**Erazo Mendoza Jeremy Sebastian**

**INFORMACIÓN PERSONAL:**

**CI:** 1316682119

**Edad:** 22 años

**Nacionalidad:**Ecuatoriano

**Cuidad**: Quito, Pichincha, Ecuador

**FORMACIÓN ACÁDEMICA**

**Institución:  UDLA**

**Título obtenido:** **Ingeniería en Ciberseguridad**

**N° de Registo Senecyt: [Ultimo Semestre]**

**FORMACIÓN COMPLEMENTARIA:**

**CURSOS, SEMINARIOS Y CERTIFICACIONES RECIBIDOS:**

• Abril 2025. OffSec Exploit Developer (OSED) – OffSec.  
• Abril 2025. Mobile Application Penetration Tester – INE.

• Julio 2025. Burp Suite Certified Practitioner (BSCP) – PortSwigger.  
• Febrero 2025. Certified AppSec Practitioner (CAP) – The SecOps Group.  
• Abril 2025. ProLab - Dante – HackTheBox - Dr. AITH.  
• Abril 2025. ProLab - Cybernetics – HackTheBox - Dr. AITH.  
• Abril 2025. ProLab - APTLabs – HackTheBox - Dr. AITH.  
• Abril 2025. ProLab - Zephir – HackTheBox - Dr. AITH.  
• Abril 2025. ProLab - RastaLab – HackTheBox - Dr. AITH.  
• Marzo 2025. API Penetration Testing – APIsec University.  
• Marzo 2025. API Security for Connected Cars and Fleets – APIsec University.  
• Diciembre 2023. Certificado de Pentesting contra la nube de AWS (CPNA) – Spartan-Cybersecurity.

• Diciembre 2025. Advanced Malware Analysis – Information Technology Institute (ITI).  
• Diciembre 2025. Foundation Level Threat Intelligence Analyst – arcX.  
• Diciembre 2025. Partner Product Technical Training – SOCRadar®.  
• Julio 2025. Certificate Fundamentals of Dark Web – SOCRadar®.  
• Agosto 2025. Open-Source Intelligence (OSINT) Fundamentals – TCM Security.  
• Julio 2025. Certified Blockchain Practitioner (CBP) – The SecOps Group.  
• Julio 2025. Certified Network Security Practitioner (CNSP) – The SecOps Group.  
• Mayo 2025. Advanced Level Concepts in Cybersecurity – Microsoft.  
• Enero 2025. Ethical Hacker – Cisco.  
• Noviembre 2023. Cybersecurity Attack and Defense Fundamentals – EC-Council.  
• Noviembre 2025. Tenable Cloud Security Specialist – Tenable.  
• Julio 2025. Cybersecurity Fundamentals – Palo Alto Networks.  
• Julio 2025. Fundamentals of Cloud Security – Palo Alto Networks.  
• Julio 2025. Network Security Fundamentals – Palo Alto Networks.  
• Mayo 2025. Python Essentials 1 – Cisco.  
• Mayo 2025. Python Essentials 2 – Cisco.  
• Julio 2025. Adlumin Certified Engineer – Adlumin.  
• Julio 2025. Adlumin Certified MSP – Adlumin.  
• Mayo 2025. Threat Visualizer Part 1 – Darktrace.  
• Mayo 2025. Threat Visualizer Part 2 – Darktrace.  
• Abril 2025. Threat Visualizer Administration – Darktrace.

• Noviembre 2023. Google Cybersecurity Professional Certificate – Google.  
• Noviembre 2023. Google Advanced Data Analytics Professional Certificate – Google.  
• Noviembre 2023. Cybersecurity Operations Fundamentals – Cisco.  
• Noviembre 2023. Intel® Telco Cloud Academy Specialization – Intel.  
• Noviembre 2023. Meta Front-End Developer Professional Certificate – Meta.  
• Noviembre 2023. Meta Back-End Developer Professional Certificate – Meta.  
• Noviembre 2023. Splunk Search Expert – Splunk.  
• Diciembre 2023. .NET FullStack Developer Specialization – Board Infinity.  
• Marzo 2025. AWS Cloud Solutions Architect – Amazon Web Services.  
• Diciembre 2023. Oracle Cloud Infrastructure 2023 Certified Foundations Associate – Oracle.  
• Diciembre 2023. Oracle Cloud Infrastructure 2023 AI Certified Foundations Associate – Oracle.  
• Diciembre 2023. Oracle Cloud Data Management 2023 Certified Foundations Associate – Oracle.  
• Noviembre 2023. Electrodynamics Specialization – KAIST.

