Desafios e Estratégias para a Inclusão de Algoritmos Pós-Quânticos na ICP-Brasil

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. *The article discusses the challenges and strategies for adapting certificate management software used in ICP-Brasil to post-quantum cryptography, in light of the threat posed by quantum algorithms such as Shor's, which compromise the security of current systems. It presents a practical study on updating the Certificate Management System (SGC) to support post-quantum algorithms, highlighting regulatory difficulties. The work details the project phases, from research and training to integration and testing with HSMs. Finally, it underscores the importance of crypto agility and the need for interoperability tests and studies on smartcards to ensure the secure continuity of ICP-Brasil in the post-quantum scenario.*

Resumo. *Este trabalho discute os desafios e estratégias para adaptar softwares de gerência de certificados utilizados na ICP-Brasil à criptografia pós-quântica, frente à ameaça imposta por algoritmos quânticos como o de Shor, que comprometem a segurança dos sistemas atuais. É apresentado um estudo prático da atualização do Sistema de Gerência de Certificados (SGC) para suportar algoritmos pós-quânticos, destacando dificuldades regulatórias. O trabalho detalha fases do projeto, desde pesquisa e capacitação até integração e testes com HSMs. Por fim, é comentado sobre a importância da agilidade criptográfica e a necessidade de testes de interoperabilidade e estudos sobre smartcards para garantir a continuidade segura da ICP-Brasil no cenário pós-quântico.*

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 visão prática sobre os desafios enfrentados e as estratégias adotadas na adaptação de um software integrante da ICP-Brasil para suportar algoritmos criptográficos pós-quânticos. O trabalho busca contribuir com a comunidade ao documentar obstáculos técnicos, decisões de projeto e caminhos possíveis para modernizar cadeias de certificação em ambientes regulamentados.

1.1. Organização

Este artigo está organizado da seguinte forma: a Seção 2 apresenta os fundamentos teóricos, incluindo um panorama da ICP-Brasil e dos algoritmos pós-quânticos. A Seção 3 descreve os principais desafios enfrentados. A Seção 4 detalha as estratégias técnicas adotadas para a atualização do sistema. A Seção 5 discute os trabalhos que devem ser realizados no futuro. Por fim, a Seção 6 apresenta as conclusões do estudo.

2. Fundamentação Teórica

Esta seção apresenta os conceitos fundamentais necessários para o entendimento do trabalho desenvolvido. São abordados os princípios de uma Infraestrutura de Chaves Públicas (ICP), fundamentos de criptografia pós-quântica e a apresentação do software de gerência de certificados.

2.1. Infraestrutura de Chaves Públicas (ICP)

A infraestrutura de chaves públicas (ICP) é um conjunto de políticas, procedimentos e componentes tecnológicos destinados a gerenciar certificados digitais e chaves criptográficas. De acordo com Weise [Weise 2001], trata-se de um "conjunto de hardware, software e pessoas, para manusear, armazenar e distribuir certificados digitais".

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-se de 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 (Intituto 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. Sistema de Gerência de Certificados (SGC)

O Sistema de Gerência de Certificados (SGC) é um conjunto de *softwares* utilizados para gerenciar a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). O sistema está presente desde o princípio da ICP-Brasil e é fruto de uma parceria de longa data entre a Universidade Federal de Santa Catarina (UFSC) e o Instituto Nacional de Tecnologia da Informação (ITI), por meio do projeto João-de-Barro. Os *softwares* que compõem o SGC são responsáveis por gerenciar todo o ciclo de vida dos certificados digitais, sejam eles certificados da autoridade certificadora Raiz, intermediária ou final. Esse ciclo de vida abrange desde a emissão da requisição, passando pela emissão do certificado, até sua expiração ou revogação. Além disso, o SGC também é responsável pela administração dos operadores que compõem as autoridades certificadoras [tiinside.com.br 2007]. O sistema também passou a ser utilizado, a partir de setembro 2020, nas Assinaturas Eletrônicas Avançadas na plataforma Gov.br, onde opera uma infraestrutura própria referenciada como ICP-GOV, paralela à cadeia da ICP-Brasil [Brasil 2020].

2.3. Criptografia Pós-Quântica

A criptografia pós-quântica é um campo da criptografia que estuda algoritmos resistentes às potenciais adversidades do advento quântico. 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). O algoritmo de Shor, em especial, é capaz de fatorar inteiros e resolver o problema do logaritmo discreto em tempo polinomial em computadores quânticos. Essa característica causa a quebra dos sistemas de chave pública, os quais sustentam grande parte da infraestrutura digital, incluindo a ICP-Brasil.

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.

2.4. Algoritmos Pós-Quânticos

Os algoritmos pós-quânticos fundamentam-se em problemas matemáticos considerados intratáveis mesmo por computadores quânticos. As principais famílias de algoritmos incluem aquelas baseadas em reticulados (*lattices*), como os esquemas Kyber e Dilithium que se apoiam nos problemas LWE (*Learning With Errors*) e SIS (*Short Integer Solution*); criptografia multivariada, que teve como proponente o algoritmo Rainbow (recentemente quebrado), baseado na resolução de sistemas de equações polinomiais; esquemas baseados em funções hash, como o SPHINCS+ para assinaturas digitais; e criptografia baseada em isogenias de curvas elípticas, cujo principal representante, SIKE, também foi quebrado.

No processo de padronização do NIST, algoritmos oriundos dessas famílias foram selecionados, sendo que o **ML-KEM (Kyber)** foi padronizado pela FIPS 203 para encapsulamento de chaves [NIST 2024b]. Para assinaturas digitais, foram padronizados o **ML-DSA (Dilithium)**, baseado em reticulados e formalizado na FIPS

204 [NIST 2024a], e o **SLH-DSA (SPHINCS+)**, baseado em funções hash e padronizado pela FIPS 205 [NIST 2024c].

