. **Inglés fluido (C1):** bachillerato en Canadá y formación en Londres.

PROYECTOS DE CIBERSEGURIDAD

Proyecto Final – Ciberseguridad y Alta Disponibilidad en Entornos OT

2026

CIFP Politécnico de Lugo · Defensa en profundidad con Siemens SCALANCE para una planta de extracción industrial

- Arquitectura por niveles (**modelo Purdue**) según **ISA/IEC 62443-3-2**: zonas y conductos en 8 VLAN, firewall de frontera **SCALANCE SC646-2C**, IDMZ y microsegmentación de células con **SCALANCE S615**.
- Acceso remoto seguro con **SINEMA Remote Connect** en la IDMZ: túneles **VPN** (OpenVPN/IPsec) con certificados **X.509**; reglas de firewall stateful con denegación por defecto y **NAT/NETMAP** para células con IP duplicadas.
- Alta disponibilidad: anillo **HRP/MRP** (SCALANCE XM408-8C y XC208) validado con cortes en caliente, **convergencia < 200 ms** sin pérdida de paquetes, y **VRRPv3** entre dos S615 para eliminar puntos únicos de fallo.
- Edge computing con **Node-RED** sobre SIMATIC IOT2000 (S7 Comm), panel web protegido con HTTPS y tokens; control con PLC S7-1200, HMI y variador de frecuencia.
- Plan de pruebas, manual de explotación segura y mejoras propuestas: IDS industrial, SIEM/Syslog, RADIUS y S7 Comm Plus con TLS.

Entorno: ISA/IEC 62443 · Purdue · SCALANCE SC646-2C, S615, XM408, XC208 · SINEMA RC · VPN · VRRPv3 · HRP/MRP · NAT · Node-RED · PRONETA

EXPERIENCIA PROFESIONAL

INYCOM

Ago 2019 – Sept 2024

Instrumentación y Componentes S.A. · Zaragoza · Hospitales de toda España

Especialista en Software de Cardiología · Implantación e Integración

2021 – 2024

- Implantación de software clínico (Sentinel, Spacelabs) sobre **infraestructuras y redes hospitalarias** en más de 60 hospitales; gestión técnica de más de 40 proyectos.
- Configuración de conectividad entre aplicaciones, servidores y equipos: TCP/IP, **VPN**, **Windows Server**, SQL Server e integración **HL7** con el HIS.
- Diagnóstico y resolución de incidencias de **comunicaciones y conectividad**, en remoto y en presencial.
- Coordinación con IT del hospital, fabricante y usuarios clave para garantizar la **continuidad del servicio**; formación a más de 100 profesionales.
- Técnico junior a mi cargo** (formación, reparto y seguimiento de su trabajo; punto de escalado de sus incidencias) y tutor de un **alumno en prácticas**, incorporado después a la plantilla.

Entorno: Redes hospitalarias · TCP/IP · VPN · Windows Server · SQL Server · HL7 · OPC UA · Soporte remoto

CERTIFICACIONES

Cisco CCST Cybersecurity

Cisco · 2025 · válida hasta 2030

Cisco CCST Networking

Cisco · 2025 · válida hasta 2026

IT Specialist – Cybersecurity

Certiport / Pearson VUE · 2025

Network Security Support Technician

Certiport / Pearson VUE · 2025

Cisco Networking Academy

Junior Cybersecurity Analyst Career Path ·
Cyber Threat Management · 2025

Verificables en Credly:

credly.com/users/santy-r

FORMACIÓN COMPLEMENTARIA

Ciberseguridad en Logística y Transporte

Redes, VLAN, VPN, firewalls, SCADA, gestión de riesgos · 150 h · 2025

Gestión de la Seguridad Informática en la Empresa

Políticas, auditoría, criptografía · 100 h · 2022

Introducción al Ethical Hacking

Nmap, Metasploit, iptables · 12 h · 2022

Hacking Web

SQLi, XSS, LFI · 6 h · 2022

Fundamentos de Redes TCP/IP · Azure AD (AZ-500)

OpenWebinars · 2022

Programación Avanzada en Python

Curso oficial Python Institute · 150 h · 2026

FORMÁNDOME AHORA

Agentes de IA y automatización

MKT Hackers · 2026 · n8n, APIs de IA

REFERENCIAS

Carta de recomendación

Director de Operaciones de Service (INYCOM) · disponible bajo petición

INYCOM — Técnico de Electromedicina

Ago 2019 – Ene 2021

Zaragoza · Etapa previa a implantación de software en la misma empresa

- Instalación, puesta en servicio y mantenimiento de equipos médicos en hospitales; diagnóstico de averías y documentación técnica.

ARALUX — Técnico de Mantenimiento Industrial

Oct 2018 – Feb 2019

Zaragoza

- Mantenimiento de instalaciones automatizadas: robots KUKA y ABB, PLC Siemens S7-1200 y TIA Portal; diagnóstico de averías en coordinación con producción.

LABORATORIO PERSONAL

Laboratorio de sistemas y seguridad

2025 – actualidad

Proyecto personal

- Máquinas virtuales Kali Linux y Ubuntu para reconocimiento con Nmap y análisis de tráfico con Wireshark.
- Administración Linux por línea de comandos (permisos, servicios, puertos), scripts Bash y servicios en Docker / Docker Compose.

CASOS PRÁCTICOS DE CIBERSEGURIDAD

Ciberseguridad en redes de Transporte y Logística

2025

Curso de 150 h (Mainjobs) · Escenario: empresa de transporte público con autobuses y trenes

- **Análisis de riesgos** de activos críticos (control de tráfico y pagos electrónicos): amenazas, impacto, probabilidad y medidas de mitigación.
- **Plan de Respuesta a Incidentes**: preparación, detección con SIEM e IDS/IPS, contención, recuperación y coordinación con INCIBE y CCN-CERT.
- **Informe de incidente real**: análisis del ataque NotPetya a Maersk y al puerto de Rotterdam (2017) con propuestas de resiliencia.
- Diseño de red segura: segmentación, firewall y ACLs, DHCP/DNS y NAT/PAT, y conectividad WAN con estaciones y flota.

FORMACIÓN ACADÉMICA

Curso de Especialización en Ciberseguridad en Entornos OT (Tecnologías de Operación)

2025 – 2026

CIFP Politécnico de Lugo · Título oficial de FP · 720 horas

- Ciberseguridad en proyectos industriales · Sistemas de control industrial seguros · Redes de comunicaciones industriales seguras · Análisis forense en ciberseguridad industrial · Seguridad integral

Técnico Superior en Automatización y Robótica Industrial

2016 – 2018

CPIFP La Salle Santo Ángel, Zaragoza · Comunicaciones industriales, informática industrial

Alberta High School Diploma (Bachillerato)

2013 – 2015

Ross Sheppard High School, Edmonton (Canadá) · Estudios en inglés