**EXPERIENCIA LABORAL Y PROYECTOS:**

|  |  |
| --- | --- |
| **Experiencia** | **Proyectos** |
| **Periodo:** diciembre 2025 – Actualmente **Duración:** 8 meses **Cargo:** Offensive Operations Head **Funciones:**   * Dirección del equipo Red Team a nivel regional (LATAM). * Desarrollo de herramientas ofensivas personalizadas. * Planificación de campañas de simulación de amenazas persistentes. * Evaluación de controles de seguridad mediante escenarios reales. * Realizar operaciones APT para entidades bancarias e instituciones Militares. | **Cliente: Cooperativa financiera (confidencial)**  **Nombre Proyecto:** Simulación APT LATAM **Periodo:** Confidencial **Duración:** 8 mese **Descripción del proyecto:** Emulación de amenazas persistentes avanzadas (APT) para validar controles de seguridad en infraestructura híbrida de una cooperativa financiera. Incluyó bypass de EDR, persistencia, y evaluación de procesos defensivos. **Arquitecturas:** Infraestructura híbrida, Active Directory, segmentación crítica, endpoints protegidos. **Tecnologías utilizadas:** Sliver, Cobalt Strike, BloodHound, SharpHound, RedELK, PowerShell, Sigma Rules, Python, Bash, Splunk. |
| **Cliente: Banco general Rumiñahui**  **Nombre Proyecto:** Inteligencia de Vulnerabilidades **Periodo:** Confidencial **Duración:** 6 meses **Descripción del proyecto:** Confidencial  **Arquitecturas:** Entorno cloud híbrido, microsegmentación, plataformas distribuidas. **Tecnologías utilizadas:** GitHub Actions, Semgrep, Snyk, Trivy, Dependency-Check, SBOM (CycloneDX), HashiCorp Vault, Terraform, Checkov. |
| **Cliente: Banco Pichincha Colombia**  **Nombre Proyecto:** Inteligencia de Vulnerabilidades **Periodo:** Confidencial **Duración:** 8 meses **Descripción del proyecto:** Recalificación y contextualización de findings de Rapid7 IVM con foco en riesgo técnico, exposición externa y criticidad del negocio bancario. Evaluación y explotación controlada de vulnerabilidades en activos claves. **Arquitecturas:** Infraestructura empresarial, servicios en nube y on-premise. **Tecnologías utilizadas:** Rapid7 IVM, OWASP ZAP, Burp Suite Pro, GitHub Actions, TruffleHog, Python, Snyk. |
| **Organización o Empresa:** HackerOne **Periodo:** Diciembre 2023 – Noviembre 2024 **Duración:** 11 meses **Cargo:** Bug Bounty Hunter **Funciones:**   * Identificación y explotación de vulnerabilidades en aplicaciones web, APIs REST y móviles para programas públicos y privados del sector financiero y tecnológico. * Reporte técnico detallado de fallos de seguridad como IDOR, XSS persistente, SSRF, bypass de autenticación y manipulación de lógica de negocio. * Uso de metodologías ofensivas OSINT y escaneo dirigido para ampliar la superficie de ataque sobre targets permitidos. * Automatización de payloads y pruebas mediante scripts personalizados en Python y herramientas como Burp Suite Pro, OWASP ZAP, ffuf y recon-ng. * Validación post-explotación en entornos sandbox, evitando falsos positivos y fortaleciendo el proceso de disclosure responsable. | **Cliente:** Plataformas pública y privada (confidencial) **Nombre Proyecto:** Cacería de vulnerabilidades en aplicaciones web y API **Periodo:** Confidencial **Duración:** 11 meses **Descripción del proyecto:** Identificación y explotación de vulnerabilidades críticas en plataformas web y servicios expuestos en programas públicos y privados. Enfoque en aplicaciones del sector financiero, SaaS y servicios de infraestructura. **Arquitecturas:** Aplicaciones web tradicionales, Single Page Applications (SPA), APIs REST, backends distribuidos en cloud pública. **Tecnologías utilizadas:** Burp Suite Pro, OWASP ZAP, ffuf, Interlace, JavaScript, Python, recon-ng, Bash. |
| **Organización o Empresa:** UPEC **Periodo:** Agosto 2024 – Octubre 2024 **Duración:** 2 meses **Cargo:** Teacher Training Specialist **Funciones:**   * Diseño e impartición de formación técnica especializada en ciberseguridad ofensiva para el personal docente y técnico de la **Universidad Estatal del Sur del Carchi (UPEC)**. * Elaboración de laboratorios prácticos sobre explotación de vulnerabilidades, reconocimiento activo/pasivo, y uso de herramientas Red Team. * Capacitación en conceptos clave como evasión de EDR, ingeniería inversa básica, y simulación de adversarios en entornos controlados. * Acompañamiento pedagógico en la construcción de contenidos académicos adaptados a la malla curricular de carreras