

COMITÊ GESTOR DA INTERNET NO BRASIL
CGI.br

RELATÓRIO DE PARTICIPAÇÃO

IETF 124 – 124th Meeting of the Internet Engineering Task Force

Montreal, Canadá – 01 a 07 de novembro de 2025

Fairmont The Queen Elizabeth

Percival Henriques de Souza Neto

Conselheiro do CGI.br

Coordenador da Câmara de Segurança e Direitos

João Pessoa, novembro de 2025

1. Sumário Executivo

A 124ª reunião da Internet Engineering Task Force (IETF 124), realizada no Fairmont The Queen Elizabeth em Montreal, Canadá, de 01 a 07 de novembro de 2025, reuniu mais de 1.000 engenheiros, arquitetos de rede, pesquisadores e desenvolvedores de todo o mundo para avançar o trabalho de padronização dos protocolos que sustentam a Internet.

Patrocinada pela Comcast e NBCUniversal, esta edição consolidou três eixos técnicos de importância estratégica para o Brasil: a transição para criptografia pós-quântica, com avanços significativos nos grupos de trabalho PQUIP e TLS, incluindo a criação do novo grupo PLANTS (PKI, Logs, and Tree Signatures); a quinta reunião do grupo GREEN (Getting Ready for Energy-Efficient Networking), consolidando métricas de eficiência energética para infraestrutura de rede; e discussões emergentes sobre padronização de IA agêntica, sinalizando novo campo de atuação para a comunidade técnica.

A participação no IETF 124 deu continuidade ao trabalho iniciado nas reuniões anteriores (IETF 122 em Bangkok e IETF 123 em Madrid), consolidando o acompanhamento estratégico do CGI.br nos processos de padronização da Internet e fortalecendo o Programa de Fomento CGI.br/NIC.br para participação de pesquisadores brasileiros.

2. Contexto e Relevância Estratégica

As reuniões do IETF constituem o principal fórum técnico global para desenvolvimento de protocolos e padrões da Internet. Diferentemente de conferências comerciais, são espaços exclusivamente dedicados ao trabalho colaborativo de engenharia, onde as decisões técnicas tomadas afetam diretamente a infraestrutura sobre a qual toda a economia digital opera.

O IETF 124 em Montreal ocorreu numa sequência de eventos estratégicos para a governança da Internet. Realizou-se imediatamente após a ICANN84 em Dublin e poucas semanas antes da revisão WSIS+20. Esta convergência temporal conferiu particular urgência às discussões sobre criptografia pós-quântica e sustentabilidade energética, temas que transversalizam as agendas política e técnica da Internet global.

Para o Brasil, a presença contínua no IETF é condição para o exercício efetivo da soberania digital. Os protocolos definidos neste fórum determinam como os dados trafegam, como a segurança é implementada e como a Internet evolui tecnicamente. Sem participação qualificada, o país se torna mero consumidor de padrões definidos por outros.

3. Temas Centrais e Grupos de Trabalho

3.1 Criptografia Pós-Quântica: PQUIP, TLS e PLANTS

O IETF 124 registrou avanços substanciais na transição para criptografia pós-quântica (PQC). O grupo PQUIP (Post-Quantum Use In Protocols) continuou seu

trabalho de coordenação transversal, orientando a implementação de algoritmos resistentes a computadores quânticos nos protocolos IETF. O draft "Post-Quantum Cryptography for Engineers" avançou para sua 14ª versão, consolidando-se como documento de referência para implementadores.

Na sessão de secdispatch, foi apresentada orientação prática para implantações atuais, recomendando fortemente a adoção de KEMs híbridos (como X25519MLKEM768 para TLS) em detrimento de abordagens puramente clássicas ou puramente pós-quânticas. Esta recomendação busca mitigar o risco de ataques do tipo "harvest now, decrypt later", em que dados cifrados hoje possam ser decifrados quando computadores quânticos criptograficamente relevantes estiverem disponíveis.

Destaque especial para a criação do grupo PLANTS (PKI, Logs, and Tree Signatures), resultante de uma sessão BoF (Birds of a Feather) bem-sucedida. O PLANTS abordará o impacto de assinaturas pós-quânticas, significativamente maiores que as atuais, sobre infraestruturas de chave pública (PKI) com Certificate Transparency, especialmente quando utilizadas em protocolos interativos como TLS. Este é um ponto crítico para a transição pós-quântica, pois as assinaturas ML-DSA e SLH-DSA apresentam tamanhos substancialmente superiores aos algoritmos RSA e ECDSA atuais.

