GUIDO JOEL NAVARRO VASQUEZ

Estudiante del noveno ciclo de Ingeniería de Sistemas de Información

Correo: jnavarro.vas@gmail.com
Teléfono: +51 999 004 903
Linkedin: https://www.linkedin.com/in/gjnv/
Github: https://github.com/Alpasec

PERFIL PROFESIONAL

Profesional en formación en ciberseguridad con experiencia práctica en evaluación de seguridad (entornos controlados), documentación de hallazgos y apoyo en iniciativas ISO 27001. Manejo de scripting/automatización básica, fundamentos de cloud y trabajo colaborativo. Interés en roles de SOC/GRC/AppSec donde prime el análisis, reporte y mejora continua.

EDUCACIÓN

Universidad Peruana de Ciencias Aplicadas | Agosto 2021 - Actualidad

Ingeniería de Sistemas de Información - Noveno ciclo (2025-2)

- *Miembro activo del grupo de estudio de ciberseguridad ofensiva HXPLOIT UPC*
- *Perteneciente al decimo superior de la carrera*

EXPERIENCIA

Desarrollador Trainee - CuevaTech | Junio 2025 - Noviembre 2025

- Desarrollo backend con Node.js, TypeScript, MySQL y Knex bajo arquitectura DDD y metodología Scrum.
- Gestión de versiones en Git/GitHub con pull requests, ramas y automatización mediante GitHub Actions y Docker. Automatización de pipelines y estandarización de despliegues; soporte a trazabilidad y evidencia técnica para cambios controlados.
- Apoyo en la implementación de políticas de ciberseguridad basadas en ISO 27001 para la Corporación Cueva.
- Participé en PoC de XDR: definición de criterios (cobertura/detección/falsos positivos), pruebas controladas y reporte comparativo para decisión técnica.
  Entregables:
  - Matriz de riesgos (probabilidad/impacto) y plan de tratamiento
  - Matriz de controles / mapeo a ISO 27001
  - Reportes de hallazgos
  - Inventario de activos / checklist de hardening
- Coordinación con equipos Frontend, QA, DevOps y PM para integración y aseguramiento de calidad.

Tutor - Hxploit UPC | Noviembre 2024 - Actualidad

- Coordiné y desarrollé el taller de verano de Ciberseguridad ofensiva como tutor, este taller se extendió por 8 semanas y contó con la participación de 90 alumnos en total.
- Participación activa en CTFs (Capture The Flag) nacionales e internacionales.
- Entrenamiento constante en pentesting y resolución de desafíos en web, reversing, forense y redes.
- Logro destacado: Puesto 51 de 8130 en Cyber Apocalypse CTF 2025 de “Hack the Box”.

Infraestructura y Operación de CTF

Dominio + Cloudflare + 2 VMs (host + retos) · DNS · IP estática · escalamiento de disco · capacidad/costos:

- Planifiqué y desplegué la infraestructura pública para un CTF (arquitectura con 2 VMs separadas: host y retos), priorizando aislamiento, estabilidad y facilidad de operación.
- Gestioné el perímetro con Cloudflare (dominio, DNS y proxy) para exponer servicios de forma controlada y reducir riesgo operativo durante el evento.
- Realicé capacity planning y cost optimization: evalué tamaños de VM y disco según asistencia esperada y presupuesto, ajustando recursos en el momento adecuado para evitar sobrepago antes del evento.
- Evadí downtime por cambios de infraestructura: migré/expandí almacenamiento (de disco base a uno mayor) justo al inicio del evento para soportar carga sin sobredimensionar días antes.
- Aseguré continuidad de servicio configurando IP estática en la VM host para mantener estabilidad de DNS/proxy y eliminar riesgo de caída por cambio de IP tras reinicios.
- Documenté decisiones técnicas (dimensionamiento, costos, trade-offs, procedimientos previos al evento) para operación y troubleshooting.

Comunidad de Ciberseguridad **“OverPwnZ”**(Contenido técnico / CTF writeups)

- Co-creo contenido técnico resolviendo CTFs nacionales (writeups/videos), explicando metodología (recon → explotación → evidencia → mitigación) para audiencia técnica.
- Practico y enseño fundamentos de AppSec/OSINT (OWASP Top 10 en escenarios controlados) con enfoque en aprendizaje reproducible.
- Ejecuto pruebas web en entornos controlados: enumeración, validación de inputs, explotación guiada y documentación (pasos, impacto, evidencia y recomendación).
- Familiaridad práctica con vulnerabilidades tipo inyección y fallas de control de acceso, reportando hallazgos con enfoque en remediación.

CERTIFICACIONES

- Junior Penetration Tester (PTI) - TryHackMe **Agosto 2025**
- Certified Professional Penetration Tester - INE Security **Junio 2025**
- INE Certified Cloud Associate - INE Security **Marzo 2025**
- Junior Penetration Tester - INE Security **Febrero 2025**
- Ciberseguridad: CyberSOC (C|CS) - CTIC UNI **Febrero 2025**
- Bootcamp AUDITOR ISO 27001 - Hackermentor **Diciembre 2024**
- Ciberseguridad: Ethical Hacking - CTIC UNI **Noviembre 2024**
- Ciberseguridad: Pentesting contra aplicaciones web - CTIC UNI **Noviembre 2024**
- Python Essentials 1 - Cisco **Agosto 2024**
- Scrum Fundamentals Certified (SFC) - SCRUMstudy **Junio 2023**
- FCE Cambridge English Level 1 Certificate - Cambridge English **Enero 2020**

HABILIDADES TÉCNICAS

- **Frameworks y tecnologías**: Spring Boot, .NET, Angular, Express.js, Flask, Entity Framework, DDD, REST APIs
- **Seguridad ofensiva:** Pentesting web y de infraestructura, explotación de vulnerabilidades (SQLi, XSS, LFI, SSRF, IDOR, RCE), escalamiento de privilegios, pivoting, post-explotación y análisis de configuraciones inseguras.
- **Excel / Google Sheets**: tablas dinámicas, filtros, validación de datos, XLOOKUP/VLOOKUP, seguimiento de riesgos/hallazgos.
- **Documentación**: Word/Docs, PowerPoint/Slides (reportes y presentaciones de hallazgos).
- **Sistemas operativos y entornos**: Windows Server, Linux (Ubuntu, Kali, Parrot OS), Active Directory, Docker, VirtualBox
- **Infraestructura y redes**: TCP/IP, DNS, VPN, firewalls, proxies, balanceadores, configuración de servicios seguros (HTTPS, SSH, SSL/TLS)
- **Cloud & DevSecOps**: AWS, Azure, Docker, Terraform, CI/CD con GitHub Actions, seguridad en contenedores y aplicación de controles nativos en la nube.
- **AppSec**: OWASP Top 10, vulnerability reporting, risk/severity.

HABILIDADES BLANDAS

Pensamiento analítico | Comunicación clara de hallazgos técnicos | Trabajo colaborativo | Aprendizaje autodirigido | Responsabilidad ética en entornos controlados.