OMAR PASSOS

Liderança em Segurança da Informação • Gestão de SOC, GRC e Vulnerabilidades • CISM

Curitiba, PR — Brasil (disponível para remoto/híbrido) | omar.ctba@gmail.com | +55 41 99968-1251
linkedin.com/in/omarpassos | omar-passos.vercel.app

RESUMO PROFISSIONAL

Líder de Segurança da Informação com 15+ anos em tecnologia e mais de 12 dedicados à segurança, com trajetória de analista a CISO em organizações como TOTVS, Copel, DNIT e scale-ups. Estruturo áreas de segurança do zero à maturidade: SGSI/ISO 27001, programas de gestão de vulnerabilidades baseada em risco (RBVM), operação de SOC, resposta a incidentes, LGPD e risco de terceiros. Coordeno equipes técnicas e traduzo ameaças, vulnerabilidades e exigências regulatórias em prioridades e indicadores que C-Level e board entendem. Fundador da zynTRIQ, plataforma de Attack Surface Management e GRC com quantificação financeira de risco (FAIR).

-60%	-45%	CISO	SOC
Tempo médio de triagem de vulnerabilidades	Backlog crítico com RBVM e governança de SLAs	Programa completo de segurança e conformidade	Estratégia, ferramentas e coordenação de equipe

COMPETÊNCIAS DE LIDERANÇA E GESTÃO

Gestão de pessoas e operação	Liderança de equipes de especialistas • Alocação de recursos • Acompanhamento de desempenho • Gestão de SLAs e indicadores
Governança, risco e conformidade	SGSI (ISO/IEC 27001) • LGPD/DPO • PCI-DSS • CIS Controls • PPSI 2.0 • Risco de terceiros • Auditorias internas e externas
Gestão de vulnerabilidades	RBVM • Attack Surface Management • Pentest e Purple Team • Priorização por risco real • FAIR
Detecção e resposta	Estratégia de SOC • SIEM (ELK) • EDR/XDR • SOAR • DFIR • Threat Intelligence • Playbooks
Inteligência e investigação	Inteligência Corporativa • Due Intelligence • OSINT • Análise de evidências • Reconstrução de incidentes
Base técnica	AWS, Azure e GCP • Arquitetura e hardening • Proteção de dados (DLP, classificação, tokenização) • Automação em Python e Go

EXPERIÊNCIA PROFISSIONAL

Founder & Head of Cyber Security | zynTRIQ

Jul/2023 – Presente

São Paulo, Brasil

- Idealizei e lidero o desenvolvimento da zynTRIQ, plataforma de Attack Surface Management, Vulnerability Intelligence e GRC que conecta exposição, vulnerabilidades e risco financeiro (FAIR).
- Reduzi em ~60% o tempo médio de triagem de achados com automação (Python, Go, Ruby) e padronização de processos.
- Projetei controles de proteção de dados (discovery, classificação, tokenização, mascaramento e DLP) integrados a SIEM (ELK) e pipelines de resposta, com detecção de exfiltração em cloud.
- Defini roadmap de segurança e políticas alinhadas a ISO/IEC 27001, LGPD, PCI-DSS, CIS Controls e PPSI 2.0.

Cyber Defense Center Coordinator | Task TI

Dez/2024 – Jul/2025

Curitiba, PR

- Defini a estratégia e o modelo operacional do SOC, conduzindo seleção e implantação de soluções de IVM, IDR, ASM, DFIR, MDR e OSINT.
- Liderei e desenvolvi equipe de especialistas em segurança, com alocação de recursos, acompanhamento de desempenho e gestão de entregas.
- Coordenei investigação e resposta a incidentes, da contenção à recuperação, incluindo comunicação com áreas de negócio e partes interessadas.
- Garanti conformidade regulatória por meio de auditorias e avaliações de segurança contínuas.

Arquiteto de Segurança da Informação | Copel
Jul/2024 – Out/2024

Curitiba, PR

- Projetei e implementei arquitetura de segurança com gestão e avaliação contínua de riscos em ambiente corporativo de grande escala.
- Implementei, monitorei e validei controles de segurança e conduzi iniciativas de conscientização para colaboradores.

