Juan David García Acevedo

Colombia • Risaralda Pereira • juan6.garcia@ucp.edu.co – ymrcuz@gmail.com • +57 3136750914

Educación

Universidad Católica de Pereira Risaralda, PEI

Ingeniería en Sistemas y Telecomunicaciones

***Articulo Científico**: System for extracting signs of suicidal ideation from texts written in Spanish language,* en publicación a Revista AiBi categorizada B, y Scopus Q4.

***Proyecto de grado**:* Software para la Extracción de Indicios de Ideas Suicidas desde Textos Escritos (MEIS).

Nota: 5.0 y postulado a trabajo de grado meritorio 2026.

***Cursos relevantes**:* Ciberseguridad, Redes de datos, *Machine Learning*, Procesamiento del Lenguaje Natural.

Actividades extracurriculares:

Representante ante el Consejo Académico (3 años),
Maratón Nacional de Programación ICPC Colombia 2024,
Grupo de Investigación en Programación Competitiva *Coders,* Líder de equipo de 3 personas (3 años),
Grupo de Investigación en Programación Competitiva *In Sillico*, Universidad Tecnológica de Pereira (3 años),
Docente Parcial en la Universidad Católica de Pereira 2024 (6 meses),
Maratón en Línea de ICPC Latinoamérica 2024,
Maratón Regional de Programación ICPC Brasil 2024,
Maratón ICPC México Gran Fecha 1 y Fecha 2 2024,
Maratón interna UTP Open 2023 Premio de primer puesto,
Maratón Nacional de Programación ICPC Colombia 2023,
Docente Parcial en la Universidad Católica de Pereira 2023 (6 meses).

Certificados y Cursos Online

INE eLearn Security

eJPT ***eLearn Junior Penetration Tester*** (c5bc8416-677c-477d-8ee2-5219b8fc010e).

i. Pentesting práctico y reconocimiento/enumeración de redes y servicios (TCP/IP, DNS, SMB, HTTP), escaneo y validación de vulnerabilidades, explotación de vulnerabilidades Windows y Linux. Pruebas de seguridad web, post explotación, recolección de credenciales, *Pivoting* y Movimiento Lateral.

ICCA ***INE Cloud Certificated Associate*** (Cursando).

i. Fundamentos de la computación en la nube incluyendo AWS, Azure, Google Cloud Platform.
ii. Gestión de la nube y fundamentos de identidad, seguridad y cumplimiento de la nube.

CyberWarfare

Web-RTA ***Web Red Team Analyst*** (698b009f398414f740f3e8fa).

i. Formación en *Pentesting* basada en el OWASP Top 10 y OWASP WSTG, BurpSuite y Nuclei.
ii. Reconocimiento y descubrimiento OSINT, DNS/Subdominios, Whois, Google Dorking y Fuzzing. Asimismo, comprensión de WAF y bypass e ataques de inyección. También ataques de autenticación y autorización bajo la concatenación de vulnerabilidades para ataques realistas.

AD-RTS ***Active Directory Red Team Specialist*** (6987d0c75f916de8158e10e9).

i. Metodología ofensiva y defensiva en entornos Microsoft de Directorio Activo como *Hardening* "Entra-ID y OnPremise-AD" al igual que flujos de autenticación/autorización e identificación de roles abusables.
ii. Competencias en detección de configuraciones incorrectas y ataques comunes ESC, técnicas de análisis y mitigación de roles Exchange OWA/EWS/MAPI/Autodiscover al igual que técnicas de escalada de privilegios en Windows.
iii. Formación en reconocimiento, acceso inicial, escalada de privilegios SQL to SYSTEM, DPAPI, movimiento lateral, suplantación con certificados, RCE en DC y exfiltración sigilosa.

CRTA ***Certified Red Team Analyst*** (6959df9e823d7631cc450d59).

i. Metodologías *Red Team*, MITRE ATT&ACK *Red Team TTPs*, Enumeración al objetivo, Reconocimiento de infraestructura

interna y externa de la organización, *Kerberos Based Attacks* y *Active Directory*, *ByPass* de redes segregadas Linux y Windows, *Pivoting* y *Lateral Movement Techniques* entre sistemas operativos.

Academia Hack4u – S4vitar

Hacking Web (51 Horas) (Cursando)

i. 31 Vulnerabilidades del OWASP y práctica de 269 Laboratorios reales / Herramienta DASTs "BurpSuite/Caido", técnicas de evasión, explotación avanzada y capacidad para entender y replicar vulnerabilidades modernas como *SSRF*, deserialización insegura, *Prototype Pollution*, *Race Conditions*, explotación de APIs, WAF ByPass, así como técnicas avanzadas para vulnerar modelos de lenguaje (LLMs) y explotar sistemas basados en inteligencia artificial.

Introducción al Hacking (53 Horas) (Cursando)

i. Fundamentos del Hacking, evaluación de vulnerabilidades, como escanear y analizar sistemas y redes, como explotar vulnerabilidades, y como reportar efectivamente los hallazgos.
ii. *Subnetting*/OSI TCP/IP, NMAP, *Fuzzing*, Docker, Enumeración de servicios comunes "FTP, SSH, HTTP-HTTPS, SMB" y gestores de contenido "WordPress, Joomla, Drupal, Magento" y "BurpSuite, Caido, WireShark, Metasploit, SQLMap".
iii. Vulnerabilidades dentro del OWASP TOP 10 "un total de 37 vulnerabilidades comunes" y explotación de malas configuraciones en sistemas Linux.
iv. Técnicas de escalada de privilegios Linux, Buffer Overflow.

