# Desafios Operacionais e Estratégias para Implantação de ICPs Pós-Quânticas em Escala Nacional

**Arthur G. C. Milanez**[1], **Victor L. de Souza**[1], **Giovani Pieri**[1], **Jean Martina**[1]

[1]Departamento de Informática e Estatística – Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brazil

arthur.crippa@posgrad.ufsc.br, souza.victor@grad.ufsc.br, giovani.pieri@ufsc.br, jean.martina@ufsc.br

***Abstract.*** *This paper presents a technical and strategic case study on preparing a national regulated Public Key Infrastructure (ICP) for post-quantum digital signatures. The study discusses migration requirements, operational constraints, crypto-agility, revocation, timestamping, HSMs, smartcards, and regulatory compliance. It also evaluates the impact of replacing classical signatures with ML-DSA using approximate operational volumes from a real certificate chain and HSM benchmarks. The results indicate that the migration affects not only cryptographic algorithms, but also storage, network traffic, HSM throughput, interoperability, and governance. The paper contributes practical evidence and lessons for PKIs that need to plan post-quantum migration under continuity and compliance constraints.*

***Resumo.*** *Este artigo apresenta um estudo de caso técnico-estratégico sobre a preparação de uma Infraestrutura de Chaves Públicas (ICP) nacional e regulada para assinaturas digitais pós-quânticas. O estudo discute requisitos de migração, restrições operacionais, agilidade criptográfica, revogação, carimbo do tempo, HSMs, smartcards e conformidade normativa. Também avaliamos o impacto da substituição de assinaturas clássicas por ML-DSA a partir de volumes operacionais aproximados de uma cadeia real e de benchmarks em HSM. Os resultados indicam que a migração afeta não apenas os algoritmos criptográficos, mas também armazenamento, tráfego de rede, vazão de HSMs, interoperabilidade e governança. O trabalho contribui com evidências práticas e lições para ICPs que precisam planejar migrações pós-quânticas sob restrições de continuidade e conformidade.*

## 1. Introdução

A Infraestrutura de Chaves Públicas (ICP) é um dos pilares para a segurança da informação em ambientes digitais, possibilitando a autenticidade, integridade e não repúdio de transações eletrônicas. No Brasil, a ICP-Brasil é responsável por garantir essa confiabilidade por meio de uma cadeia hierárquica de entidades certificadoras. No entanto, o advento da computação quântica impõe ameaças concretas aos algoritmos criptográficos atualmente utilizados por essa infraestrutura.

A expectativa de que computadores quânticos sejam capazes de executar, em um tempo viável, algoritmos como o de Shor [Shor 1994], que quebra os principais esquemas de criptografia de chave pública, tem motivado uma corrida mundial pela padronização de

algoritmos resistentes à computação quântica. A introdução de alternativas pós-quânticas em sistemas já estabelecidos, como a ICP-Brasil, representa um grande desafio, especialmente considerando os requisitos legais e operacionais.

Este artigo apresenta uma análise prática dos desafios e das estratégias envolvidos na adaptação de uma infraestrutura de chaves públicas para suportar algoritmos criptográficos pós-quânticos, tomando a ICP-Brasil como estudo de caso.

## 2. Fundamentação Teórica

### 2.1. Infraestrutura de Chaves Públicas (ICP)

De acordo com Weise [Weise 2001], uma Infraestrutura de Chaves Públicas (ICP) é um conjunto de hardware, software e pessoas destinado a manusear, armazenar e distribuir certificados digitais, apoiado em políticas e procedimentos que regem o gerenciamento de certificados e chaves criptográficas.

A padronização dos certificados digitais utilizados na ICP é definida principalmente pela *Request for Comments* (RFC) 5280, que estabelece o perfil dos certificados X.509 para a infraestrutura de chaves públicas na Internet [Housley et al. 2008]. Essa padronização permite que aplicações possam adotar uma base comum para implementar suas próprias infraestruturas, garantindo interoperabilidade e segurança. O papel da ICP é emitir, gerenciar, armazenar e revogar certificados digitais, garantindo a confiabilidade e segurança do sistema. Para isso, a ICP utiliza uma cadeia de confiança.

#### 2.1.1. ICP-Brasil

A Medida Provisória nº 2.200-2 [Brasil 2001] instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão e de empresas. O modelo brasileiro é o de certificação com raiz única. A AC-Raiz é a primeira autoridade da cadeia de certificação. Na ICP-Brasil, o ITI (Instituto Nacional de Tecnologia da Informação) é responsável pela AC-Raiz, que executa as políticas de certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Além disso, o ITI também é responsável por credenciar e descredenciar os demais participantes da cadeia, supervisionar e auditar os processos [Instituto Nacional de Tecnologia da Informação 2024].

### 2.2. Criptografia Pós-Quântica

A criptografia pós-quântica é um campo da criptografia que estuda algoritmos resistentes às ameaças decorrentes da computação quântica. A principal motivação por trás dessa área é a existência de algoritmos quânticos, como o de Shor [Shor 1994], que comprometem a segurança dos esquemas criptográficos atualmente utilizados em larga escala, como RSA (Rivest-Shamir-Adleman) e DSA (Digital Signature Algorithm).

A criptografia pós-quântica busca soluções baseadas em problemas matemáticos difíceis, até mesmo para computadores quânticos, mantendo a compatibilidade com computadores clássicos. Por isso, é considerada a alternativa mais viável para modernizar os sistemas atuais. Nos últimos anos, diversas instituições de

padronização, como o NIST (*National Institute of Standards and Technology*), têm conduzido processos rigorosos de avaliação e seleção de algoritmos criptográficos pós-quânticos [Bernstein and Lange 2017].

