

## **Relatório de Viagem – IETF 123 (Madrid, 19 a 25 de julho de 2025)**

Participante: Percival Henriques de Souza - Conselheiro do CGI.br

### **1. Sumário Executivo**

- Participação presencial no IETF 123, em Madrid.
- Foco em criptografia pós-quântica (PQC) e tecnologias quânticas emergentes.
- Reunião estratégica com Telefónica de España sobre redes híbridas quânticas e comunicação quântica via satélite.
- Implicações diretas para a estratégia brasileira de segurança e soberania digital.

### **2. Objetivos da Participação**

- Acompanhar debates do PQUIP WG sobre PQC.
- Observar estado da arte em implementações de QKD na Europa.
- Levantar possibilidade de estabelecer cooperações técnicas com empresas e centros de pesquisa.
- Posicionar o Brasil em debates sobre padronização de protocolos quânticos.
- Identificar oportunidades de formação e capacitação em tecnologias emergentes.

### **3. Informações Gerais do Evento**

- Local e Data: IETF 123, realizado no Hotel Meliá Castilla, Madrid, Espanha, de 19 a 25 de julho de 2025.
- Participantes: Aproximadamente 1.089 presencialmente e 543 online, totalizando mais de 1.600 participantes globais.
- Formato: Hackathon (19–20 jul), Grupos de Trabalho (21–25 jul), Plenária (23 jul) e sessões como IRTF Open (24 jul), com transmissão ao vivo e gravações no portal IETF Live.
- Programas de apoio: “New Participant Program” com tutoriais, mentoria e integração para recém-chegados.
- Infraestrutura técnica: Rede de 10 Gb/s, Wi-Fi WPA3/WPA2 com IPv6 preferencial, área de trabalho compartilhada equipada e suporte técnico via Help Desk.

### **4. Principais Atividades e Resultados**

#### **4.1 Criptografia Pós-Quântica (PQUIP WG)**

- Discussões sobre algoritmos híbridos (clássico + resistente a quantum).
- Impactos de novos padrões NIST (ML-DSA, ML-KEM, SLH-DSA).

#### **4.2 Cooperação com Telefónica de España**

- Modelo de rede híbrida em Madrid (fibra clássica + QKD).
- Potencial adaptação ao Brasil (uso incremental da infraestrutura de fibra existente).
- Oportunidades em comunicação quântica por satélite (essencial para países continentais).

#### 4.3 Apresentação de John Preuß Mattsson (Ericsson Research)

- Desafios da PQC em redes móveis 5G/6G.
- Viabilidade em países com infraestrutura heterogênea.

#### 4.4 Hackathon

- Implementações PQC em software livre: Wireshark, GnuTLS, nmap/zmap.

#### 4.5 Sustentabilidade e Direitos Humanos

- Criação do GREEN WG (eficiência energética em redes).
- Debate “Let’s Rewild the Internet” (diversidade tecnológica e riscos da centralização).

### 5. Implicações para o Brasil

- Oportunidades: liderança regional, rede nacional híbrida, parcerias com Europa.
- Desafios técnicos: custos elevados, latência, integração com legado.
- Desafios regulatórios: espectro, certificação, soberania sobre satélites.

### 6. Recomendações

- Formalizar parceria CGI.br Nic.br – Telefónica.
- Criar força-tarefa nacional sobre tecnologias quânticas.
- Implementar programa de capacitação em PQC/QKD.
- Estruturar Quantum Lab no NIC.br e pilotos via RNP.
- Monitorar sistematicamente drafts e decisões do PQUIP WG.

### 7. Conclusão

A participação no IETF 123 mostrou que a transição para a era quântica já está em curso, com implementação real na Europa e Ásia. O Brasil deve agir rapidamente para não depender de arquiteturas definidas por terceiros. O CGI.br tem papel estratégico como articulador nacional e regional para garantir soberania digital e alinhamento internacional.