# Jorge Luis Sánchez Casanova

## Especialista en Ciberseguridad | SOC Nivel 3 | Respuesta a Incidentes | DevSecOps

R. Hélio Dirceu Woitikiw, 40 - Pinheirinho, Curitiba - PR, 81870-350 | jorgeluis961224@gmail.com | +55 (41) 99228-0044

linkedin.com/in/jorgelsc-dev | github.com/jorgelsc-dev | jorgelsc.dev

**Roles objetivo:** Cybersecurity Specialist, Security Analyst, SOC Analyst, SOC Level 3, Incident Response Analyst, Blue Team Analyst, DevSecOps Engineer, Cloud Security Engineer.

## Resumen Profesional

Especialista en ciberseguridad con más de 6 años de experiencia en respuesta a incidentes, operaciones SOC/CERT, SOC Level 3, blue team, SIEM, hardening, infraestructura crítica, cloud security y DevSecOps. Apoyó a empresas afectadas por ransomware en la contención, recuperación y prevención de recurrencias, restableciendo ambientes críticos en menos de 72 horas. Elevó en más de 3 veces la capacidad de detección mediante tuning de reglas, correlación de eventos y mejoras en SIEM. Creó un área de ciberseguridad alineada con ISO 27001 y actualmente integra seguridad, cloud security y liderazgo técnico en ambientes AWS y Kubernetes.

**10+ profesionales liderados** | **5+ proyectos simultáneos** | **AWS + Kubernetes + CI/CD** | **Recuperación en menos de 72 horas** | **Detección de amenazas 3x mayor**

## Competencias Técnicas

**SOC y respuesta a incidentes:** triaje, contención, erradicación, recuperación, ransomware, playbooks, incident response, incident management, coordinación de incidentes, blue team y protección de infraestructura crítica.

**Detección y monitoreo:** SIEM, Elastic Stack, Elasticsearch, Suricata, IDS/IPS, network security monitoring, análisis de tráfico, tuning de reglas, correlación de eventos, threat hunting, investigación y reducción de falsos positivos.

**Seguridad ofensiva y gobernanza:** vulnerability management, gestión de vulnerabilidades, pruebas de penetración, penetration testing, hardening, políticas, controles, gestión de riesgos, risk management y prácticas alineadas con ISO 27001.

**Cloud y DevSecOps:** AWS, Kubernetes, Docker, Linux, IAM, WAF, CloudTrail, CloudWatch, cloud security, security automation, GitHub Actions y GitLab CI/CD.

**Automatización:** Python, Bash, integración de herramientas de seguridad, APIs HTTP, WebSocket y PostgreSQL.

## Experiencia Profesional

### Líder Técnico de Desarrollo y DevOps | Marox

**abr 2025 - actualidad**

- Lidera un equipo multidisciplinario con más de 10 profesionales y participación en más de 5 proyectos, orientando arquitectura, revisión técnica, priorización, troubleshooting y resolución de incidentes.
- Diseña y opera infraestructura para aplicaciones frontend y backend, bases de datos y servidores web en AWS, Kubernetes, Docker, Linux, Nginx y PostgreSQL, con foco en confiabilidad y escalabilidad.
- Modernizó cargas de trabajo basadas en EC2 hacia una arquitectura contenedorizada y autoescalable, con balanceo, health checks, monitoreo y alertas, reduciendo puntos únicos de falla e intervención manual.
- Estandarizó pipelines CI/CD y procesos de despliegue para crear ambientes reproducibles, mejorar la trazabilidad de los cambios y fortalecer la continuidad operacional.

### Consultor DevOps | DiangTech

**2025**

*Contrato part-time, con alcance definido y concluido*

- Condujo la migración de repositorios y del flujo de entrega hacia GitHub, estructurando automatizaciones y pipelines con GitHub Actions.
- Estandarizó branches, rutinas de integración y documentación operativa, concluyendo la transferencia de las funcionalidades previstas en el contrato.

### Líder de Ciberseguridad | Avangenio S.R.L.

**jul 2024 - ene 2025**

- Creó el área de ciberseguridad y definió políticas, controles, responsabilidades, gestión de riesgos y prácticas alineadas con ISO 27001.
- Condujo auditorías técnicas, hardening, pruebas de penetración y priorización de corrección de vulnerabilidades críticas, fortaleciendo la gobernanza y la postura defensiva.
- Capacitó a más de 80 colaboradores en cultura de seguridad, prevención de incidentes y buenas prácticas operativas.

## Experiencia Profesional - Continuación

**Especialista SOC Nivel 3 e Instructor | ETECSA** **nov 2023 - may 2024**

- Actuó en un SOC responsable de apoyar a organizaciones afectadas por incidentes de alta criticidad en telecomunicaciones y servicios esenciales, con triaje, investigación, escalamiento y coordinación de respuesta.
- Apoyó a empresas afectadas por ransomware en la contención, recuperación operacional, análisis de causa y prevención de recurrencias, restableciendo ambientes críticos en menos de 72 horas.
- Elevó en más de 3 veces la capacidad de detección mediante tuning de reglas, integración de fuentes de datos y mejora de casos de uso en SIEM.
- Formó especialistas en análisis, respuesta a incidentes y operación SOC, difundiendo procedimientos para investigación y escalamiento.

**Especialista en Ciberseguridad | OSRI CuCERT** **ene 2021 - nov 2023**

- Gestionó y coordinó incidentes cibernéticos en colaboración con organismos nacionales e internacionales, estructurando comunicación, análisis y respuesta operacional.
- Implementó monitoreo para infraestructuras críticas con SIEM, IDS/IPS, Suricata, análisis de tráfico, investigación de eventos y respuesta operacional.
- Participó en la protección del evento G77 + China mediante monitoreo preventivo, análisis de amenazas, inteligencia operacional y mitigación de incidentes.

## Proyectos Open Source

**wsbuilder** github.com/jorgelsc-dev/wsbuilder
Framework modular en Python para servidores HTTP y WebSocket, con ORM SQLite, cache, seguridad, métricas, tareas en background, DNS local y replicación. Proyecto mantenido con documentación, pruebas, versionado y releases públicos.

**PortHound** github.com/jorgelsc-dev/porthound
Scanner de red en Python para auditorías autorizadas, con TCP, UDP, ICMP y SCTP, banner grabbing, persistencia SQLite, API HTTP/WebSocket e interfaz en Vue 3; distribuido públicamente como **porthound4**.

**SniffHound** github.com/jorgelsc-dev/sniffhound
Capturador y analizador de tráfico en Python nativo, con modos sniffer y honeypot, parsing de protocolos, autenticación, persistencia SQLite, dashboard Vue 3 y eventos en tiempo real vía WebSocket.

## Formación Académica

**Ingeniero en Ciencias de la Computación**
Universidad de Ciencias Informáticas (UCI), Cuba | 2017 - 2023

Tesis de graduación aplicada a infraestructura crítica nacional, evaluada con nota máxima (5/5). Tutor de dos tesis de graduación, ambas evaluadas con nota máxima (5/5).

## Certificaciones

- Forense Digital | QAX Qianxin, 2024
- Monitoreo de Redes Inalámbricas | QAX Qianxin, 2024
- Gobernanza y Gestión del Ciberespacio | AIBO / Ministerio de Comercio de China, 2024
- ISO 9001 en Profundidad | Lloyd's Register, 2019

## Idiomas

**Español:** nativo | **Portugués:** básico, comprende e interactúa en situaciones simples | **Inglés:** básico