No processo de padronização conduzido pelo NIST, algoritmos de diferentes famílias matemáticas foram avaliados, resultando na seleção de um conjunto de esquemas considerados seguros e eficientes. Entre os principais algoritmos padronizados, destacam-se ML-KEM (Kyber), ML-DSA (Dilithium) e SLH-DSA (SPHINCS+) [NIST 2024b, NIST 2024a, NIST 2024c]. Acompanhando esse movimento global, a transição para algoritmos pós-quânticos na ICP-Brasil foi oficialmente regulamentada pela Instrução Normativa ITI nº 35/2026 [Instituto Nacional de Tecnologia da Informação (ITI) 2026].

## 3. Trabalhos Relacionados

O processo de padronização conduzido pelo NIST consolidou os primeiros algoritmos pós-quânticos recomendados para uso geral, incluindo ML-KEM, ML-DSA e SLH-DSA [NIST 2024b, NIST 2024a, NIST 2024c]. Esses documentos definem as primitivas criptográficas e seus parâmetros, mas não descrevem, por si só, como infraestruturas de certificação digital já implantadas devem conduzir a migração. De forma complementar, o relatório de transição do NIST discute prazos e diretrizes gerais para a substituição de algoritmos clássicos vulneráveis a computadores quânticos [Moody et al. 2024].

Outra linha de trabalhos discute agilidade criptográfica como requisito para sistemas capazes de substituir algoritmos e parâmetros com menor impacto operacional. Nelson [Nelson 2011] trata esse conceito no contexto de protocolos de autenticação, enquanto Alnahawi et al. [Alnahawi et al. 2023] analisam o estado da arte em criptoagilidade e os desafios de sua adoção. O NIST também relaciona a dificuldade histórica de migração de SHA-1 à ausência de mecanismos adequados de interoperabilidade, compatibilidade e substituição coordenada de primitivas criptográficas [National Institute of Standards and Technology 2022, Barker et al. 2025].

Estudos recentes também analisam obstáculos específicos para a adoção de criptografia pós-quântica em ambientes governamentais e de identidade digital. Vakarjuk et al. [Vakarjuk et al. 2024], por exemplo, avaliam desafios da migração pós-quântica no ecossistema da Estônia, destacando limitações associadas a *smartcards*, requisitos regulatórios e compatibilidade com sistemas existentes. Esses aspectos são próximos aos enfrentados por ICPs nacionais, nas quais dispositivos de usuário, *Hardware Security Modules* (HSMs), políticas de certificação e aplicações legadas precisam evoluir de forma coordenada.

Diferentemente desses trabalhos, este artigo analisa a preparação de uma ICP nacional regulada em contexto brasileiro real, considerando não apenas desempenho criptográfico, mas também HSMs, Listas de Certificados Revogados (LCRs), Autoridades de Carimbo de Tempo (ACTs), *smartcards*, conformidade normativa e continuidade operacional. A contribuição está no relato técnico-estratégico da migração no contexto da ICP-Brasil e na identificação de requisitos práticos para adoção de assinaturas pós-quânticas em uma infraestrutura nacional de certificação digital.

## 4. Problemas e Requisitos

Nos últimos anos, algoritmos criptográficos pós-quânticos (PQC) passaram de propostas acadêmicas para implementações amplamente disponíveis em bibliotecas criptográficas modernas, como versões recentes do OpenSSL e outras pilhas de software consolidadas. Apesar dessa maturidade crescente, a adoção prática desses algoritmos enfrenta desafios significativos em ambientes reais, especialmente devido à presença de sistemas legados. Muitas dessas aplicações operam sobre versões antigas de sistemas operacionais, linguagens de programação ou dependências que não oferecem suporte nativo a primitivas pós-quânticas. A atualização desses componentes nem sempre é trivial, podendo envolver riscos operacionais, incompatibilidades e altos custos de manutenção, o que cria uma barreira relevante para a migração efetiva rumo a um ecossistema criptográfico resistente a ataques quânticos.

A migração de SHA-1 ilustra que a substituição de primitivas criptográficas em sistemas reais pode levar anos, especialmente quando há dependência de compatibilidade retroativa, interoperabilidade e sistemas legados [National Institute of Standards and Technology 2022, Barker et al. 2025]. Esse padrão de inércia é recorrente e decorre de causas distintas. No caso do RC4, a defasagem entre a publicação de ataques práticos, em 2013 [AlFardan et al. 2013], e sua desabilitação pelos principais navegadores evidencia que a fragilidade demonstrada de um algoritmo não se traduz automaticamente em sua remoção do ecossistema: medições longitudinais indicam que parcela expressiva dos clientes ainda anunciava suporte à cifra em 2018 [Kotzias et al. 2018]. No caso dos parâmetros Diffie-Hellman de "grau de exportação", herdados de restrições legais da década de 1990 e mantidos por retrocompatibilidade mesmo após a revogação dessas restrições, a dívida técnica acumulada permaneceu explorável por décadas, culminando no ataque Logjam [Adrian et al. 2015]. Em dispositivos de rede embarcados, por sua vez, a limitação é estrutural: restrições de entropia disponível na inicialização comprometem a geração de chaves e representam um obstáculo que se acentua à medida que novos esquemas impõem requisitos mais rigorosos de aleatoriedade e de capacidade computacional [Heninger et al. 2012]. Tomados em conjunto, esses casos indicam que a adoção de algoritmos pós-quânticos pode enfrentar atritos análogos, decorrentes de inércia de ecossistema, de dívida técnica acumulada por retrocompatibilidade e de limitações de hardware legado. Isso reforça a necessidade de estratégias graduais e de mecanismos de transição que viabilizem a convivência entre tecnologias antigas e novas por um período prolongado.

Embora a experiência histórica indique que a adoção de novos padrões criptográficos ocorre de forma gradual, o cenário atual é marcado por um senso de urgência maior, impulsionado pelo risco de avanços na computação quântica e pelas recomendações de órgãos de padronização. O NIST estabelece que RSA-2048, ECDSA-224, DH-2048 e ECDH-224, todos com aproximadamente 112 bits de segurança, serão depreciados em 2030 e proibidos a partir de 2035, recomendando que sistemas críticos dependentes de criptografia de chave pública iniciem com urgência a migração para algoritmos resistentes a ataques quânticos [Moody et al. 2024]. Isso torna imprescindível o início dos testes com algoritmos pós-quânticos, ao mesmo tempo em que demanda cautela para não comprometer a interoperabilidade e a conformidade com padrões ainda em definição.

