Transição Criptográfica Pós-Quântica: Estratégias Híbridas e Impactos Práticos no TLS, PKI e Governança

Jaqueline Silva, MSc

UFRPE

Dez. 15, 2025

AGENDA

GTER 54 GTS 40

1. Introdução
2. Estratégias Híbridas
3. Impactos no TLS
4. PKI e Certificados Híbridos
5. Governança
6. Encerramento

INTRODUÇÃO: A Era da Computação Quântica

A infraestrutura PKI atual depende de algoritmos como **RSA, DH e ECC** para certificados digitais, transações financeiras e comunicações seguras. Computadores quânticos com o **algoritmo de Shor** podem quebrar esses sistemas em tempo polinomial.

Criptografia Assimétrica

✓ **RSA, ECDH, ECDSA, X25519, ED25519**

ATAQUE QUÂNTICO (SHOR) - ≈ 1.330 qubits lógicos – ≈1 dia (Quebra)

Criptografia Simétrica

✓ **AES, ChaCha20, sha-256/384**

Grover: Reduz segurança pela metade

Harvest Now, Decrypt Later: Adversários já coletam dados criptografados hoje para descriptografar quando computadores quânticos estiverem disponíveis

Protocolos afetados: TLS, SSH, IPsec/IKEv2, S/MIME, OpenPGP, MQTT — toda comunicação segura da Internet

INTRODUÇÃO: Infraestrutura Crítica no Brasil

GTER 54 GTS 40

12M+
Certificados ICP-Brasil

20+
ACs Credenciadas

5.000+
ARs em Operação

35+
PTTs NIC.br

Sistemas Financeiros

- PIX (BCB)
- Open Banking/Finance
- SPB e SITRAF
- Gateways de pagamento

Governo Digital

- Gov.br (autenticação)
- e-CAC Receita Federal
- SERPRO/DATAPREV
- Sistemas judiciais

Infraestrutura Rede

- Backbone RNP
- PTTs IX.br
- Roteadores e firewalls
- VPNs corporativas

IoT e Indústria

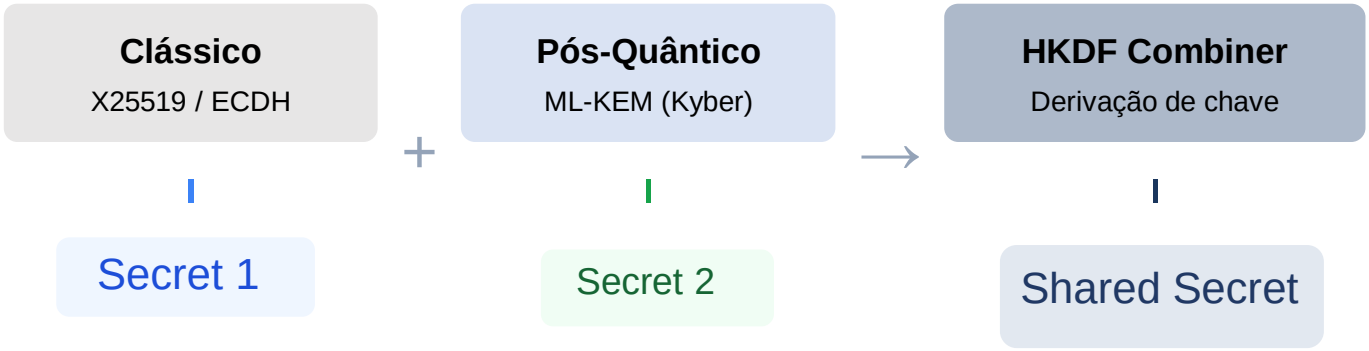
- Smart grids
- Automação industrial
- Dispositivos embarcados
- Sensores e gateways

Todos esses sistemas dependem de RSA/ECC — vulneráveis a ataques quânticos via algoritmo de Shor

Estratégias Híbridas na Prática

Abordagem Híbrida: Combina algoritmos clássicos (testados por décadas) com pós-quânticos (novos) garantindo segurança mesmo que um seja comprometido.