Especialista em Segurança da Informação | meutudo.
Dez/2022 – Mai/2024

Fortaleza, CE (remoto)

- Estruturei o programa de segurança da fintech: Política de Segurança da Informação, SGSI, RBVM e gestão de risco de terceiros.
- Implantei monitoramento de segurança de aplicação com dashboards SIEM (ELK) e controles de rede (PFSense, IDS/IPS Snort e Suricata).
- Atuei em Pentest e Purple Team e liderei o programa de awareness (palestras, cartilhas, vídeos e gamificação).

CISO — Chief Information Security Officer | Exago Innovation
Jan/2022 – Nov/2022

Portugal (remoto)

- Respondi pela segurança da informação da empresa, implantando programa de segurança e conformidade com RBVM, SGSI e gestão de risco de terceiros.
- Liderei iniciativas de segurança de aplicação, gestão de risco de fator humano e cultura de cibersegurança.

Senior Information Security Analyst | TOTVS
Dez/2020 – Jan/2022

Curitiba, PR

- Contribuí para a Política de Segurança da Informação e para o programa de RBVM/SGSI em uma das maiores empresas de software do Brasil.
- Executei testes de intrusão e exercícios de Purple Team, validando controles de perímetro e detecção.
- Desenvolvi dashboards SIEM (ELK) para monitoramento e conduzi campanhas de conscientização com gamificação.

EXPERIÊNCIA ANTERIOR

Analista de Segurança / Pentester | Rentcars.com — Dez/2019 – Ago/2020
Pentest, gestão de vulnerabilidades, investigação de incidentes e disseminação de LGPD.

Consultor de Segurança, Pentester e Bug Bounty | Independente — Ago/2018 – Dez/2019
Testes de intrusão, engenharia reversa e resposta a DDoS.

Analista de Segurança de Redes | DNIT — Jun/2014 – Jun/2018
Forense digital, SIEM, análise de DDoS e gestão de firewalls (Fortigate) e VPNs.

Coordenador de TI e Projetos | Levier Tecnologia — Jul/2008 – Nov/2012
Infraestrutura, dados e desenvolvimento de sistemas com redes neurais.

FORMAÇÃO ACADÊMICA

- **Administração de Empresas**, ênfase em Comércio Exterior — PUC-PR (1998 – 2004)

CERTIFICAÇÕES

- **CISM** — Certified Information Security Manager — ISACA
- **SANS FOR508** — Advanced Computer Forensics & Incident Response — SANS Institute, 2012
- **EXIN PDPE** — Privacy & Data Protection Essentials (LGPD) — 2020
- **ISO/IEC 27001** — Foundation Essentials — PMG Academy, 2020

CURSOS E FORMAÇÃO COMPLEMENTAR

Governança, risco e privacidade	CIS Controls (ENAP, 2024) • LGPD (ENAP, 2019) • CRISC (Cybrary, 2019) • Direito Digital Contemporâneo (Unieducar, 2019) • Preparatórios CISSP, CISA, CISM e PMP (CIP Cyber, 2019)
Segurança ofensiva	OSCP – Kali Linux • Practical Ethical Hacking (Udemy) • CEH v10 (CIP Cyber, 2019) • Physical Penetration Testing (Cybrary, 2019)
Forense e investigação	Introdução à Criminalística (Unova Cursos, 2019) • Hidden Website Using TOR (CIP Cyber, 2019)
Redes, infraestrutura e nuvem	CompTIA Network+ (Cybrary) • Segurança de Redes (WR Educacional, 2019) • Redes de Computadores (Prime Cursos, 2019) • EIGRP Training e Cisco Labs/GNS3 (CIP Cyber, 2019) • Fundamentos de Computação em Nuvem (SOFTEX, 2019)
Dados, IA e programação	Redes Neurais e Deep Learning, 320h – TensorFlow/PyTorch • CS50 (Harvard / Fundação Estudar, 2023) • Introdução à Ciência de Dados (DSA, 2019) • Python (Udemy)
Cibersegurança geral	Maratona rumo a CYBER (CECyber, 2022) • Segurança e Privacidade do Computador – Microsoft (SOFTEX, 2019)