### 4.1. Modelo de ameaça

O conceito de Harvest Now, Decrypt Later (HNDL) refere-se a uma estratégia de ataque na qual adversários coletam e armazenam grandes volumes de dados cifrados no presente, com o objetivo de decifrá-los no futuro, quando recursos computacionais mais avançados se tornarem disponíveis. Dessa forma, mesmo que os dados estejam protegidos atualmente, informações sensíveis com longo tempo de sigilo, como registros governamentais, dados financeiros e comunicações estratégicas, podem estar expostas a uma quebra retroativa de confidencialidade. Esse cenário reforça a necessidade de adoção antecipada de mecanismos resistentes a ataques quânticos, especialmente em contextos em que a proteção da informação deve ser garantida por longos períodos.

### 4.2. Cenário de ruptura criptográfica

Diante de uma ruptura criptográfica causada por computadores quânticos, o primeiro passo seria identificar os componentes de maior impacto. Em uma Infraestrutura de Chaves Públicas, os elementos mais críticos são as Autoridades Certificadoras, em especial a AC-Raiz, que representa a âncora de confiança de toda a cadeia. A contenção inicial passaria pela redução da superfície de ataque: interrupção da emissão de certificados baseados em algoritmos clássicos, redução do período de validade dos certificados ainda ativos e exigência de revalidações mais frequentes, limitando o tempo de exposição e dificultando a exploração de chaves comprometidas.

Após a contenção, uma das estratégias possíveis envolve o estabelecimento de uma nova cadeia de confiança baseada em algoritmos pós-quânticos, iniciada pela criação de uma nova AC-Raiz e operando em paralelo à cadeia existente, o que permitiria uma transição gradual e controlada. Essa abordagem traz desafios relevantes de interoperabilidade, gestão de confiança entre cadeias distintas e complexidade operacional.

### 4.3. Continuidade operacional e interoperabilidade

A ausência de mecanismos de transição agrava significativamente o problema. Sem a possibilidade de coexistência entre algoritmos clássicos e pós-quânticos, torna-se necessário optar entre segurança e compatibilidade. Essa limitação força uma migração abrupta, aumentando consideravelmente o risco de falhas operacionais e a possibilidade de indisponibilidade de serviços críticos. Por esse motivo, abordagens híbridas são frequentemente apontadas como uma estratégia conservadora para viabilizar a transição, permitindo a convivência entre diferentes paradigmas criptográficos durante o período de adaptação.

Apesar dessa vantagem, a adoção ampla de uma cadeia híbrida introduz custos relevantes em uma ICP nacional regulada. Perfis de certificados precisam ser redefinidos, HSMs homologados, políticas de certificação atualizadas, aplicações adaptadas e testes de interoperabilidade repetidos para cada novo formato adotado. Um modelo transitório híbrido exigiria, portanto, dupla adequação normativa e sistêmica do ecossistema: uma primeira revisão regulatória e de *software* para suportar o padrão híbrido e, posteriormente, uma nova migração para o modelo exclusivamente pós-quântico. Considerando que atores relevantes da indústria, como o Google, passaram a tratar 2029 como marco de prontidão para migração para criptografia pós-quântica [Adkins and Schmieg 2026], e que certificados de AC-Raiz podem ter validade de até dez anos, esse esforço duplicado pode não ser operacionalmente viável dentro do horizonte disponível. Soma-se a isso o

fato de que a combinação de chaves clássicas e pós-quânticas aumenta o tamanho de certificados e assinaturas, agravando os custos de armazenamento, tráfego e validação. Por essas razões, neste trabalho a abordagem totalmente pós-quântica é priorizada como caminho de preparação direta da infraestrutura, enquanto mecanismos híbridos permanecem como alternativas pontuais para compatibilidade e fases controladas de transição.

### 4.4. Revogação e preservação temporal

Um desafio crítico no contexto de uma ruptura criptográfica está relacionado ao processo de revogação de certificados. Em um cenário em que algoritmos clássicos, como RSA, tornam-se vulneráveis, as próprias LCRs, por serem assinadas por autoridades potencialmente comprometidas, deixam de ser confiáveis como fonte operacional de revogação. Isso compromete mecanismos tradicionais de gestão de confiança dentro da ICP e reforça a necessidade de preparação antecipada das autoridades responsáveis por revogação.

Para mitigar esse problema, as Autoridades Certificadoras Raiz devem estar preparadas para operar, direta ou indiretamente, com algoritmos pós-quânticos, possibilitando a emissão de novas LCRs assinadas com primitivas resistentes a ataques quânticos. Listas históricas de revogação não devem ser reutilizadas diretamente como fonte de confiança operacional em um cenário de quebra criptográfica; sua preservação deve ser tratada como evidência temporal, não como mecanismo ativo de continuidade.

Nesse contexto, o carimbo do tempo pós-quântico surge como mecanismo complementar. Uma ACT baseada em algoritmos pós-quânticos pode atestar que determinado certificado, assinatura ou documento existia antes de um marco temporal específico e não foi alterado desde então. Essa abordagem pode auxiliar na preservação de evidências e na transição de documentos assinados com algoritmos clássicos, mas não elimina a necessidade de migração completa para novos certificados, novas LCRs e cadeias de confiança resistentes a ataques quânticos.

### 4.5. Conformidade normativa

Um dos principais desafios enfrentados no processo de adaptação do Software de Gerenciamento de Certificados para o cenário pós-quântico foi o fato de o desenvolvimento ter se iniciado antes da finalização do processo de padronização dos algoritmos pós-quânticos realizado pelo NIST. Na época, diversos esquemas estavam em fase de avaliação, e ainda não havia uma definição clara sobre quais algoritmos seriam recomendados para uso em aplicações reais. Essa incerteza exigiu que o projeto fosse conduzido com flexibilidade, prevendo alterações futuras na escolha das primitivas criptográficas, interfaces e parâmetros de segurança.