3. Desafios

Um dos principais desafios enfrentados no processo de adaptação do SGC 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 realizados 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.

Além disso, o próprio NIST emitiu alertas importantes sobre o tempo de vida restante de algoritmos clássicos como o RSA. Em sua comunicação, a recomendação foi de que sistemas críticos que dependem de criptografia de chave pública devem considerar a migração para algoritmos resistentes à computação quântica com urgência. Isso tornou 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 [Moody et al. 2024].

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. Estratégias de Migração e Adaptação

A estratégia de migração dos SGCs da ICP-Brasils 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. Nesta 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.

4.1. 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 Open Quantum Safe (OQS)[2].

4.2. Fase 2: Análise de Dependências e Inventário Criptográfico

Uma análise sistêmica identificou os pontos de maior impacto da migração. Considerando que os SGCs utilizam *Hardware Security Modules* (HSMs) para armazenamento seguro e operações criptográficas, a atualização destes módulos surgiu como um pré-requisito crítico. Esta 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. Esta 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: Foco da migração em algoritmos de assinatura digital; E desconsiderar, neste momento, implementações híbridas que combinam criptografia clássica e pós-quântica, focando apenas na abordagem totalmente PQC.

4.3. 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.

4.4. Fase 4: Estado Atual e Próximos Passos: O Ciclo da Agilidade Criptográfica

A recente conclusão do processo de padronização do NIST, com a publicação dos padrões FIPS 203, 204 e 205, impõe 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 será

[1] `https://www.bouncycastle.org/`
[2] `https://openquantumsafe.org/`
[3] `https://kryptus.com/`

reiniciado, reforçando a importância da agilidade criptográfica como pilar estratégico do projeto. A experiência prévia dos SGCs com a 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.

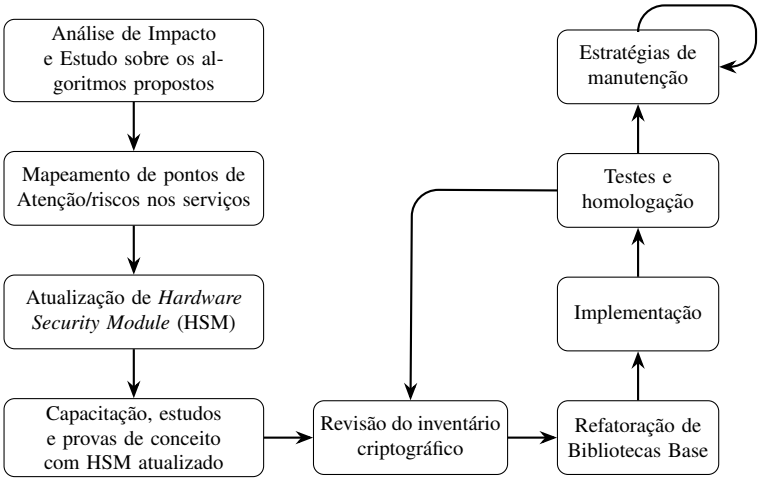

Figura 1. Fluxograma de estratégia para migração pós-quântica.

5. Trabalhos Futuros

Como próximos passos, destaca-se a necessidade de conduzir testes de interoperabilidade entre os componentes da ICP-Brasil e os novos algoritmos criptográficos pós-quânticos adotados. Assim como simular cenários reais de emissão, validação e revogação de certificados com algoritmos pós-quânticos é essencial para garantir que a adoção tecnológica não comprometa o ecossistema. Algoritmos como ML-DSA e ML-KEM, introduzem aumentos significativos no tamanho das chaves públicas e no tempo de execução, é preciso realizar *benchmarks* de desempenho do sistema e um estudo de técnicas de otimização.

É necessário analisar à viabilidade do uso de *smartcards* em um cenário com algoritmos pós-quânticos. Esses dispositivos ocupam papel central nos SGCs, porém, potencialmente, não suportarão processamento de algorítimos PQC [Vakarjuk et al. 2024]. Por fim é necessário um estudo mais aprofundado sobre estratégias de adaptação é essencial para viabilizar a adoção completa de criptografia pós-quântica em ambientes com *tokens* criptográficos certificados.

6. Conclusão

Este artigo apresentou os esforços em curso para adaptar o Sistema de Gerência de Certificados (SGC), utilizado na ICP-Brasil, à realidade da criptografia pós-quântica. Como contribuição principal, discutimos o processo de suporte a novos algoritmos indicados pelo NIST, dentro de um contexto institucional rígido, como o da ICP-Brasil. 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, como a exigência de uso de smartcards, padrões fixos de certificado e infraestrutura legada, dificultam a adoção de novas abordagens criptográficas, especialmente no que diz respeito ao tamanho das chaves e desempenho dos algoritmos.

Questões ainda em aberto incluem a definição de procedimentos para auditoria e homologação de módulos que utilizem criptografia pós-quântica. Como próximos passos, destaca-se a necessidade de realizar testes de interoperabilidade entre as ACs, estudar o impacto da nova criptografia em dispositivos como smartcards e tokens, além de acompanhar os desdobramentos internacionais no processo de padronização. A adoção consciente desses novos algoritmos é fundamental para garantir a continuidade e a segurança da ICP-Brasil em um cenário pós-quântico.

Referências

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

Brasil (2020). Lei nº 14063/2020, de 23 de setembro de 2020. *Diário Oficial [da] República Federativa do Brasil*.

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].

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.

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.

tiinside.com.br (2007). ITI launches new phase of crypto platform — tiinside.com.br. `https://tiinside.com.br/en/22/08/2007/iti-inicia-nova-fase-da-plataforma-criptografica/`. [Accessed 14-07-2025].

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.