Modelo de Combinação de Chaves



Compatibilidade

Sistemas legados usam chave clássica, novos verificam ambas

Segurança Dupla

Seguro mesmo se um algoritmo for quebrado no futuro

Transição Gradual

Migração sem ruptura de serviços em produção

Google, Cloudflare e Apple já implementam TLS híbrido (X25519 + ML-KEM) em produção desde 2024

Algoritmos de Criptografia Pós-Quântica

GTER 54 GTS 40

🔐 ML-KEM (Kyber)

Key Encapsulation Mechanism

Uso: Troca de chaves no TLS handshake

Níveis: ML-KEM-512/768/1024

Recomendação: ML-KEM-768 para TLS (Level 3)

🛡️ SLH-DSA (SPHINCS+)

Stateless Hash-Based Signatures

Uso: Root CAs (máxima segurança)

Trade-off: Assinaturas ~17KB, zero risco lattice

Recomendação: SLH-DSA-128f para CAs raiz

✍️ ML-DSA (Dilithium)

Digital Signature Algorithm

Uso: Assinaturas em certificados X.509

Níveis: ML-DSA-44/65/87

Recomendação: ML-DSA-65 para-PKI (Level 3)

⚡ Estratégia Híbrida

Best of Both Worlds

TLS: X25519 + ML-KEM-768 (já em produção)

Certificados: ECDSA P-256 + ML-DSA-44

Vantagem: Seguro mesmo se PQC tiver falhas

📦 **Bibliotecas com Suporte PQC:** OpenSSL 3.2+ | BoringSSL (ML-KEM nativo) | liboqs 0.10+ | wolfSSL 5.6+

💡 **Foco: Testar híbrido HOJE, não esperar algoritmo "perfeito"**

Desafios de Implementação no TLS

MTU e Fragmentação

Mensagens excedem MTU de 1500 bytes, causando fragmentação TCP

Aumento de Latência

Operações PQ mais custosas. Impacto em redes de borda e IoT

Compatibilidade Retroativa

Sistemas legados não suportam novos algoritmos

Aceleração de Hardware

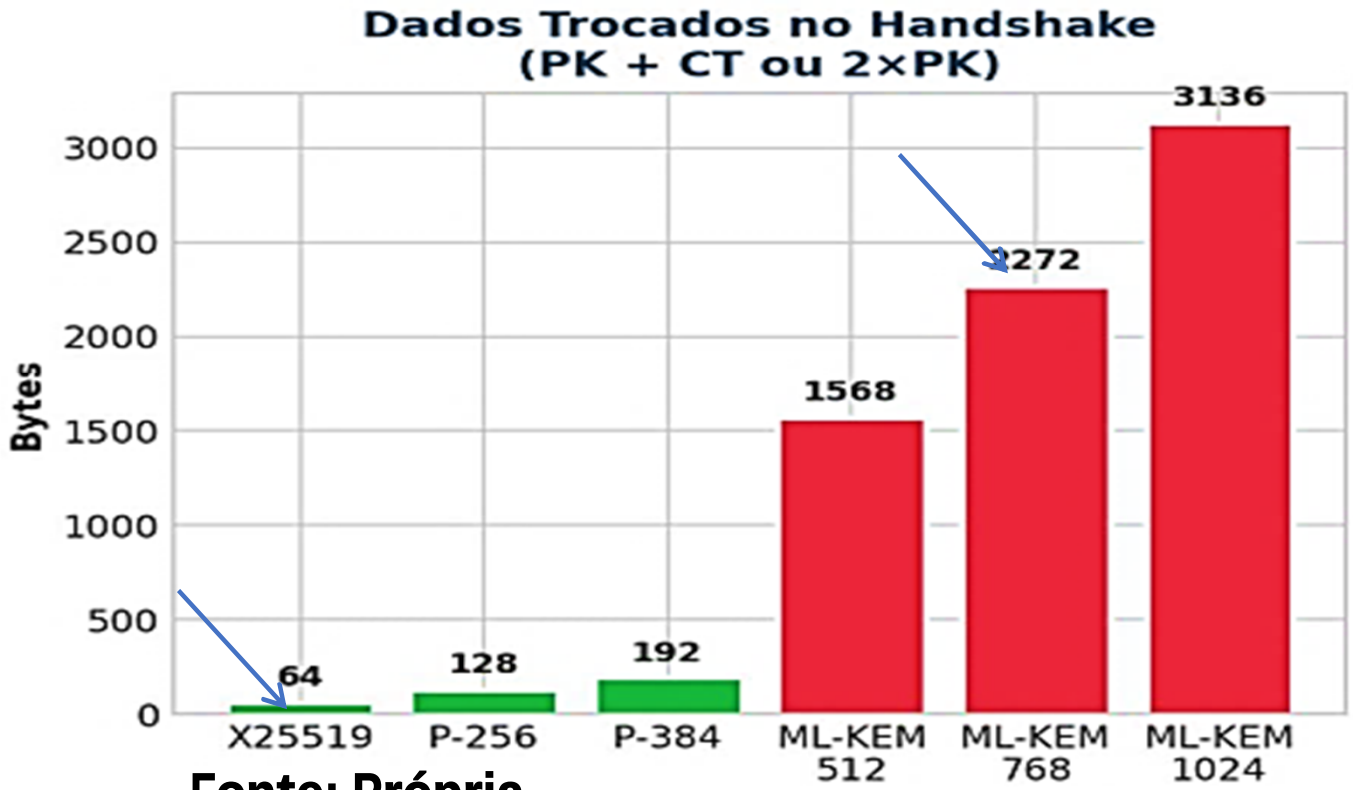
HSMs ainda sem suporte nativo para algoritmos PQ