No contexto da ICP-Brasil, a situação se mostra ainda mais delicada. A infraestrutura nacional segue um modelo altamente regulado, com normas técnicas e políticas de certificação rígidas, definidas por documentos como a DOC-ICP-01 e suas complementares. Qualquer modificação no formato dos certificados digitais, nos algoritmos utilizados ou nos processos de emissão e validação deve respeitar essas diretrizes e, em muitos casos, depende de alterações formais nas regras da cadeia.

Assim, a combinação entre padronizações ainda em evolução, alertas de descontinuidade de algoritmos tradicionais e o ambiente restritivo da ICP-Brasil impôs um

cenário de transição particularmente complexo. O desenvolvimento do SGC-PQ, portanto, precisou considerar não apenas os aspectos técnicos da substituição criptográfica, mas também estratégias para garantir compatibilidade, conformidade e flexibilidade para futuras mudanças normativas.

### 4.6. Dispositivos criptográficos

Dispositivos como *smartcards* ou *tokens* são utilizados em diversas ICPs para autenticação de operadores, porém esses dispositivos apresentam limitações relevantes no contexto da transição para criptografia pós-quântica. Em geral, são tecnologias legadas com baixa capacidade de processamento e memória restrita, dificultando o suporte a algoritmos pós-quânticos, cujas chaves e assinaturas possuem dimensões significativamente maiores. Além disso, a ausência de padronização histórica resultou em um ecossistema heterogêneo, no qual diferentes fabricantes utilizam interfaces e softwares proprietários, ampliando desafios de integração, manutenção e interoperabilidade.

Nesse cenário, surge o desafio de garantir a autenticidade das entidades em cadeias de certificação híbridas, nas quais algoritmos clássicos e pós-quânticos coexistem simultaneamente. Paralelamente, observa-se uma tendência de substituição dos smartcards por dispositivos criptográficos mais modernos, como tokens USB e HSMs compactos, que oferecem maior capacidade computacional, melhor suporte a novos algoritmos e maior flexibilidade de integração. Essa evolução tecnológica pode representar um elemento importante para viabilizar a adoção gradual de mecanismos pós-quânticos em infraestruturas de certificação digital.

### 4.7. Escolha de algoritmos e agilidade criptográfica

A escolha dos algoritmos criptográficos a serem adotados em uma ICP pós-quântica representa um dos principais desafios da transição. Diferentemente dos algoritmos clássicos, como RSA e ECC, que possuem décadas de análise e validação, os algoritmos pós-quânticos ainda são relativamente recentes e continuam sendo objeto de estudo pela comunidade científica. Durante o processo de padronização conduzido pelo NIST, diversos algoritmos candidatos foram propostos e posteriormente descartados após a identificação de vulnerabilidades. Esse histórico reforça a necessidade de cautela na adoção de novos esquemas criptográficos, especialmente em infraestruturas críticas como as ICPs.

A escolha de um algoritmo envolve uma série de *trade-offs*, incluindo o tamanho das chaves e assinaturas, o desempenho computacional e a viabilidade de implementação em diferentes ambientes. Algoritmos com melhor desempenho computacional, como os esquemas baseados em reticulados (*lattices*) representados pelo ML-DSA [NIST 2024a], podem exigir chaves públicas e assinaturas digitais consideravelmente maiores, o que aumenta o tamanho final dos certificados e impacta diretamente o armazenamento e a transmissão na rede. Por outro lado, alternativas que focam em chaves substancialmente menores, como os esquemas baseados em isogenias (com destaque para o SQI-sign [De Feo et al. 2020]), podem impor custos computacionais significativamente mais elevados para a geração e verificação de assinaturas.

Outro aspecto crítico a ser considerado é o longo ciclo de vida dos certificados digitais, especialmente em níveis superiores da cadeia, como certificados de Autoridades Certificadoras raiz, que podem ter validade de até uma década. A substituição ou

revogação desses certificados é um processo complexo e sensível, o que reforça a importância de uma escolha criteriosa dos algoritmos a serem adotados desde as fases iniciais da migração.

## 5. Metodologia

Este trabalho adota uma metodologia de estudo de caso técnico em uma infraestrutura de certificação digital nacional e regulada. O objeto de análise é a preparação do Sistema de Gerência de Certificados (SGC), utilizado no contexto da ICP-Brasil, para suportar algoritmos de assinatura pós-quânticos, combinando análise documental, inventário criptográfico, provas de conceito, integração com componentes criptográficos e avaliação comparativa de impactos. O estudo concentra-se nos componentes relacionados ao ciclo de vida de certificados digitais, incluindo geração e armazenamento de chaves, emissão, assinatura, validação e revogação. O escopo foi limitado a algoritmos de assinatura digital, por afetarem diretamente certificados X.509, LCRs, cadeias de certificação, documentos assinados e operações realizadas por ACs; mecanismos de encapsulamento de chaves e estratégias híbridas são discutidos como requisitos de transição, mas não constituem o foco experimental desta etapa.

## 6. Estratégia de Migração no SGC

A estratégia de migração estudada para aplicação na ICP-Brasil partiu do princípio da agilidade criptográfica [Nelson 2011]. Este conceito, definido como a capacidade de um sistema substituir algoritmos criptográficos com impacto reduzido, orientou as fases do projeto. Embora os diálogos sobre a ameaça quântica à soberania digital do país tenham sido iniciados previamente junto ao órgão gestor, o projeto de adaptação teve seu início formal em 2024. Nessa etapa, o entendimento da ameaça já estava consolidado entre as partes interessadas, fruto de um esforço prévio de conscientização.

A abordagem metodológica adotada combinou o caráter exploratório da pesquisa universitária com as necessidades pragmáticas de um sistema em produção. O processo foi estruturado em fases sequenciais e iterativas, conforme detalhado a seguir.

