

OMAR PASSOS

Head de Segurança da Informação / CISO | Curitiba, PR

omar.ctba@gmail.com | (41) 99968-1251 | [LinkedIn](#) | [GitHub](#)

RESUMO PROFISSIONAL

Profissional com 15+ anos em Segurança da Informação e Proteção de Dados, combinando experiência estratégica e hands-on em SGSI (ISO/IEC 27001), LGPD (Atuação como Encarregado/DPO), SOC e resposta a incidentes. Atuação comprovada em desenho e operação de SOC, integração e tuning de SIEM/EDR/XDR, gestão de vulnerabilidades e investigações DFIR em ambientes híbridos e multi-cloud (AWS/Azure/GCP). Experiência com frameworks NIST, CIS e MITRE ATT&CK e habilidade em traduzir requisitos regulatórios em controles técnicos e programas de governança.

EXPERIÊNCIA PROFISSIONAL

Head of Cyber Security - CyberARMOR (julho de 2023 - Presente)

- Idealizei e liderei o desenvolvimento do cyberARMOR (ferramenta interna de análise de vulnerabilidades e pentest automatizado) reduzindo tempo médio de triagem em ~60% mediante automações em Python/Ruby/Go.
- Projetei e operacionalizei controles de proteção de dados (data discovery, classification, tokenização/mascaramento, DLP) integrados a SIEM (ELK) e pipelines de resposta, suportando processos de detecção de exfiltração em cloud.
- Defini roadmap de segurança corporativa e políticas alinhadas a ISO/IEC 27001 e LGPD; participei ativamente na preparação para auditorias internas e externas.

Especialista em Segurança da Informação - meutudo. (dezembro de 2022 - maio de 2024)

- Conduzi implantação e evolução de SGSI e programa de RBVM, integrando gestão de vulnerabilidades com processos de remediação e TI, reduzindo backlog crítico em 45%.
- Desenvolvi detecções, playbooks e dashboards SIEM (ELK) e executei operações Purple Team / Pentes para elevar maturidade de detecção; conduzi investigações DFIR focadas em exfiltração e contenção.
- Implementação de programas de Awareness com gamificação e integração com controles de terceiros para suporte à conformidade com LGPD.

CISO - Exago Innovation (janeiro de 2022 - novembro de 2022)

- Liderança na implementação do SGSI alinhado à ISO/IEC 27001: definição de políticas, matriz de controles, gestão de riscos e governança de terceiros.
- Traduzi requisitos legais e de privacidade (LGPD) em controles técnicos e processos (incluindo DPIA/RIPD), além de políticas DLP e validação de segurança de aplicações.
- Suporte executivo em auditorias regulatórias e interface com stakeholders externos.

Coordenador Cyber Defense Center - Task TI (dezembro de 2021 - julho de 2022)

- Defini estratégia e operação do SOC: seleção e integração de ferramentas (SIEM, IVM, IDR, ASM, DFIR, MDR) e centralização de alertas, aumentando correlação entre endpoints, perímetro e threat intel.
- Coordenei resposta a incidentes críticos, desenvolvimento de playbooks e redução do MTTR em incidentes de média/alta severidade.

Analista de Segurança da Informação / Pentester - Rentcars.com (dezembro de 2019 - agosto de 2020)

- Realizei testes de intrusão, gestão de vulnerabilidades e investigação de incidentes relacionados à integridade e exfiltração de dados; atuei em programas de bug bounty.
- Colaborei na implementação de requisitos de proteção de dados e iniciativas internas de conformidade com LGPD.

FORMAÇÃO ACADÊMICA

- Bacharelado - Administração de Empresas - PUC-PR (1998 - 2004)

- **Tecnologia da Informação** - CIP Cyber (2019)

HABILIDADES

ISO/IEC 27001, LGPD / Encarregado de Dados (DPO/CDPO), SGSI, SOC design & operation, SIEM (ELK, RSA), SOAR, EDR / XDR, DFIR, Incident Response, RBVM, Gestão de Vulnerabilidades, DLP, CASB, IAM, Firewall / WAF, Cloud Security (AWS, Azure, GCP), NIST, CIS, MITRE ATT&CK, DPIA / RYPD, Pentest / Red/Purple Team, Scripting & Automação (Python, Ruby, Go), Threat Intelligence, integração com SaaS (Google Workspace, O365, Slack).

CONQUISTAS

- Liderança e entrega do cyberARMOR: ferramenta interna de análise automatizada de vulnerabilidades e pentest que aumentou a capacidade de triagem e priorização de riscos em 60%.
- Implementação e evolução de SGSI/ISO27001 e programas de RBVM em múltiplas organizações, com redução significativa de backlog crítico e melhoria nos tempos de contenção.
- Certificações e formações relevantes: CISM (ISACA); EXIN PDPE Essentials (LGPD); cursos em Ethical Hacking e DFIR.