IMPACTOS NO TLS - Impactos no Handshake

Aumento massivo no tamanho das mensagens

- O KEM **64 bytes** (X25519) - **Clássico**
- O KEM **2.272 bytes** (ML-KEM-768) – **PQC**

35,5 vezes maior!!



Fonte: Própria

KEMTLS: Variante que usa KEMs para autenticação, eliminando assinaturas PQ grandes e reduzindo latência em até 54%

IMPACTOS NO TLS - Impactos em Certificados X.509

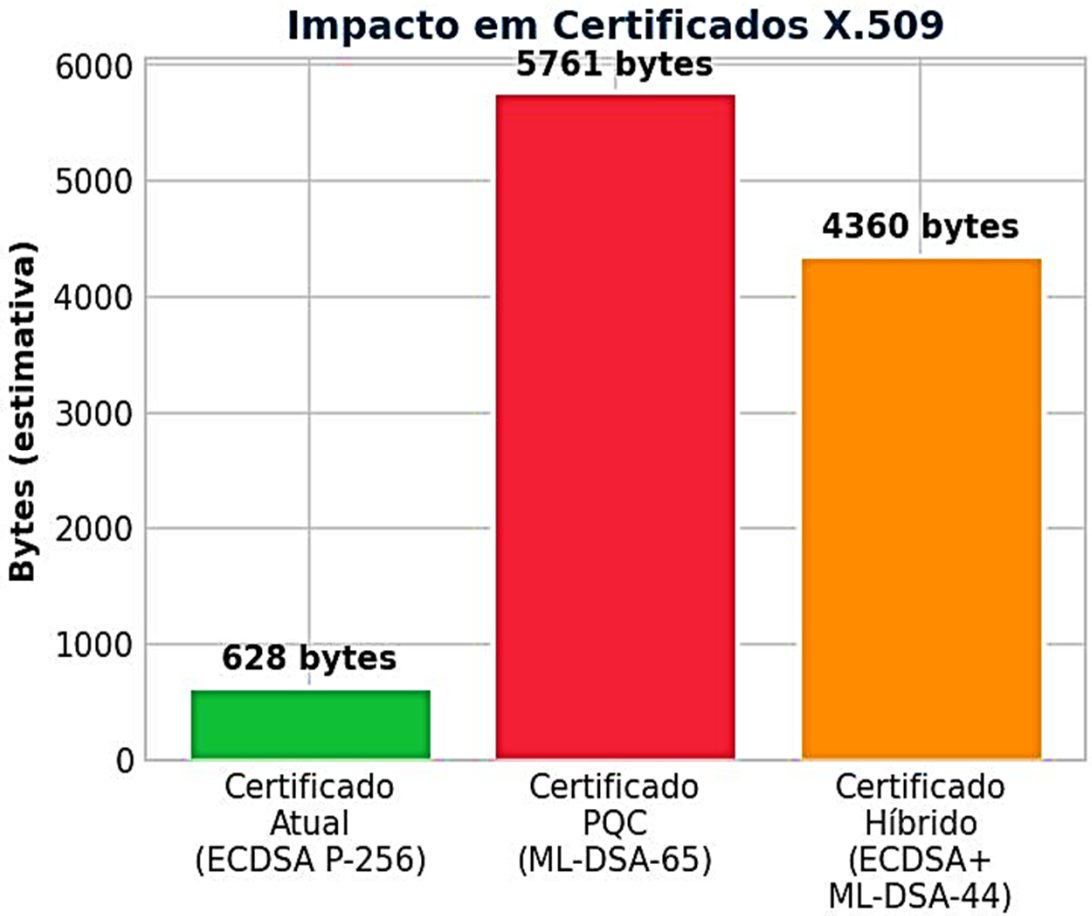
GTER 54 GTS 40

Aumento massivo no tamanho das mensagens

- Certificado **628 bytes** (ECDSA P-256) - **Clássico**
- Certificado de **5.761 bytes** com (ML-DSA-65) – **PQC**
- Certificado de **4.360 bytes** com (ECDSA P-256 + ML-DSA-44) - **Híbrido**

