Juan Mathews Rebello Santos

Profissional de Cibersegurança | Operações de Segurança de Redes | Infraestrutura e Conformidade | Microsoft MVP

São Gonçalo – Rio de Janeiro, RJ · (21) 98727-2583 · contato@juanmathewsrebellosantos.com · www.linkedin.com/in/juanmathewsrebellosantos · juanmathewsre

RESUMO PROFISSIONAL

Profissional de Cibersegurança, Microsoft MVP e pesquisador de segurança da informação, com mais de 3 anos de experiência em operações de segurança de redes, infraestrutura de TI, defesa cibernética, gerenciamento de vulnerabilidades e conformidade. Graduado em Defesa Cibernética, especialista em Cyber Threat Intelligence e Segurança da Informação, com formação complementar em Perícia Forense Computacional, Crime Scene Investigation, Telecomunicações e Segurança Cibernética, além de mestrando em Ciência da Computação.

Possui mais de 50 certificações profissionais nacionais e internacionais, incluindo qualificações de instituições e organizações como Microsoft, Fortinet, Oxford Home Study Centre, Linux Foundation, Asian Development Bank Institute, Saviynt, The SecOps Group e University of Maryland. Certificado em ISO/IEC 27001:2022 Lead Auditor, ITIL 4, Fortinet NSE 3, Microsoft SC-900, Cyber Threat Intelligence, SOC Analysis, Ransomware Protection, Social Engineering Defense e Identity Security.

Experiência em ambientes corporativos e multinuvem, envolvendo Microsoft Azure, AWS e Google Cloud, administração de Windows Server, Linux e Active Directory, gerenciamento de identidades e acessos (IAM/RBAC), análise e aprovação de regras de firewall e proxy, hardening, proteção de endpoints, SIEM, IDS/IPS, WAF, monitoramento de eventos, resposta a incidentes e gerenciamento de vulnerabilidades. Participação em situações de crise cibernética, incluindo o incidente global envolvendo a CrowdStrike, contribuindo com suporte técnico e estratégias de mitigação.

Atua na identificação, análise e divulgação responsável de vulnerabilidades, com reconhecimento por contribuições à segurança de organizações e plataformas como Google, Microsoft, Nubank e Smiles. Primeiro profissional cego a publicar uma vulnerabilidade no National Vulnerability Database (NVD), mantido pelo governo dos Estados Unidos, com registro da CVE-2025-26326. Fundador do Banco Nacional de Vulnerabilidades (BNVD.org), iniciativa voltada à democratização do acesso a informações sobre vulnerabilidades e à disseminação de conhecimento em segurança cibernética.

Autor do livro Golpes Digitais: Como se Proteger na Era da Internet, publicado em português e inglês, e de artigos técnicos e pesquisas sobre segurança da informação, fraudes digitais, inteligência artificial, engenharia social e proteção de ambientes tecnológicos. Possui participações em entrevistas, reportagens e publicações de veículos e comunidades internacionais, incluindo HackerNoon, freeCodeCamp, e27, CSO Online, Help Net Security, TechRound e ProLion.

Pioneiro na integração entre cibersegurança e acessibilidade digital, reconhecido como o primeiro profissional cego do Brasil a se formar em Defesa Cibernética e Segurança da Informação e como primeiro profissional de segurança cibernética totalmente cego do país a receber o reconhecimento global Microsoft MVP. Desenvolve soluções tecnológicas acessíveis para pessoas com deficiência visual, contribui com ferramentas e projetos de código aberto e utiliza tecnologias assistivas, como NVDA e TalkBack, em atividades de desenvolvimento, pesquisa e operações de segurança.