### 6.1. Fase 1: Pesquisa, análise e capacitação

O marco inicial do projeto foi dedicado ao estudo dos algoritmos PQC. Foram conduzidas provas de conceito isoladas, desvinculadas inicialmente da complexidade dos SGCs, com o objetivo de compreender as características operacionais, as particularidades de implementação e levantar métricas de desempenho preliminares dos novos algoritmos criptográficos. Paralelamente, esta fase foi crucial para a capacitação técnica da equipe de desenvolvimento, que adquiriu experiência na manipulação de bibliotecas PQC como Bouncy Castle[1] e liboqs[2].

### 6.2. Fase 2: Análise de dependências e inventário criptográfico

Uma análise sistêmica identificou os pontos de maior impacto da migração. Considerando que os SGCs utilizam HSMs para armazenamento seguro e operações criptográficas, a

[1] `https://www.bouncycastle.org/`

[2] A liboqs é uma biblioteca C de código aberto para algoritmos criptográficos pós-quânticos, mantida pelo projeto Open Quantum Safe (OQS). Disponível em: https://github.com/open-quantum-safe/liboqs

atualização destes módulos surgiu como um pré-requisito crítico. Essa tarefa foi priorizada por ser uma dependência externa que poderia ser executada em paralelo com a reestruturação do código. Para viabilizar o desenvolvimento, o fornecedor do hardware (Kryptus[3]) disponibilizou uma versão beta do firmware e do software, permitindo o início imediato dos trabalhos. Essa etapa foi seguida da capacitação da equipe para operar o HSM com o algoritmo de assinatura Dilithium, garantindo autonomia para a realização de testes e pilotos.

Concluída a análise de dependências, foi realizado um inventário criptográfico, mapeando todos os algoritmos em uso e os respectivos trechos de código impactados. Neste ponto, foram estabelecidas duas restrições de escopo fundamentais: priorizar a migração de algoritmos de assinatura digital e desconsiderar, nesta etapa, implementações híbridas que combinam criptografia clássica e pós-quântica. Essa delimitação permitiu concentrar os esforços iniciais na abordagem totalmente pós-quântica e nos componentes mais diretamente afetados pela emissão e validação de certificados.

Com base neste inventário, a equipe de coordenação priorizou as funcionalidades a serem migradas, utilizando como critérios o valor de negócio, o risco associado e a complexidade técnica da implementação.

### 6.3. Fase 3: Implementação, integração e validação

Nesta fase, as bibliotecas criptográficas internas foram atualizadas para incorporar os novos algoritmos disponibilizados pelo HSM e pelas bibliotecas de software. A atualização das dependências nos módulos do sistema resultou em quebras de compatibilidade, que foram identificadas e corrigidas durante os ciclos de homologação interna. Seguindo a ordem de priorização definida, iniciou-se a modificação dos módulos para gerenciar todo o ciclo de vida de certificados pós-quânticos. Os componentes exigiram alterações coordenadas para manter a consistência do sistema. Os desafios de compatibilidade foram recorrentes, demandando um esforço contínuo de integração e teste.

### 6.4. Fase 4: Ciclo de agilidade criptográfica

A conclusão do processo de padronização do NIST, com a publicação dos padrões FIPS 203, 204 e 205, impôs a necessidade de um novo ciclo iterativo. Este ciclo, ilustrado no fluxograma 1, compreende a atualização dos artefatos de hardware e software para as versões estáveis que implementam os algoritmos padronizados. Em seguida, o processo de revisão do inventário criptográfico, refatoração de bibliotecas e implementação foi reiniciado, reforçando a importância da agilidade criptográfica como pilar estratégico do projeto. A experiência prévia com substituição de algoritmos, embora de menor impacto, forneceu uma base de código que facilita essa evolução, ainda que a migração para PQC apresente desafios de segurança, integração e desempenho.

## 7. Avaliação de Impacto

Esta seção avalia o impacto da substituição de algoritmos clássicos por assinaturas pós-quânticas em uma cadeia de certificação real. A análise considera dois eixos: o aumento no tamanho dos artefatos criptográficos e o impacto operacional observado a partir de volumes reais de certificados e assinaturas. Os dados apresentados são agregados e extraídos

[3] `https://kryptus.com/`

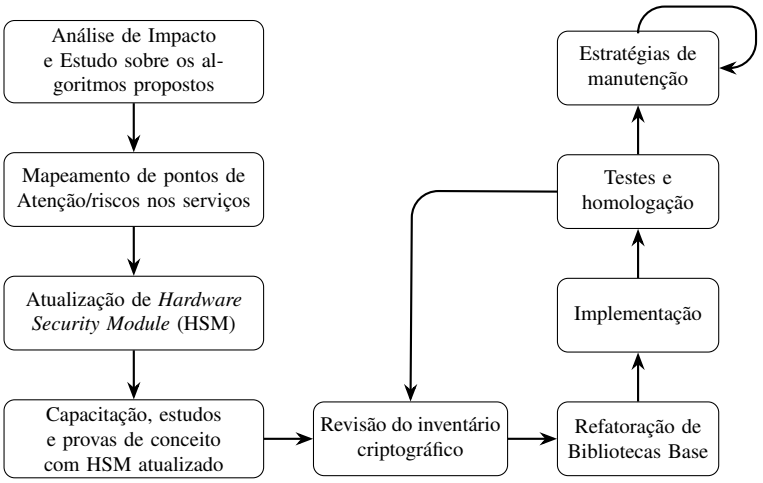


**Figura 1. Fluxograma de estratégia para migração pós-quântica.**

de registros internos da infraestrutura analisada. Por restrições de confidencialidade, não são divulgados identificadores de entidades, detalhes de configuração ou séries completas, e os volumes são apresentados de forma aproximada, com arredondamentos que preservam a ordem de grandeza e permitem avaliar o impacto técnico sem expor valores exatos.