de TI. * Aplicación de metodologías activas de enseñanza-aprendizaje para elevar el nivel técnico y didáctico del cuerpo académico. | **Cliente:** Universidad Estatal del Sur del Carchi (UPEC) **Nombre Proyecto:** Capacitación en técnicas ofensivas aplicadas **Periodo:** Confidencial **Duración:** 2 meses **Descripción del proyecto:** Formación técnica especializada para personal docente y administrativo en ciberseguridad ofensiva. Se impartieron sesiones prácticas sobre simulación de ataques, evasión de defensas y análisis forense en entornos controlados. **Arquitecturas:** Laboratorio simulado, infraestructura académica, entornos Windows/Linux aislados. **Tecnologías utilizadas:** Cobalt Strike, Sliver, PowerShell, SharpHound, BloodHound, Volatility, Python. |
| **Organización o Empresa:** NetSose **Periodo:** Mayo 2023 – Octubre 2023 **Duración:** 6 meses **Cargo:** IoT Researcher **Funciones:**   * Investigación aplicada en ciberseguridad de dispositivos IoT para entornos industriales y domésticos, enfocada en vulnerabilidades de firmware y protocolos propietarios. * Análisis de binarios embebidos mediante ingeniería inversa utilizando herramientas como Ghidra, Binwalk y radare2. * Evaluación de seguridad en arquitecturas ARM/MIPS y protocolos de comunicación propietarios (UART, Telnet, HTTP embebido). * Automatización de procesos de extracción y montaje de firmware utilizando scripting en Bash y Python. * Redacción de informes técnicos con hallazgos, CVEs internos, y recomendaciones para fabricantes y distribuidores tecnológicos. | **Cliente**: NetSose **Nombre Proyecto:** Investigación y análisis de seguridad en dispositivos IoT industriales y domésticos **Periodo:** Confidencial **Duración**: 6 meses Descripción del proyecto: Investigación aplicada en ciberseguridad para dispositivos IoT, con enfoque en identificación y mitigación de vulnerabilidades en firmware y protocolos propietarios. Se realizaron análisis profundos de binarios embebidos y protocolos de comunicación para mejorar la seguridad de dispositivos críticos. **Arquitecturas**: Plataformas ARM y MIPS, arquitecturas SoC, protocolos UART, Telnet y HTTP embebidos, redes aisladas de prueba. **Tecnologías utilizadas:** Ghidra, Binwalk, Firmware-Mod-Kit, radare2, scripting en Bash y Python para automatización de extracción y análisis, generación de reportes técnicos con hallazgos y recomendaciones. |
| **Organización o Empresa:** EPN-TECH **Periodo:** Diciembre 2022 – Febrero 2023 **Duración:** 3 meses **Cargo:** Full-Stack Developer **Funciones:**   * Desarrollo de una plataforma web educativa con enfoque en usabilidad y despliegue multiplataforma, en colaboración con el equipo de ingeniería de software. * Implementación de componentes front-end utilizando **React**, **Ionic** y **TypeScript**, garantizando compatibilidad móvil y diseño responsive. * Desarrollo de lógica de negocio y consumo de APIs en el lado cliente y servidor, con integraciones a bases de datos y servicios externos. * Automatización de flujos de CI/CD mediante **GitHub Actions** para testing y despliegue controlado. * Contenerización del entorno de desarrollo con **Docker** para asegurar portabilidad entre entornos locales y de producción. | **Cliente**: EPN-TECH **Nombre Proyecto:** Desarrollo de plataforma educativa híbrida **Periodo**: Confidencial **Duración**: 3 meses **Descripción del proyecto:** Desarrollo de una plataforma web educativa con funcionalidades móviles y despliegue multiplataforma, enfocada en la usabilidad y automatización de despliegues. **Arquitecturas:** Arquitectura SPA (Single Page Application), contenedores Docker, CI/CD básico. **Tecnologías** **utilizadas**: React, Ionic, JavaScript, TypeScript, GitHub Actions, Docker. |
| **Organización o Empresa:** HackSyndicate **Periodo:** Junio 2019 – Diciembre 2022 **Duración:** 3 años y 6 meses **Cargo:** Offensive Security Engineer **Funciones:**   * Participación activa en operaciones ofensivas para **entidades bancarias y cooperativas de Colombia**, desarrollando campañas de intrusión, post-explotación y movimiento lateral en redes corporativas. * Ejecución de pruebas de penetración tipo caja negra y caja gris contra infraestructuras internas y externas, incluyendo aplicaciones web, redes, servicios expuestos y APIs. * Simulación de ataques internos en entornos Windows con dominio Active Directory, explotando debilidades en