Python Ofensivo (35 Horas) (1618-2315-5584-2483)

i. Dominio de Python desde lo básico hasta Programación Orientada a Objetos, herencia, polimorfismo, módulos, paquetes y gestión de datos, biblioteca estándar de Python y desarrollo de aplicaciones GUI.
ii. Python Ofensivo; desde técnicas de *pentesting* y *web scraping* hasta la construcción de herramientas, como escáneres de red, envenenadores ARP, rastreadores, interceptores, *keyloggers*, *malware* y *Forward Shells*.

Personalización de Entorno Linux (3 Horas) (3954-6028-1362-3450).

i. Configuración de sistemas Linux, proyectos Git y *dotfiles*.

Introducción a Linux (15 Horas) (1618-2315-5584-2483).

i. Bases fundamentales de Linux, Consola-Terminal en lenguaje Bash, Scripting de herramientas.

Cisco Networking Academy

Introduction to Cybersecurity

Colombo Americano Risaralda, PEI
English Language Proficiency: B2 *Level* (*CEFR*). Dec 15, 2021

Institución Educativa Byron Gaviria Risaralda, PEI
Bachiller Académico. Nov 25, 2020

Servicio Nacional de Aprendizaje (SENA) Risaralda, PEI
Técnico en Programación de Software. Nov 25, 2020
ACMESKILLS. 2019
Fortalecimiento de la Lógica y el Pensamiento Matemático como Herramienta en el campo de la Tecnología. 2019
Motivación y Liderazgo. 2019

Experiencia

Bug Bounty

Prosavis Vulnerability Disclosure Program VPD Ene 2026

i. Desde una auditoria web se reporta una vulnerabilidad con severidad alta conocida como *Information Leakage* al sitio web de Prosavis a través de un trabajo de *Pentesting/*Hacking ético a los activos de la empresa.

Juan David García Acevedo

Capture The Flag Player – Hack The Box, TryHackMe y VulnHub
***Pentesting* de máquinas Linux y Windows** 3 Años - Presente

i. Desarrollo de Scripts en Python y Bash para explotar vulnerabilidades web.
ii. Creación de un Script en Bash para establecer conexiones VPN a Hack The Box y Scripts en Python para AutoPwns.
iii. Escritura de reportes sobre máquinas vulnerables Windows y Linux (Blog personal y Excel Comunitario).

Universidad Católica de Pereira Risaralda, PEI
Docente parcial – Metodología de la Programación II 6 Meses

i. Brindé apoyo académico a estudiantes en programación orientada a objetos y desarrollo lógico.
ii. Asistencia en el diseño de soluciones para problemas algorítmicos.

Risaralda, PEI
Docente parcial – Metodología de la Programación II 6 Meses

i. Refuerzos teóricos y prácticos en programación orientada a objetos.
ii. Apoyé a los estudiantes en la conexión entre conocimientos básicos e intermedios de programación.
iii. Se potenció el pensamiento crítico y resolución sistemática de problemas a través del acompañamiento estructurado.

Universidad Tecnológica de Pereira y Universidad Católica de Pereira Risaralda, PEI
***In Sillico* y *Coders*– Programación Competitiva** Oct 2022 – Oct 2024

i. Participación en eventos internacionales a través de RPC en competencias de programación ICPC.
ii. Aplicación de algoritmos para resolver problemas en el equipo UTP Fernant, Codex y Ascii38.
iii. Colaboración semanal entre compañeros para mejorar el rendimiento como equipo y resolver retos en RPC.

ICPC Colombia – National Programming Marathon (ACIS-REDIS) Sep 2023 y Oct 2024

i. Participación en ICPC Colombia con 100 equipos de Universidades Colombianas.
ii. Solución a problemas complejos bajo presión de tiempo en entornos competitivos.
iii. Contribución a la presencia y visibilidad de la universidad en concursos nacionales de programación.
iv. Líder de equipo y contribución con clases y tutorías a los estudiantes de primeros semestres.
v. Representación para la universidad en el **UTP Open 2023**, obteniendo el primer lugar entre equipos internos.

Habilidades y Intereses

Técnicos: Python, C/C++, Java, SQL, Bash/PowerShell,
Linux server administration (Debian, Ubuntu, Arch, Red Hat) y despliegue de máquinas virtuales y Buckets/Storage en AWS, AZURE, Google Cloud Platform,
Red Team scripting y Bug Bounty en HackerOne y BugCrowd / Captura la Bandera CTFs (Hack the Box, TryHackMe, VulnHub),
Directorio Activo,
Procesamiento del Lenguaje Natural PLN y Aprendizaje de Máquina,
Conceptos de Redes de datos (Cisco).
Idiomas: Español, *English* (B2 *CEFR*, *Certified*).
Intereses: Ciberseguridad y Hacking Ético,
Desarrollo de *Scripts* en Python y *Bash* para *Pentesting* y *Red Teaming*,
Sistemas Operativos (Embebidos y Distribuidos) y Linux Kernel,
Elaboración de reportes en LaTeX.

Referencias

LinkedIn: juan-garciaa2
Ing. Juan Carlos Blandón Andrade, M.Sc.,Ph.D: Docente Investigador en Sistemas y Software, Universidad Católica de Pereira, 317 4591969, Correo: juanc.blandon@ucp.edu.co.
Ing. Rafael Ricardo Rubiano Pavia. M.Sc., Esp. en Telecomunicaciones: Docente en Telecomunicaciones, 316 5248388.