### 7.1. Impacto no tamanho dos artefatos

A atualização de uma Infraestrutura de Chaves Públicas (ICP) para um cenário pós-quântico demanda um estudo abrangente não apenas do ponto de vista lógico, mas também das implicações físicas e operacionais decorrentes da adoção de novos algoritmos. Neste trabalho, foram realizados testes comparativos entre algoritmos clássicos (RSA) e pós-quânticos (ML-DSA), considerando artefatos diretamente afetados por uma cadeia de certificação: assinaturas, chaves públicas e certificados. Para ML-DSA, os tamanhos de chaves públicas e assinaturas seguem os parâmetros definidos na FIPS 204 [NIST 2024a]; os tamanhos de certificados X.509 dependem do perfil, extensões e codificação utilizados, e por isso foram medidos em certificados de teste com perfil compatível com o cenário analisado.

| Algoritmo | Assinatura | Chave pública | Certificado |
|---|---|---|---|
| RSA-2048 | 0,25 KB | 451 B | 1,3 KB |
| RSA-3072 | 0,38 KB | 625 B | 1,7 KB |
| RSA-15360 | 1,88 KB | 2,7 KB | 5,7 KB |
| ML-DSA-44 | 2,42 KB | 1,31 KB | 5,6 KB |
| ML-DSA-65 | 3,31 KB | 1,95 KB | 7,6 KB |
| ML-DSA-87 | 4,63 KB | 2,59 KB | 11,0 KB |

**Tabela 1. Tamanho de assinaturas, chaves públicas e certificados em algoritmos clássicos e pós-quânticos [NIST 2024a]**

Os resultados da Tabela 1 indicam que, no nível 1 de segurança, a substituição de RSA-2048 por ML-DSA-44 aumenta o tamanho da assinatura de aproximadamente 0,25

KB para 2,42 KB, ou cerca de 9,7 vezes. O tamanho do certificado passa de cerca de 1,3 KB para 5,6 KB, crescimento de aproximadamente 4,3 vezes. Esse aumento é administrável para operações isoladas, mas torna-se relevante em uma infraestrutura nacional, na qual certificados e assinaturas são produzidos, armazenados, transmitidos e verificados em escala.

### 7.2. Impacto em uma cadeia real

Os registros operacionais analisados mostram uma infraestrutura com volume acumulado da ordem de dezenas de milhões de certificados e centenas de milhões de assinaturas. Para preservar a confidencialidade da cadeia analisada, os valores são apresentados de forma aproximada na Tabela 2. Ainda assim, os números permitem observar a escala do problema: em um único ano recente, a infraestrutura produziu dezenas de milhões de certificados e mais de duzentos milhões de assinaturas, com picos diários superiores a um milhão de operações de assinatura.

| **Métrica operacional** | **Valor aproximado** |
|---|---:|
| Certificados gerados | $\approx$ 57 milhões |
| Certificados válidos | $\approx$ 26 milhões |
| Assinaturas realizadas | $\approx$ 467 milhões |
| Certificados gerados em um ano recente | $\approx$ 24 milhões |
| Assinaturas realizadas em um ano recente | $\approx$ 214 milhões |
| Maior volume mensal de certificados | $\approx$ 2,2 milhões |
| Maior volume mensal de assinaturas | $\approx$ 21 milhões |
| Maior volume diário de certificados | $\approx$ 130 mil |
| Maior volume diário de assinaturas | $\approx$ 1,3 milhão |

**Tabela 2. Volumes agregados aproximados observados na cadeia real analisada**

Com base nesses volumes, a diferença de tamanho dos artefatos deixa de ser irrelevante. A Tabela 3 estima o impacto em armazenamento considerando RSA-2048 como referência clássica e ML-DSA-44 como alternativa pós-quântica de menor parâmetro. A projeção considera apenas o tamanho dos certificados e assinaturas, sem incluir metadados de banco de dados, índices, logs, replicação, backups ou estruturas auxiliares. Portanto, os valores devem ser interpretados como uma estimativa conservadora do impacto mínimo sobre dados armazenados e trafegados.

A projeção mostra que certificados gerados em um ano recente passariam de aproximadamente 31 GB para 134 GB caso fossem emitidos com ML-DSA-44. No acumulado da cadeia analisada, o volume associado apenas a certificados passaria de aproximadamente 74 GB para 319 GB. O impacto é ainda mais expressivo quando se consideram assinaturas armazenadas ou transmitidas de forma independente: o volume anual passaria de aproximadamente 54 GB para 520 GB, enquanto o acumulado sairia de aproximadamente 117 GB para cerca de 1,1 TB. Assim, a principal preocupação não é apenas o tamanho de um certificado individual, mas o efeito acumulado sobre armazenamento, transmissão, replicação e processamento em sistemas de alto volume.

| Cenário | RSA-2048 | ML-DSA-44 | Aumento |
|---|---|---|---|
| Certificados em um ano recente | $\approx$ 31 GB | $\approx$ 134 GB | 4,3x |
| Certificados acumulados | $\approx$ 74 GB | $\approx$ 319 GB | 4,3x |
| Assinaturas em um ano recente | $\approx$ 54 GB | $\approx$ 520 GB | 9,7x |
| Assinaturas acumuladas | $\approx$ 117 GB | $\approx$ 1,1 TB | 9,7x |

**Tabela 3. Estimativa aproximada de armazenamento para certificados e assinaturas**

### 7.3. Desempenho em HSM

Além do tamanho dos artefatos, o desempenho em HSM é um ponto crítico para uma ICP, pois autoridades certificadoras dependem de *hardware* criptográfico para operações sensíveis. Para avaliar esse impacto, foram conduzidos testes de desempenho focados na geração e verificação de assinaturas digitais. O ambiente experimental utilizou uma instância única (sem configuração de *cluster*) de um HSM modelo kNET[4], fabricado pela Kryptus. A comunicação com o equipamento foi realizada por meio de um *wrapper* privado desenvolvido sobre uma biblioteca Java de comunicação KMIP (versão 4.8.1), fornecida pela própria fabricante.

