

# TULIO CRUVINEL GOMES

Piracicaba, SP • (19) 995-777-123 • [tulio.c.gomes@gmail.com](mailto:tulio.c.gomes@gmail.com)  
[Linkedin](#) – [Github](#) – [Blog](#)

## OBJETIVO

Trabalhar na área de cybersecurity, com interesses em ethical hacking, penetration testing, análise de vulnerabilidades e Appsec em ambiente DevSecOps. Metódico, dedicado, ético, resiliente e sempre exercitando o aprendizado contínuo. Possui uma excelente comunicação, com foco em relatórios técnicos e desenvolvimento de políticas e normas. Atualmente trabalho em uma posição técnica realizando também tarefas de governança em TI. Hoje busco me desenvolver profissionalmente na área de segurança da informação. Eu também possuo:

- Experiência em traduzir informações de cunho técnico para a terminologia de gerência/usuários.
- Experiência em programação de scripts utilizando Python e Bash.
- Experiência em administração de serviços em ambiente Linux/Windows.
- Experiência em infraestrutura de redes.
- Inglês Intermediário, com grande ênfase em leitura técnica e acadêmica.
- Estudo de machine learning aplicados a problemas na área de segurança.
- Estudo de conjuntos de ferramentas de segurança como Kali Linux, Metasploit e Burp Suite para aplicar em CTF, HTB, THM e VulnHub.
- Iniciando o estudo das linguagens Go e Java.

## EDUCAÇÃO

### FATEC Americana – Tecnólogo em Segurança da Informação (2017-2020)

- Iniciação Científica: [Machine Learning aplicado a Esteganálise](#).
- Monografia: [Aprendizado de Máquina na detecção de Tráfego de Botnet](#)

## CERTIFICAÇÕES

- Fortinet – Network Security Associate (NSE1)
- ICSI – Certified Network Security Specialist (CNSS)
- Linuxtips – Uncomplicating Docker
- Dsec Security – DCPT (Em progresso)

## EXPERIÊNCIA

### Securityfirst, Piracicaba - SP Cyber Security Analyst

Mai de 2017 até o presente

- Operação do SIEM Wazuh Stack.
- Monitoração de logs e eventos de segurança, análise e triagem de incidentes.
- Analisar, criar e sintonizar alertas gerados pelo SIEM Wazuh, IPS ou Firewall.
- Criação de regras e correlação de logs no SIEM.
- Gerenciamento de Vulnerabilidades.
- Contato com clientes no processo de investigação e resposta a incidentes.
- Auxílio na melhoria contínua dos procedimentos operacionais do SOC.

### FATEC Piracicaba, Piracicaba - SP Auxiliar de Docente de TI

Fev de 2017 até Mai de 2021

- Responsável pela manutenção e gestão dos computadores da instituição.
- Criação de Políticas e normas para o departamento de TI utilizando COBIT/NIST/ISO.
- Gerenciamento dos serviços de rede, como: AD, CUPS, Squid, OpenBiblio e Firewall (PfSense).
- Manutenção dos servidores e gerenciamento de scripts ativos.
- Suporte Técnico aos discentes, docentes e funcionários.
- Treinamento e supervisão de estagiários, incentivando projetos para implementação na instituição.

**Biocapital Participações S.A**, Charqueada - SP

Jan de 2013 até Dez de 2016

**PJ - Assistente de TI**

- Administração de usuários/grupos no AD.
- Administração de contas de e-mail Exchange 2010.
- Gerenciamento de servidor proxy (Linux-BRMA/OMNE).
- Configuração de servidor Windows Server 2012 (AD/FileServer).
- Implementação do ERP Ti9.
- Suporte aos usuários/equipamentos e consultoria para adesão de novas tecnologias.

**FUMEP**, Piracicaba - SP

Jan de 2010 até Out de 2011

**Estagiário de TI**

- Gestão nos laboratórios de informática e manutenção de computadores.
- Atendimento a alunos e professores da instituição.
- Treinamento de novos estagiários de acordo com as políticas de TI.

**CURSOS E  
EVENTOS**

- Cisco – Cybersecurity Essentials
- Cisco – Introduction to Networks (CCNA R&S)
- FATEC Americana - Iniciação Científica 2019/2020 - "Machine Learning aplicado a Esteganálise"
- Beco do Exploit – Desafio 2 "Hackear 30 máquinas em 30 dias"
- Uniciv – 1º Bootcamp de Ethical Hacking
- FIAP Nano Courses – DevOps & Agile Culture

**CTFs**

Esses são os que tenho jogado ultimamente, mais detalhes sobre os desafios estão no meu blog <https://0xNymerio.github.io> .

- [HacktheBox](#)
- [TryHackMe](#)
- [Root-me.org](#)
- [OverTheWire](#)
- [CryptoHack](#)

**INFORMAÇÕES  
ADICIONAIS**

- CNH A/B.
- Horários flexíveis.
- Disponibilidade para mudança de cidade/estado.
- Disponibilidade para trabalho remoto ou trabalho híbrido.