Para o Brasil, que coordena iniciativas de computação quântica e prepara a instalação de computadores quânticos na Paraíba em 2026, o acompanhamento desses desenvolvimentos é estratégico. A capacidade nacional de implementar protocolos pós-quânticos de forma autônoma depende do domínio técnico desses padrões em fase de definição.

3.2 GREEN – Eficiência Energética da Internet

O grupo GREEN (Getting Ready for Energy-Efficient Networking) realizou sua quinta reunião no IETF 124, avançando na exploração de casos de uso, definição de requisitos e desenvolvimento de soluções para identificação e caracterização de métricas de eficiência energética, métodos de monitoramento e controle de consumo energético de dispositivos de rede, e otimização da eficiência energética em toda a Internet.

A consolidação progressiva do GREEN reflete a importância crescente da sustentabilidade na infraestrutura digital. Para o Brasil, com seu parque de data centers em expansão e o projeto de R\$ 265 milhões em Campina Grande, a adoção precoce de padrões de eficiência energética pode representar vantagem competitiva significativa e alinhamento com compromissos climáticos nacionais.

3.3 QIRG – Quantum Internet Research Group

O Quantum Internet Research Group (QIRG) continuou o desenvolvimento de seu framework arquitetural para redes quânticas, delineando funções e definições de nós de rede para construir um vocabulário comum e servir como primeiro passo para uma arquitetura de rede quântica. O objetivo do QIRG é abordar a questão fundamental de como projetar e construir redes quânticas.

Este grupo de pesquisa é de particular relevância para o Brasil, considerando os investimentos nacionais em computação quântica e a necessidade de preparar a infraestrutura de telecomunicações para a futura Internet quântica. A participação brasileira no QIRG pode posicionar o país como contribuidor ativo na definição da arquitetura da próxima geração de redes.

3.4 IA Agêntica e Padronização

As discussões no IETF 124 sinalizaram o início de um novo campo de trabalho em padronização de IA agêntica. Com a proliferação de ferramentas de IA capazes de ações autônomas na rede, emergem questões sobre quais aspectos necessitam padronização técnica. Os desafios vão dos protocolos de comunicação entre agentes aos mecanismos de autenticação e autorização. Este tema conecta-se diretamente ao trabalho sobre governança algorítmica e ao conceito de "sujeito da predição" em desenvolvimento no âmbito acadêmico brasileiro.

3.5 SRv6 e Evolução de Redes

O grupo SRv6ops discutiu a evolução das arquiteturas de rede baseadas em Segment Routing sobre IPv6, com apresentações da Verizon sobre migração de pontos de encapsulação para hosts e da Bell Canada sobre SRv6 como catalisador de transformação de redes. Estas discussões são relevantes para operadoras brasileiras que planejam modernização de infraestrutura e para o projeto de conectividade associado ao data center de Campina Grande.

3.6 SCONE – Comunicação com Elementos de Rede

O grupo SCONE (Standard Communication with Network Elements) trabalhou no desenvolvimento de mecanismos para que aplicações recebam notificações contendo orientações de throughput para tráfego upstream e downstream. Este trabalho tem implicações diretas para a qualidade de serviço na Internet brasileira e para a implementação de políticas de neutralidade de rede.

4. Hackathon e Atividades Complementares

O Hackathon do IETF 124, realizado nos dias 1º e 2 de novembro, precedeu a semana de reuniões formais. Desenvolvedores e especialistas colaboraram na implementação prática de padrões IETF, com destaque para projetos relacionados a criptografia pós-quântica e eficiência energética. O Code Sprint, também no dia 1º de novembro, reuniu voluntários para trabalhar no código do IETF Datatracker e outras ferramentas da comunidade.

O New Participant Program, no domingo 2 de novembro, ofereceu programa de dia inteiro para novos participantes, facilitando a compreensão dos processos do IETF. Esta é uma oportunidade relevante para os pesquisadores brasileiros apoiados pelo Programa de Fomento CGI.br/NIC.br.

5. Programa de Fomento CGI.br/NIC.br

O IETF 124 representou oportunidade fundamental para acompanhar e apoiar os pesquisadores brasileiros selecionados pelo Programa de Fomento CGI.br/NIC.br para participação no IETF/IRTF. A presença institucional do CGI.br permitiu orientar os participantes, maximizar o aproveitamento das sessões técnicas e avaliar in loco a efetividade do programa.