Foram executados *benchmarks* de geração de chaves e assinatura em HSM com RSA-2048, RSA-3072, RSA-4096 e os parâmetros ML-DSA-44, ML-DSA-65 e ML-DSA-87. A Tabela 4 apresenta a média e o percentil 95 (P95) de ambas as operações. Optou-se pelo P95 em vez do desvio padrão porque medições de latência de rede e de I/O de *hardware* apresentam distribuição assimétrica de cauda longa, na qual *outliers* esporádicos distorcem a variância; percentis são, nesse cenário, estimadores mais robustos do limite superior do tempo de resposta.

| Algoritmo | Geração de Chaves | | Assinatura | |
|---|---|---|---|---|
| | Média | P95 | Média | P95 |
| RSA-2048 | 782,6 ms | 1350,6 ms | 5,5 ms | 6,2 ms |
| RSA-3072 | 1695,8 ms | 3315,0 ms | 14,6 ms | 16,57 ms |
| RSA-4096 | 3920,7 ms | 8017,2 ms | 11,2 ms | 12,78 ms |
| ML-DSA-44 | 126,8 ms | 165,2 ms | 54,9 ms | 68,9 ms |
| ML-DSA-65 | 132,9 ms | 173,9 ms | 57,9 ms | 74,5 ms |
| ML-DSA-87 | 141,9 ms | 194,9 ms | 58,0 ms | 78,6 ms |

**Tabela 4. Desempenho em HSM: Tempo de geração de chaves e assinatura para algoritmos clássicos e pós-quânticos**

Os resultados indicam que ML-DSA apresenta tempo médio de assinatura aproximadamente 9,3 a 9,8 vezes maior que RSA-2048 e aproximadamente 4,9 a 5,2 vezes

[4]Kryptus kNET HSM. Disponível em: `https://kryptus.com/knet-hsm/`

maior que RSA-4096 no HSM avaliado (Tabela 4). Em termos de vazão teórica sequencial, RSA-2048 alcançaria cerca de 169 assinaturas por segundo, enquanto ML-DSA operaria em torno de 17 a 18 assinaturas por segundo. Embora a operação real de uma ICP possa distribuir carga entre múltiplos HSMs, filas e serviços, essa diferença mostra que o gargalo de implantação não está apenas no tamanho dos certificados, mas também na capacidade de assinatura em *hardware* certificado.

A geração de chaves apresenta comportamento inverso, conforme também evidenciado na Tabela 4. Embora ML-DSA aumente o tempo de assinatura, a geração de pares de chaves foi aproximadamente 5,5 a 6,2 vezes mais rápida que RSA-2048 e cerca de 27,6 a 30,9 vezes mais rápida que RSA-4096.

Em termos de impacto operacional e de riscos para a arquitetura atual, quando esses tempos de processamento são comparados com os volumes aproximados da Tabela 2, observa-se que um pico diário da ordem de 1,3 milhão de assinaturas equivale a uma média de aproximadamente 15 assinaturas por segundo se distribuído ao longo de 24 horas, ou cerca de 45 assinaturas por segundo em uma janela operacional de 8 horas. Esse valor supera a vazão sequencial estimada para um único HSM executando ML-DSA, indicando gargalos críticos de capacidade e a necessidade mandatória de paralelismo, balanceamento de carga, dimensionamento de filas ou expansão do parque de *hardware* em cenários de alta demanda. Para a emissão de certificados, um pico diário da ordem de 130 mil artefatos equivale a cerca de 1,5 emissão por segundo em 24 horas, ou 4,5 emissões por segundo em 8 horas, representando uma carga mais administrável, mas ainda restrita por cerimônias criptográficas, políticas de emissão e pelo tempo de geração de chaves.

### 7.4. Discussão

Os resultados reforçam que a migração para assinaturas pós-quânticas também deve ser tratada como um problema de engenharia de infraestrutura. O aumento de tamanho dos artefatos impacta armazenamento, repositórios, tráfego e compatibilidade de aplicações. O desempenho em HSM, por sua vez, afeta a capacidade de emissão e assinatura em períodos de pico. Em uma cadeia com centenas de milhões de assinaturas acumuladas e dezenas de milhões de certificados emitidos, diferenças aparentemente pequenas por operação tornam-se relevantes em escala.

Por fim, tokens criptográficos e *smartcards* podem não suportar algoritmos pós-quânticos sem atualização ou substituição, cujo custo envolve aquisição de equipamentos, testes, certificações e integração. A transição exige, portanto, coordenação entre múltiplos atores em uma ICP nacional regulada, na qual desempenho, conformidade e interoperabilidade precisam evoluir de forma conjunta.

## 8. Trabalhos Futuros

Como trabalhos futuros, pretende-se aprofundar os testes de interoperabilidade de uma cadeia de certificação totalmente pós-quântica com os componentes do ecossistema da ICP-Brasil. Embora bibliotecas criptográficas recentes já ofereçam suporte a algoritmos como ML-DSA, ainda é necessário avaliar a compatibilidade desses certificados com validadores, assinadores, leitores de certificado, aplicações governamentais e padrões amplamente utilizados, como X.509, *Cryptographic Message Syntax* (CMS), *Online Certificate Status Protocol* (OCSP) e *Transport Layer Security* (TLS).

A adoção de estratégias híbridas, frequentemente recomendada na literatura para o período de transição, foi deliberadamente mantida fora do escopo experimental deste trabalho pelas razões discutidas na Seção 4.3, associadas ao esforço duplicado de adequação normativa e sistêmica exigido pelo contexto regulado brasileiro. Ainda assim, trata-se de um eixo relevante para investigação futura, sobretudo quanto ao custo real de validação de certificados híbridos e a cenários em que a compatibilidade com cadeias legadas seja requisito inegociável.

Outro eixo relevante envolve estudos aprofundados sobre revogação e preservação temporal em um cenário pós-quântico. Trabalhos futuros devem avaliar o impacto de assinaturas pós-quânticas em LCRs e respostas OCSP, bem como o uso de Autoridades de Carimbo do Tempo pós-quânticas para preservar evidências associadas a documentos e certificados emitidos antes da migração completa. Essa linha é especialmente importante para garantir continuidade jurídica e operacional durante a substituição gradual das cadeias clássicas.