Kerberos, delegaciones, políticas de grupo y relaciones de confianza. * Desarrollo y personalización de cargas maliciosas utilizando técnicas de evasión para bypass de EDR (AMSI bypass, obfuscación de scripts, DLL sideloading). * Recolección de información privilegiada mediante herramientas como **BloodHound**, **SharpHound**, **Mimikatz**, **Rubeus**, y scripting en **PowerShell** para automatizar tareas de reconocimiento y explotación. * Ingeniería inversa de malware detectado en endpoints de clientes del sector financiero: desempaquetado, análisis estático con **IDA Pro**, **Ghidra**, y análisis de comportamiento en entornos sandbox. * Generación de reglas **YARA** para detección personalizada y reporte técnico de indicadores de compromiso (IOCs). * Colaboración directa con equipos defensivos (Blue Team) durante ejercicios Purple Team, orientados a mejorar la postura de detección y respuesta en entornos productivos. * Diseño de informes técnicos ejecutivos y tácticos para áreas de TI y gerencia, con hallazgos críticos y recomendaciones accionables. | **Cliente:** Banco cooperativo colombiano (confidencial) **Nombre Proyecto:** Pentesting ofensivo interno y simulación de ataque avanzado **Periodo:** Confidencial **Duración:** 3 meses **Descripción del proyecto:** Ejecución de pruebas de penetración tipo caja negra y gris sobre la red interna de la entidad. Se evaluaron vectores relacionados con Kerberos, delegaciones inseguras, trust entre dominios, movimiento lateral y persistencia post-explotación. **Arquitecturas:** Infraestructura corporativa Windows con Active Directory, servicios bancarios internos, redes segmentadas. **Tecnologías utilizadas:** BloodHound, Rubeus, Mimikatz, PowerView, Cobalt Strike, SharpHound, PowerShell, Bash. |
| **Cliente:** Cooperativa de ahorro y crédito (confidencial) **Nombre Proyecto:** Reversing y análisis de malware dirigido a clientes financieros **Periodo:** Confidencial **Duración:** 2 meses **Descripción del proyecto:** Ingeniería inversa de malware recolectado desde endpoints de clientes, incluyendo análisis estático/dinámico, extracción de IOCs y generación de reglas YARA personalizadas. Se identificaron campañas activas contra usuarios de banca electrónica. **Arquitecturas:** Entornos Windows 10, infraestructura protegida, entornos sandbox de análisis. **Tecnologías utilizadas:** IDA Pro, Ghidra, radare2, PEStudio, Autopsy, Volatility, Python, YARA, C++. |
| **Cliente:** Entidad financiera regional (confidencial) **Nombre Proyecto:** Desarrollo de cargas ofensivas con evasión avanzada **Periodo:** Confidencial **Duración:** 6 meses **Descripción del proyecto:** Creación de payloads personalizados y técnicas ofensivas para bypass de EDR, incluyendo AMSI bypass, DLL sideloading y ejecución en memoria. Se desarrollaron herramientas ofensivas internas para mantener acceso y control post-explotación. **Arquitecturas:** Infraestructura protegida con soluciones EDR comerciales, endpoints Windows y servidores críticos. **Tecnologías utilizadas:** Cobalt Strike, Sliver, PowerShell, Python, C++, Shellter, Veil-Evasion. |
| **Cliente:** Banco cooperativo colombiano (confidencial) **Nombre Proyecto:** Ejercicios Purple Team para robustecer detección y respuesta **Periodo:** Confidencial **Duración:** 4 meses **Descripción del proyecto:** Ejecución de simulaciones Red Team junto con Blue Team para fortalecer las capacidades defensivas. Se ajustaron casos de uso en SIEM, se generaron reglas Sigma y se trabajó en la detección basada en comportamiento ofensivo real. **Arquitecturas:** Infraestructura híbrida, SIEM centralizado, endpoints con protección EDR. **Tecnologías utilizadas:** Sigma Rules, Splunk, Cobalt Strike, PowerShell, RedELK, Sysmon. |
| **Cliente:** Diversos clientes financieros (confidencial) **Nombre Proyecto:** Consultoría técnica y reporte ejecutivo/técnico de hallazgos **Periodo:** Confidencial **Duración:** Continuo (a lo largo de toda la experiencia) **Descripción del proyecto:** Redacción de informes tácticos y estratégicos post-evaluación ofensiva. Se brindaron recomendaciones accionables a equipos de TI, gerencia y oficiales de seguridad sobre segmentación, endurecimiento de sistemas y priorización de parches. **Arquitecturas:** Activos financieros críticos, redes mixtas, servidores Linux y Windows. **Tecnologías utilizadas:** Word, PowerPoint, herramientas de gestión de hallazgos, correlación de riesgos. |