A continuidade desta presença é essencial para garantir retorno adequado do investimento público e para estabelecer bases sólidas de participação brasileira sustentável nos processos de padronização da Internet. As lições aprendidas no IETF 123 em Madrid foram aplicadas no acompanhamento dos bolsistas em Montreal, com resultados positivos em termos de engajamento nos grupos de trabalho.

6. Análise e Implicações para o Brasil

6.1 Transição Pós-Quântica e Soberania Tecnológica

A criação do grupo PLANTS e os avanços nos grupos PQUIP e TLS sinalizam que a transição pós-quântica está passando da fase teórica para a implementação prática. O Brasil, que se prepara para instalar computadores quânticos na Paraíba em 2026 e coordena o projeto de data center de R\$ 265 milhões em Campina Grande, possui interesse direto em participar da definição desses padrões. A capacidade de implementar criptografia pós-quântica de forma autônoma é componente essencial da soberania tecnológica nacional.

6.2 Sustentabilidade e Infraestrutura Digital

A consolidação do grupo GREEN oferece ao Brasil a oportunidade de incorporar, desde o início, padrões internacionais de eficiência energética em seus novos projetos de infraestrutura digital. O crescimento acelerado da demanda por processamento de dados, impulsionado por IA e computação em nuvem, torna a eficiência energética dos data centers questão não apenas ambiental, mas econômica e competitiva.

6.3 Formação de Capacidade Técnica

A participação continuada no IETF, articulada com o Programa de Fomento, constitui o caminho mais eficaz para aumentar a presença técnica brasileira nos processos de padronização. Montreal demonstrou que a combinação de acompanhamento institucional com apoio a pesquisadores individuais produz resultados concretos, com brasileiros contribuindo ativamente em grupos de trabalho estratégicos.

7. Recomendações

7.1 Ações Imediatas

- Produzir material de orientação sobre a transição pós-quântica para operadores de infraestrutura crítica brasileira, com base nas recomendações emanadas do IETF 124;
- Avaliar os resultados do Programa de Fomento CGI.br/NIC.br com base na experiência de Montreal e propor ajustes para a próxima chamada;

- Organizar workshop com operadoras brasileiras sobre as implicações dos novos padrões de eficiência energética (GREEN) para a infraestrutura nacional.

7.2 Ações de Médio Prazo

- Garantir participação brasileira contínua nos grupos PQUIP, PLANTS, TLS, GREEN e QIRG, preferencialmente com pesquisadores nacionais como coautores de drafts;
- Integrar o acompanhamento dos padrões IETF à Estratégia Nacional de Cibersegurança (E-Ciber 2025), particularmente no eixo de criptografia pós-quântica;
- Articular com universidades e centros de pesquisa brasileiros a formação de grupos específicos de acompanhamento dos grupos de trabalho do IETF.

7.3 Ações Estratégicas

- Propor ao CGI.br a criação de grupo técnico dedicado ao acompanhamento da transição pós-quântica, conectando o trabalho do IETF às iniciativas nacionais de computação quântica;
- Ampliar o Programa de Fomento para incluir estágios de pesquisa em laboratórios internacionais que contribuem ativamente para drafts do IETF;
- Manter e fortalecer a presença brasileira no IETF 125, previsto para março de 2026.

8. Conclusão

O IETF 124 em Montreal confirmou a centralidade da padronização técnica para o futuro da Internet segura e sustentável. A criação do grupo PLANTS, os avanços concretos na transição pós-quântica e a consolidação do trabalho sobre eficiência energética demonstram que os padrões definidos hoje determinarão a arquitetura da Internet nas próximas décadas.

Para o Brasil, que se encontra num momento de investimento significativo em infraestrutura digital e computação quântica, a participação qualificada no IETF não é opção. É imperativo estratégico. Os protocolos e padrões em fase de definição impactarão diretamente a segurança, a eficiência e a autonomia da infraestrutura digital nacional.

O Programa de Fomento CGI.br/NIC.br, aliado à presença institucional contínua, constitui o instrumento adequado para assegurar que o Brasil seja participante ativo, e não mero destinatário, dos padrões que regem a Internet global.

Percival Henriques de Souza Neto

Conselheiro do CGI.br

Coordenador da Câmara de Segurança e Direitos