Clássico → PQC puro (ML-DSA-65): ~9,2x maior

PQC puro → Híbrido (ECDSA + ML-DSA-44):Redução de ~24%



Fonte: Própria

IMPACTOS NO TLS - Impactos da Fragmentação no Handshake TLS

GTER 54 GTS 40

Fragmentação obrigatória - IMPACTOS:

✓ Latência direta, perda de pacotes, Firewalls/Proxies legados e amplificação de Ataque (DDoS)

IMPACTOS NO TLS - Impactos da Fragmentação no Handshake TLS

GTER 54 GTS 40

Por que a Fragmentação PQC Impacta a Infraestrutura da Internet

ROTEADORES — 3-4x

- Buffers para pacotes de 1.5KB
- Explosão de estado em memória
- Drop de pacotes na borda

CDNs — 6x

- TLS termination na borda
- Milhoes x 5-8 pacotes cada
- Impacto em Core Web Vitals

FIREWALLS — 30-60s

- Reassembly antes de inspecionar
- Timeout por sessão fragmentada
- Drop de TLS desconhecido

MIDDLEBOXES — 20-50x

- NAT com tabelas limitadas
- Proxies sem suporte TLS 1.3
- CGNAT: milhões de usuários

LOAD BALANCERS — -70%

- Roteamento depende do 1o pacote
- Estado ate reassembly completo
- Afinidade de sessão complexa

Fragmentação gera retransmissões TCP, congestionamento, timeouts e retry storms que amplificam o problema em toda a rede.

PKI E CERTIFICADOS HÍBRIDOS

GTER 54 GTS 40

Certificado Clássico

Public Key
RSA-2048 (256 bytes)

Signature
RSA-SHA256 (256 bytes)

Total: ~1.5KB

Certificado Híbrido

Key 1
ECDSA P-256

Key 2
ML-DSA-65 (1.9KB)

Sig 1
ECDSA (64B)

Sig 2
ML-DSA-65 (3.3KB)

Total: ~6-8KB

Compatibilidade: Legados usam chave clássica

Segurança: Atualizados verificam ambas

Transição: Migração sem ruptura

ROADMAP DE MIGRAÇÃO PKI

GTER 54 GTS 40

1 — 2025-2026

Inventário

Mapeamento de sistemas

2 — 2026-2028

Piloto Híbrido

AC Raiz paralela

3 — 2028-2030

Migração

Certificados híbridos

4 — 2030-2035

Consolidação

Fim do legado

Crypto-Agility

Suportar troca de algoritmos sem reemissão

Revogação

CRLs e OCSP com novos tamanhos

Validade Longa

Certificados de hoje ativos até 2030+

GOVERNANÇA DA TRANSIÇÃO PQC

GOVERNO	TÉCNICO	ACADEMIA E INDÚSTRIA
GSI/PR Política de Segurança	**NIC.br / CGI.br** Governança Internet	**Universidades** Pesquisa em Criptografia
ITI ICP-Brasil	**RNP** Backbone Acadêmico	**SENAI CIMATEC** Capacitação Industrial
ANATEL Telecom	**CERT.br** Resposta a Incidentes	**Setor Financeiro** Bancos e Fintechs
BACEN Sistema Financeiro	**CPqD** P&D Telecom	**ISPs e Telecom** Operadoras

Salvo neste PC

Necessidade: Coordenação multissetorial para cronogramas, padrões e políticas alinhadas

|Lacuna: Brasil não possui legislação ou normativas específicas para transição criptográfica pós-quântica|

