

# Caio B. Franca

Network & Security Engineer | Infrastructure Operations | Cloud & Automation

[braga.caio@outlook.com](mailto:braga.caio@outlook.com) | [LinkedIn](#) | [GitHub](#)

## Professional Summary

IT professional with 10+ years of experience supporting large-scale, highly available network environments across enterprise and data center operations. Currently supporting Meta network operations, working with engineering, operations, and vendor teams to ensure reliable L1–L3 services in complex, multi-vendor environments.

Strong background in enterprise routing and switching across Cisco, Juniper, Arista, and Nexus platforms, with experience in change execution, lifecycle management, and SLA-driven operations. Exposure to network modernization initiatives including cloud-adjacent networking (AWS, Azure), SD-WAN (VMware VeloCloud), firewall policy management (Palo Alto, Fortinet), and traffic management with F5, with a focus on operational rigor, automation, and process improvement.

## Core Competencies

- **Network Infrastructure & Architecture:** Enterprise and data center networking fundamentals including BGP, OSPF, MPLS, VLANs, STP, EtherChannel, VRRP, and HSRP, supporting large-scale, highly available environments.
- **Multi-Vendor Network Platforms:** Experience operating and coordinating across heterogeneous network environments including Cisco IOS/NX-OS, Juniper, Arista, and Nexus, with a focus on interoperability, standardization, and lifecycle consistency.
- **Network Operations & Program Delivery:** End-to-end support of network operations and delivery activities, including L1–L3 incident coordination, root cause analysis, SOP/MOP development, NOC workflows, and major incident management in SLA-driven environments.
- **Automation & Tooling (Foundational):** Exposure to automation and operational tooling using Python, Ansible, Terraform (foundational), REST APIs, and Git to improve efficiency, repeatability, and deployment hygiene.
- **Monitoring, Observability & Diagnostics:** Use of platforms such as SolarWinds, Wireshark, tcpdump, SNMP, NetFlow, Zabbix, and Splunk to support proactive operations, troubleshooting, and data-driven decision-making.
- **Cloud & Hybrid Networking:** Familiarity with cloud-adjacent and hybrid networking concepts across AWS and Azure, including VPC/VNet design, subnetting, VPN connectivity, peering, and enterprise hybrid integration models.

- **Network Security & Access Controls:** Experience working with firewall and security platforms including Palo Alto and Fortinet (Check Point familiarity), supporting ACLs, VPNs, IDS/IPS, and Zero Trust-aligned access models.
- **Governance, Risk & Change Management:** Experience operating within regulated environments, supporting ISO 27001, GDPR, structured change management, audit documentation, and risk-aware network operations.



## Portfolio & Projects

Hands-on projects and learning in networking, cybersecurity, cloud, and automation.

<https://caiofrnca.github.io>

## Certifications & Education

- Postgraduate Certificate in Cybersecurity Management – MTU Ireland (in progress)
- Higher Diploma in Science in Computing – CCT College, Dublin (2021)
- Amazon Cloud Architect Solution - SAA-C03 (in progress)
- CompTIA Security+ (Valid until Aug 2026)
- Google Professional Certificate (2024)
- BSc (Hons) in Computing Science, Estácio de Sá University (2018)
- Cisco CCNA R&S Coursework (2018)

## Work Experience

### Network Operations Engineer – Meta (via Astreya), Dublin, Ireland

May 2025 – Present

- Support Meta's global enterprise and data-center network infrastructure across a multi-vendor environment (Cisco, Juniper, Arista, Nexus), operating within large-scale, high-availability production networks.
- Handle L1–L3 incident coordination and major incident response, managing escalations, impact assessments, and root cause analysis to maintain service continuity and meet SLA objectives.
- Partner with global network engineering, operations, and deployment teams across regions to support backbone and fabric reliability within hyperscale environments.
- Drive incident response by performing RCA, impact assessments, and follow-ups, with clear stakeholder communication through internal monitoring and ticketing systems.
- Support network observability through dashboard enhancements, metric refinement, and alert tuning.
- Manage VLAN changes, DNS updates, subnet assignments, and vendor RMA coordination.
- Drive operational improvements through SOP/MOP refinement, escalation path standardization, and MTTR reduction initiatives.

### **IT Deployment Operations & Asset Management Associate – PwC Ireland, Dublin, Ireland**

June 2022 – May 2025

- Support enterprise-wide deployment and secure configuration of IT assets (laptops, mobile devices, networking hardware) across PwC offices, operating within strict security, encryption, and compliance standards.
- Contribute to IT asset lifecycle management activities including provisioning, refresh, recovery, and inventory accuracy, aligning operational execution with audit and governance requirements.
- Support global hybrid environments through patching, system updates, and remote issue resolution, contributing to platform stability and consistency at scale.
- Act as an escalation point for access, VPN, and endpoint security issues, working with infrastructure and network teams to resolve provisioning and identity-related dependencies.
- Participate in process and documentation improvements to standardize deployment workflows, reduce rework, and improve operational efficiency.

### **IT Support Engineer – PFH Technology Group (Clients: PwC, Irish Rail, Dublin Bus), Ireland**

Nov 2021 – June 2022

- Provided on-site and remote support for enterprise clients in the public and private sector, focusing on network access, VPN tunnel troubleshooting, and endpoint connectivity.
- Diagnosed hardware, software, and basic network issues, escalating complex cases appropriately.
- Delivered device provisioning and supported secure onboarding processes for users.
- Coordinated with client-side IT departments and vendors for escalations and incident recovery.

### **Network Operations Centre (NOC) Engineer – RTM – Rede de Telecomunicações para o Mercado, Brazil - April 2012 – April 2019**

- Supported a nationwide MPLS backbone serving Brazil's financial sector, operating and monitoring over 1,800 network devices across Cisco, Juniper, and Huawei platforms in high-availability environments.
- Performed L1–L3 incident response for service degradation and outages impacting BGP, OSPF, VLANs, STP, and EtherChannel, meeting strict SLA and uptime requirements.
- Worked alongside senior network engineers on network expansion and resilience initiatives, including new POP integrations, redundancy enhancements, and customer onboarding.
- Contributed to execution of network rollout activities from planning through deployment, supporting site readiness, device provisioning, and operational documentation.
- Utilized network monitoring and telemetry platforms (SolarWinds, SNMP, NetFlow) to proactively identify performance issues and validate remediation.
- Operated within strict change management, documentation, and compliance frameworks aligned with Central Bank of Brazil regulatory standards.

## **References**

Available upon request.