EXPERIÊNCIA PROFISSIONAL

Metadados

Analista de Suporte de TI (IT Help Desk)

Abril de 2024 – Novembro de 2026

- Gerenciamento e resolução colaborativa de incidentes e solicitações de TI, com foco no cumprimento de metas e indicadores de SLA/SLO.
- Atendimento e suporte aos usuários na abertura e no acompanhamento de chamados, incluindo solicitações de liberação de acesso e configurações de rede por meio do Jira.
- Configuração, manutenção e atualização de ambientes e servidores, incluindo Active Directory, Windows Server e Linux, com atenção a práticas de hardening e conformidade.
- Implantação, administração e suporte de soluções de segurança e gerenciamento de endpoints, incluindo CrowdStrike e Automox.
- Administração de identidades e acessos (IAM/RBAC) em ambientes locais (Active Directory) e de computação em nuvem (Microsoft Azure e AWS).
- Elaboração e manutenção de documentações técnicas, processos e procedimentos de segurança e infraestrutura utilizando Jira e Confluence.
- Participação em cerimônias e atividades de metodologias ágeis (Scrum), contribuindo para a melhoria contínua dos processos.
- Atuação em situações de crise cibernética, oferecendo suporte técnico e contribuindo para estratégias de mitigação e melhoria da postura de segurança corporativa.

Newt Lab

Security Software Researcher (Freelance)

Outubro de 2026 – Atual

- Pesquisa e análise de segurança de software, com foco em identificação de vulnerabilidades, análise de ameaças e divulgação responsável.
- Atuação como pesquisador freelance em operações de security testing e avaliação de aplicações.

CegosBrasil

Atendimento ao Cliente

Junho de 2018 – Dezembro de 2018

- Atendimento e suporte aos clientes em tempo real, esclarecendo dúvidas e auxiliando na resolução de problemas.
- Foco na experiência do usuário e na satisfação dos clientes.
- Desenvolvimento de habilidades de comunicação, empatia, escuta ativa e resolução de problemas.

FORMAÇÃO ACADÊMICA

Koneru Lakshmaiah Education Foundation (KL University)

Mestrado em Ciência da Computação (Master of Computer Applications / Computer Science)

Novembro de 2026 – Novembro de 2029

EM ANDAMENTO

Instituto Daryus de Ensino Superior Paulista (IDESP)

Pós-graduação Lato Sensu em Cyber Threat Intelligence

Outubro de 2024 – Agosto de 2026

CONCLUÍDO

Faculdade Alcance (FAAL)

Pós-graduação em Cyber Crime e Cyber Security: Prevenção contra Crimes Digitais

Agosto de 2025 – Novembro de 2025

CONCLUÍDO

Faculdade IMES

Pós-graduação Lato Sensu em Segurança da Informação, Gestão de Redes e Segurança de Sistemas

Março de 2025 – Setembro de 2025

CONCLUÍDO

UniFavip Wyden

Graduação em Defesa Cibernética

Janeiro de 2023 – Março de 2025

CONCLUÍDO

Faculdade Prisma (FacPrisma)

Pós-graduações e cursos de especialização

- MBA em Telecomunicações com Ênfase em Redes, Sistemas de Informação e Internet das Coisas (IoT) — Abril de 2026 a Julho de 2026. Concluído.
- Pós-graduação em Perícia Forense Computacional — Abril de 2026 a Julho de 2026. Concluído.
- Pós-graduação em Crime Scene Investigation (CSI) — Abril de 2026 a Julho de 2026. Concluído.
- MBA Executivo em Segurança Cibernética — Abril de 2026 a Julho de 2026. Concluído.
- Curso de Extensão em Investigação Criminal e Neuropsicologia Forense — Abril de 2026 a Julho de 2026. Concluído.

Instituto Militar de Engenharia (IME)

Curso de Defesa de Redes – Cyber Security

Março de 2025

CONCLUÍDO

CERTIFICAÇÕES PROFISSIONAIS

2026

- **Cyber Security Certification™** — Asian Development Bank Institute (ADBI), setembro de 2026.
- **Saviynt Identity Security Certification for the AI Age (ISAA)** — Saviynt, novembro de 2026.
- **Certified Online Fraud Prevention Specialist (COFPS)** — Sumsub, maio de 2026.
- **Certified Social Engineering Defense Practitioner (CSEDP)** — The SecOps Group, junho de 2026.
- **Stellar Cyber SOC Analyst Associate Certification** — Stellar Cyber, julho de 2026.

