Ricardo Nahuel Prieto

AI SECURITY ENGINEER

CONTACTO

Argentina
Remoto global y abierto a reubicación
Email a pedido vía LinkedIn
philocyber.com
linkedin.com/in/richieprieto

ESPECIALIDADES PRINCIPALES

AI & GenAI Security
Threat Modeling de LLMs, Sistemas Multi-Agente, MCP Security, Seguridad de Pipelines RAG, OWASP Top 10 para LLMs / Aplicaciones Agénticas / MCPs y Skills, NIST AI RMF, MITRE ATLAS

Application Security
Pentesting de Apps Web y APIs, SAST/DAST/SCA, Seguridad CI/CD, Triage de Vulnerabilidades, Revisión de Código

Gestión de Seguridad
Programas de Security Champions, Colaboración Interfuncional, Capacitación Técnica, Evaluación de Riesgos

HERRAMIENTAS Y FRAMEWORKS

MITRE ATT&CK, MITRE ATLAS, OWASP ASVS, ISO 27001, NIST CSF, Burp Suite, HackerOne, Qualys, Nessus, Python, SQL

CERTIFICACIONES

Certified AI Security Professional (CAISP)
Practical DevSecOps

Trusted AI Safety Expert (TAISE)
Cloud Security Alliance

HTB Certified Bug Bounty Hunter (cBBH)
Hack The Box & HackerOne

eWPT / eJPT
eLearnSecurity

CCSK
Cloud Security Alliance

C-AI/MLPen
Certified AI/ML Pentester

HTB Certified Offensive AI Expert (COAE)
Hack The Box · En curso

IDIOMAS

Español — Nativo

Inglés — Profesional

EDUCACIÓN

Maestría en Seguridad de la Información
Universidad de Buenos Aires (UBA)
Estimado Dic 2026

Diplomatura en Seguridad Informática
Universidad Tecnológica Nacional (UTN)
Completado 2020

RESUMEN PROFESIONAL

Ingeniero de Seguridad de IA y líder Senior de AppSec con 7+ años protegiendo aplicaciones empresariales, sistemas de IA/ML e infraestructuras complejas. Actualmente lidero programas de AI Security a nivel organizacional: modelado de amenazas de pipelines LLM, aseguramiento de sistemas multi-agente e implementaciones MCP, y establecimiento de baselines de AI Security alineados con OWASP LLM Top 10, NIST AI RMF y MITRE ATLAS.

Especializado en la intersección entre seguridad ofensiva y AI/GenAI security, con experiencia práctica en red team y blue team en empresas Fortune 500, consultoría internacional de pentesting y liderazgo de comunidades globales de ciberseguridad.

EXPERIENCIA PROFESIONAL

Senior AI Security Engineer
Jul 2026 – Presente
CookUnity — Remoto, EE.UU.

- Convocado para construir y liderar la práctica de AI Security desde cero, asegurando productos impulsados por GenAI en toda la plataforma
- Responsable del threat modeling de pipelines LLM, sistemas agénticos e integraciones MCP (OWASP Top 10 para LLMs, NIST AI RMF, MITRE ATLAS)
- Trabajo junto a los equipos de ingeniería y datos para integrar guardrails de seguridad de IA y prácticas secure-by-design en todo el SDLC

itti
Jun 2025 – Jul 2026
Remoto, Argentina

Senior AI Security Engineer
Oct 2025 – Jul 2026

Lideré la función end-to-end de AI Security y fui el punto focal de AI Security dentro de Ciberseguridad.

- Threat modeling end-to-end de aplicaciones de IA Generativa: mapeo de superficies de ataque en pipelines LLM, vectores de prompt injection y riesgos de fuga de datos
- Establecimiento de un AI Security Baseline organizacional alineado con OWASP Top 10 para LLMs, NIST AI RMF y MITRE ATLAS
- Definición de guardrails y límites de confianza para sistemas multi-agente e implementaciones MCP
- Revisiones de seguridad de configuraciones de plataformas de IA, incluyendo Kore.ai y AWS Bedrock

Senior Application Security Engineer
Jun 2025 – Oct 2025

- Program Owner del programa de Security Champions: diseño de iniciativa de cultura de seguridad que integra prácticas threat-aware en toda la organización
- Punto focal de AppSec para la estrategia de AI security de la organización, iniciando las bases del threat modeling de GenAI
- Integración de herramientas SAST, DAST y SCA en pipelines CI/CD para adelantar la seguridad (shift left)

Tutor de Ciberseguridad
Feb 2025 – Presente
TripleTen — Remoto, EE.UU.

- Mentoría especializada en seguridad ofensiva a 50+ estudiantes en sesiones en vivo
- Reducción del tiempo de aprendizaje de estudiantes en un 35% mediante rutas de aprendizaje 1 a 1 personalizadas
- Calificación de instructor de 4.9/5 según feedback de estudiantes

Co-Fundador & Ambassador
May 2024 – Presente
Hack The Box (HTB) — Argentina y Nueva Zelanda

- Fundé el meetup de HTB en Nueva Zelanda y luego me sumé como organizador al capítulo de Argentina, ayudando a crecer las comunidades a 200+ practicantes
- Negociación de alianzas con 8 instituciones para asegurar espacios de eventos 100% gratuitos, reduciendo costos en $12,000 anuales
- Coordinación de equipos cross-regionales gestionando 12 organizadores voluntarios, incrementando la retención de miembros en 45%

Senior Penetration Tester & Consultor de Seguridad
Jun 2023 – Dic 2024
Bastion Security Group — Wellington, Nueva Zelanda