DESAFIOS DA GOVERNANÇA

GTER 54 GTS 40

⚖️ Marco Regulatório Ausente

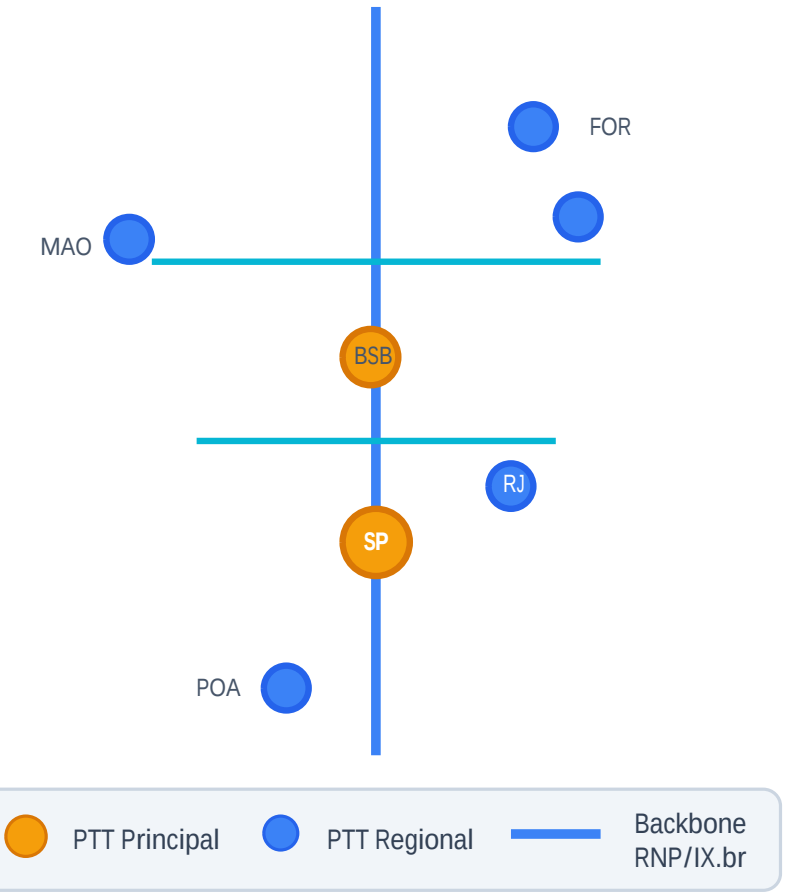
Sem legislação específica para transição PQC

🏛️ Fragmentação Institucional

Múltiplos órgãos sem coordenação central

🎓 Gap de Conhecimento

Escassez de profissionais em PQC



🌐 Interoperabilidade Global

Alinhamento NIST, ETSI, IETF necessário

🔒 Soberania Tecnológica

Dependência de HW/SW estrangeiro

💰 Custos de Migração

Investimentos em HSMs e capacitação

ENCERRAMENTO

GTER 54 GTS 40

1 Inventário Criptográfico

⏱️ Esta semana

Liste todos os certificados RSA/ECC em produção (TLS, VPN, APIs)

Identifique certificados que expiram após 2030

Mapeie equipamentos sem TLS 1.3

📋 openssl s_client -connect

2 Teste TLS Híbrido

⏱️ Este mês

Chrome/Edge já suportam X25519+ML-KEM-768 desde 2024

Cloudflare: Ative PQC grátis via dashboard

Nginx/Apache: oqs-provider + OpenSSL 3.2

🧪 blog.cloudflare.com/post-quantum-tunnel

3 Prepare a Infraestrutura

⏱️ Próximos 6 meses

Revise políticas — handshakes PQC fragmentam em 1500

Teste reassembly de pacotes TLS grandes

Métricas de latência no handshake

📊 KPI: handshake < 100ms

📚 Recursos Essenciais

- 🔗 pq-crystals.org — Implementações NIST
- 🔗 openquantumsafe.org — liboqs e oqs-provider
- 🔗 blog.cloudflare.com/pq — Guias práticos

⚠️ Por que a Urgência?

Harvest Now, Decrypt Later: Dados capturados HOJE serão descriptografados quando computadores quânticos estiverem disponíveis (2030-2035).

cgi.br nic.br

GTER 54 GTS 40

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

UFCG

1. **Doutorado em Cibersegurança**
   UFCG • 2024-2027
2. **Especialização em Microeletrônica**
   UFCG/UFSM • 2025-2026
3. **Pós em Segurança da Informação**
   PUC-PR • Completo
4. **Mestrado em Engenharia Elétrica**
   UFRN • 2016-2018
5. **Graduação em Engenharia Elétrica**
   UFRN • 2009-2015

Obrigada!

Jaqueline Silva
Jaqueline.silva@ufrpe.edu.br