Por fim, pretende-se investigar a adequação normativa e operacional da ICP-Brasil para certificados pós-quânticos, incluindo perfis de certificado, políticas de certificação, requisitos de auditoria e dispositivos criptográficos utilizados por operadores e usuários finais. Nesse contexto, a coexistência entre cadeias clássicas legadas e novas cadeias pós-quânticas deve ser analisada como problema de governança e interoperabilidade, sem depender necessariamente da adoção ampla de certificados híbridos.

## 9. Conclusão

Este artigo apresentou um estudo de caso técnico-estratégico sobre a preparação do Sistema de Gerência de Certificados (SGC), utilizado no contexto da ICP-Brasil, para a adoção de assinaturas pós-quânticas. A partir da análise de uma ICP nacional regulada, mostramos que a transição para criptografia pós-quântica não pode ser tratada apenas como substituição por novos algoritmos. A migração afeta certificados, LCRs, HSMs, dispositivos criptográficos, políticas de certificação, processos de homologação e aplicações que dependem da cadeia de confiança. O desenvolvimento começou antes da padronização final dos algoritmos pós-quânticos, exigindo decisões baseadas em versões ainda em análise. Além disso, limitações legais da ICP-Brasil, padrões fixos de certificado e infraestrutura legada dificultam a adoção de novas abordagens criptográficas, especialmente no que diz respeito ao tamanho das chaves e ao desempenho dos algoritmos.

Os principais desafios identificados estão associados à operação da infraestrutura, e não apenas às propriedades matemáticas dos algoritmos. HSMs precisam oferecer suporte estável e homologável aos novos algoritmos; serviços de carimbo do tempo podem ser utilizados para preservar confiança e validade temporal em cenários de ruptura criptográfica; smartcards e tokens podem impor limitações de armazenamento e processamento; e normas técnicas precisam evoluir para permitir novos perfis de certificados e procedimentos de auditoria.

Como contribuição, este trabalho documenta requisitos, decisões de escopo e impactos práticos envolvidos na preparação de uma ICP nacional regulada para assinaturas pós-quânticas. Ao discutir o caso do SGC/ICP-Brasil, o artigo oferece subsídios para outras infraestruturas de certificação digital que precisem planejar migrações pós-quânticas sob restrições de continuidade operacional, interoperabilidade e conformidade normativa.

## Referências

Adkins, H. and Schmieg, S. (2026). Quantum Frontiers May Be Closer Than They Appear. Google Blog, https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/. [Accessed 28-05-2026].

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., and Zimmermann, P. (2015). Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*, pages 5–17. ACM.

AlFardan, N., Bernstein, D. J., Paterson, K. G., Poettering, B., and Schuldt, J. C. N. (2013). On the security of RC4 in TLS. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 305–320, Washington, D.C. USENIX Association.

Alnahawi, N., Schmitt, N., Wiesmaier, A., Heinemann, A., and Grasmeyer, T. (2023). On the state of crypto-agility. Cryptology ePrint Archive, Paper 2023/487.

Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, W., Housley, R., Turner, S., Barker, W., and Kent, K. (2025). Considerations for Achieving Crypto Agility: Strategies and Practices. NIST Cybersecurity White Paper 39, https://doi.org/10.6028/NIST.CSWP.39. [Accessed 28-05-2026].

Bernstein, D. J. and Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671):188–194.

Brasil (2001). Medida provisória nº 2200-2, de 24 de agosto de 2001. *Diário Oficial [da] República Federativa do Brasil*.

De Feo, L., Kohel, D., Leroux, A., Petit, C., and Wesolowski, B. (2020). Sqisign: Compact post-quantum signatures from quaternions and isogenies. In Moriai, S. and Wang, H., editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham. Springer International Publishing.

Heninger, N., Durumeric, Z., Wustrow, E., and Halderman, J. A. (2012). Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Security Symposium (USENIX Security 12)*. USENIX Association.

Housley, R., Polk, W., Turner, S., and Polk, T. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. Internet Engineering Task Force (IETF).

Instituto Nacional de Tecnologia da Informação (2024). gov.br. https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais/Resolucao192_DOCICP01_compilada.pdf. [Accessed 14-07-2025].

Instituto Nacional de Tecnologia da Informação (ITI) (2026). Instrução normativa ITI nº 35, de 30 de janeiro de 2026. Diário Oficial da União, Brasília, DF. Acessado em: 5 de agosto de 2026.

Kotzias, P., Razaghpanah, A., Amann, J., Paterson, K. G., Vallina-Rodriguez, N., and Caballero, J. (2018). Coming of age: A longitudinal study of TLS deployment. In

*Proceedings of the 2018 Internet Measurement Conference (IMC '18)*, Boston, MA, USA. ACM.

Moody, D., Perlner, R., Regenscheid, A., Robinson, A., and Cooper, D. (2024). Transition to post-quantum cryptography standards. Technical report, National Institute of Standards and Technology.

National Institute of Standards and Technology (2022). NIST Transitioning Away from SHA-1 for All Applications. https://www.nist.gov/news-events/news/2022/12/nist-transitioning-away-sha-1-all-applications. [Accessed 28-05-2026].

Nelson, D. B. (2011). Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS). RFC 6421.

NIST (2024a). Module-lattice-based digital signature standard. https://doi.org/10.6028/NIST.FIPS.204. [Accessed 14-07-2025].

NIST (2024b). Module-lattice-based key-encapsulation mechanism standard. https://doi.org/10.6028/NIST.FIPS.203. [Accessed 14-07-2025].

NIST (2024c). Stateless hash-based digital signature standard. https://doi.org/10.6028/NIST.FIPS.205. [Accessed 14-07-2025].

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.

Vakarjuk, J., Snetkov, N., and Laud, P. (2024). Identifying obstacles of pqc migration in e-estonia. In *2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon)*, pages 63–81.

Weise, J. (2001). Public key infrastructure overview. *Sun BluePrints OnLine, August*, pages 1–27.