2025 – 2026

- **Certified Ransomware Protection Officer (CRPO)** — ICTTF – United for Cyber Resilience, abril de 2026.
- **Certified Cybersecurity Educator Professional (CCEP)** — Red Team Leaders, abril de 2026.
- **Certified: AI and Career Enablement™** — University of Maryland, Robert H. Smith School of Business, março de 2026.
- **ISO/IEC 27001:2022 Lead Auditor** — Mastermind, outubro de 2025.
- **Supply Chain Detection and Response (SCDR) for Government Agencies** — SecurityScorecard, outubro de 2025.
- **Certificação Profissionalizante de Analista de Cibersegurança Júnior** — Fatec Zona Sul, outubro de 2025.
- **Governance Officer – Certificação em Assessoria de Governança Corporativa** — Instituto Empresa, novembro de 2025.
- **PeopleCert Ambassador** — PeopleCert, novembro de 2025.
- **Unified Endpoint Management (UEM)** — ManageEngine, novembro de 2025.
- **Certified Phishing Prevention Specialist (CPPS)** — Hack & Fix Academy, dezembro de 2025.
- **Gestão de Incidentes de Serviços de TI com ITIL 4** — Wellington Monaco, setembro de 2025.
- **Fortinet Network Security Expert (NSE 3)** — Fortinet, 2025.
- **Gerenciamento de Ameaças Cibernéticas** — ESCOM/CCOMGEX e Cisco Networking Academy, setembro de 2025.
- **CrowdSec Threat Intelligence Certification** — CrowdSec Academy, setembro de 2025.
- **Certified Developing Secure Software (CDSS)** — Linux Foundation, julho de 2025.

2024 – 2025

- **Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900)** — Microsoft, 2024.
- **Certified Cyber Security Analyst (CCSA)** — CyberWarFare Labs, 2025.
- **Certified Network Security Practitioner (CNSP)** — The SecOps Group, 2024.
- **ISO/IEC 27001 Information Security Foundation (ISFS)** — 2024.
- **Lei Geral de Proteção de Dados (LGPD) – Fundamentos** — 2024.
- **Especialização em Active Directory e Windows Server 2022** — 2024.
- **Diploma in Cyber Security** — Oxford Home Study Centre, 2024.
- **Cybersecurity Awareness Professional Certification (CAPC)** — CertiProf, 2024.

HABILIDADES TÉCNICAS

Segurança de Redes e Infraestrutura	Firewall, Proxy, Web Application Firewall (WAF), Intrusion Detection and Prevention Systems (IDS/IPS), Network Detection and Response (NDR), Network Access Control (NAC), IEEE 802.1X, Secure Access Service Edge (SASE), VPN, Hardening, análise de tráfego, Wireless Security, monitoramento de logs, SIEM, SOC, Blue Team, MITRE ATT&CK, gerenciamento de vulnerabilidades, VAPT, Pentest e Zero Trust.
Fundamentos de Redes	IPv4, IPv6, TCP/IP, DNS, VLAN, NAT e protocolos de comunicação.
Sistemas Operacionais e Servidores	Windows, Linux, Windows Server e Active Directory.
Computação em Nuvem	Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Entra ID e Cloud Security.
Governança, Risco e Conformidade (GRC)	ISO/IEC 27001, LGPD, modelagem de ameaças, gerenciamento de riscos, Business Continuity Management (BCM), ITSM, gerenciamento de incidentes, mudanças e problemas.
Gerenciamento de Identidades e Acessos	Identity and Access Management (IAM), Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA) e Single Sign-On (SSO).
Análise de Ameaças e Segurança Ofensiva	Cyber Threat Intelligence (CTI), análise de malware, engenharia reversa, Security Orchestration, Automation and Response (SOAR – conceitos) e análise de ameaças cibernéticas.
Ferramentas e Plataformas	Jira, Confluence, Monday.com, TeamViewer, Zabbix, Microsoft 365, CrowdStrike e Automox.
Desenvolvimento e Infraestrutura	HTML5, JavaScript, CI/CD, Backup & Recovery e Storage Corporativo.

COMPETÊNCIAS COMPORTAMENTAIS

Comunicação eficaz | Trabalho em equipe e colaboração | Resolução de problemas | Aprendizado contínuo e adaptabilidade | Gestão do tempo e organização | Inteligência emocional | Empatia e escuta ativa | Pensamento crítico e analítico | Resiliência e proatividade

IDIOMAS

Português: Nativo **Inglês:** Básico (A2) **Espanhol:** Iniciante (A1)