**RESUMEN TECNOLOGÍAS**

|  |  |  |  |
| --- | --- | --- | --- |
| Tecnología / Herramienta | Años de Experiencia | Nivel de Conocimiento | Último Año Usado |
| Python | **5** | **Avanzado** | **2025** |
| JavaScript / TypeScript | **5** | **Intermedio-alto** | **2023** |
| React / Angular / Ionic | **4** | **Intermedio** | **2023** |
| C / C++ / ASM | **4** | **Avanzado** | **2025** |
| Bash / PowerShell | **4** | **Avanzado** | **2025** |
| PHP | **2** | **Intermedio** | **2019** |
| Java | **2** | **Básico** | **2018** |
| IDA Pro / Ghidra / Hopper / radare2 | **4** | **Avanzado** | **2025** |
| Burp Suite Pro / OWASP ZAP | **5** | **Avanzado** | **2025** |
| CodeQL / Semgrep / SonarQube | **3** | **Intermedio-alto** | **2025** |
| Snyk / Trivy / Dependency-Check | **3** | **Intermedio** | **2025** |
| OWASP ZAP CLI / Zest scripts | **3** | **Intermedio** | **2025** |
| GitHub Actions / GitLab CI / Jenkins | **4** | **Avanzado** | **2025** |
| Docker / Kubernetes / Serverless | **3** | **Intermedio** | **2025** |
| Terraform / Checkov / KICS | **3** | **Intermedio** | **2025** |
| HashiCorp Vault / GitLeaks / TruffleHog | **2** | **Intermedio** | **2025** |
| BloodHound / SharpHound / Rubeus | **4** | **Avanzado** | **2025** |
| Cobalt Strike / Sliver / Brute Ratel | **4** | **Avanzado** | **2025** |
| Splunk / Elastic / Graylog | **3** | **Intermedio** | **2025** |
| Volatility / Autopsy / Rekall | **3** | **Avanzado** | **2025** |
| CrowdStrike CSPM / Tenable / Darktrace | **2** | **Intermedio** | **2025** |

**IDIOMAS:**

* Español: Nativo
* Inglés: Intermedio - Alto