- Entrega de 40+ engagements de penetration testing y evaluaciones/revisiones de configuración de seguridad en apps web, APIs, infraestructura cloud y redes
- Identificación y documentación de 250+ vulnerabilidades con estrategias de remediación accionables
- Contacto técnico principal para clientes empresariales, con 95% de satisfacción
- Contribución a 15+ propuestas ganadas por un valor de $500K+

Ricardo Nahuel Prieto

AI SECURITY ENGINEER

CONTACTO

Argentina
Remoto global y abierto a reubicación
Email a pedido vía LinkedIn
philocyber.com
linkedin.com/in/richieprieto

ESPECIALIDADES PRINCIPALES

AI & GenAI Security

Threat Modeling de LLMs, Sistemas Multi-Agente, MCP Security, Seguridad de Pipelines RAG, OWASP Top 10 para LLMs / Aplicaciones Agénticas / MCPs y Skills, NIST AI RMF, MITRE ATLAS

Application Security

Pentesting de Apps Web y APIs, SAST/DAST/SCA, Seguridad CI/CD, Triage de Vulnerabilidades, Revisión de Código

Gestión de Seguridad

Programas de Security Champions, Colaboración Interfuncional, Capacitación Técnica, Evaluación de Riesgos

HERRAMIENTAS Y FRAMEWORKS

MITRE ATT&CK, MITRE ATLAS, OWASP ASVS, ISO 27001, NIST CSF, Burp Suite, HackerOne, Qualys, Nessus, Python, SQL

CERTIFICACIONES

Certified AI Security Professional (CAISP)
Practical DevSecOps

Trusted AI Safety Expert (TAISE)
Cloud Security Alliance

HTB Certified Bug Bounty Hunter (cBBH)
Hack The Box & HackerOne

eWPT / eJPT
eLearnSecurity

CCSK
Cloud Security Alliance

C-AI/MLPen
Certified AI/ML Pentester

HTB Certified Offensive AI Expert (COAE)
Hack The Box · En curso

IDIOMAS

Español — Nativo

Inglés — Profesional

EDUCACIÓN

Maestría en Seguridad de la Información
Universidad de Buenos Aires (UBA)
Estimado Dic 2026

Diplomatura en Seguridad Informática
Universidad Tecnológica Nacional (UTN)
Completado 2020

Ingeniero de Ciberseguridad Sep 2022 – Abr 2023
Mercado Libre (MELI) Buenos Aires, Argentina

- Liderazgo de programa integral de gestión de vulnerabilidades, coordinando remediación en 15 equipos de desarrollo y 200+ aplicaciones
- Gestión de priorización de vulnerabilidades a escala empresarial integrando bug bounty de HackerOne y hallazgos de red team interno
- Automatización de escaneo de dependencias de seguridad con Python y SQL, mejorando la detección en un 40%
- Creación de capacitaciones de seguridad para 100+ desarrolladores, reduciendo patrones de vulnerabilidades recurrentes en 25%

Investigador de Ciberseguridad Dic 2020 – Sep 2022
Onapsis Buenos Aires, Argentina

- Ejecución de 30+ evaluaciones de vulnerabilidades para clientes top-tier de Norteamérica
- Revisiones de código SAST/DAST identificando 150+ fallas de seguridad
- Reportes de seguridad bilingües para ejecutivos C-level en Canadá, Argentina y mercados de EE.UU.

Analista de Seguridad Ofensiva Dic 2019 – Dic 2020
Deloitte Buenos Aires, Argentina

- Desarrollo de framework de validación de seguridad para plataformas SaaS empresariales usando automatización en Python
- Desarrollo de 15+ módulos de seguridad, previniendo 200+ potenciales vulnerabilidades de autorización
- Dictado de 20+ sesiones de capacitación como referente técnico interno

LIDERAZGO DE PENSAMIENTO

Fundador y Creador de Contenido philocyber.com
PhiloCyber

Plataforma activa enfocada en seguridad de IA/LLM, sistemas RAG e investigación en seguridad ofensiva.

- Publicación de 25+ artículos técnicos sobre seguridad de IA/LLM y metodologías de penetration testing
- Canal de YouTube con contenido educativo sobre análisis de CVEs y técnicas de evaluación de seguridad
- Comunidad digital de conocimiento con 2,000+ visitantes mensuales

INFORMACIÓN ADICIONAL

- (2019, 2020, 2022) y CHcon Christchurch Security Conference (2023)
- del refugio)
- modeling de IA en una conferencia de seguridad relevante
- Participación en Conferencias: Voluntario activo en Ekoparty Security Conference
- Servicio Comunitario: Voluntario en SPCA (departamento canino, cuidado de animales
- Objetivo de Speaking 2025: Presentación técnica sobre seguridad de LLMs o threat

DIFERENCIALES CLAVE

- de programas de seguridad
- vulnerabilidades empresariales
- con capacidad bilingüe
- miembros desde cero en dos países
- Maestría en curso, publicando contenido técnico regularmente
- Intersección de expertise única: seguridad ofensiva + seguridad de IA/ML + gestión
- Impacto probado a escala: de evaluaciones individuales a programas de
- Experiencia internacional: Argentina, Nueva Zelanda, mercados remotos de EE.UU.
- Liderazgo comunitario: construcción de una comunidad de seguridad de 200+
- Aprendizaje continuo: 7 certificaciones activas (incl. CAISP y TAISE de IA), HTB COAE y

REFERENCIAS PROFESIONALES

Disponibles a pedido. Las referencias incluyen liderazgo de seguridad de: itti (roles de AI Security y AppSec), TripleTen (Educación en Ciberseguridad), Hack The Box (Liderazgo Comunitario), Bastion Security Group (Consultoría de Pentesting), Mercado Libre (Seguridad Empresarial), Onapsis (Investigación de Seguridad), Deloitte (Seguridad Ofensiva).