UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA DE MODELO DE AVALIAÇÃO DE MATURIDADE PARA PREPARAÇÃO À TRANSIÇÃO CRIPTOGRÁFICA PÓS-QUÂNTICA EM OPERADORAS DE TELECOMUNICAÇÕES BRASILEIRAS

LUIZ RICARDO FREITAS DE ABREU

ORIENTADOR: DR. LAERTE PEOTTA DE MELO
TRABALHO DE CONCLUSÃO DE CURSO DE ESPECIALIZAÇÃO
LATO SENSU EM ENGENHARIA ELÉTRICA

BRASÍLIA/DF JUNHO/2026

RESUMO

A computação quântica desafia organizações que dependem de criptografia de chave pública, sobretudo em infraestruturas críticas. Em telecomunicações, a criptografia sustenta certificados digitais, protocolos seguros, VPNs, autenticação de rede, sistemas operacionais, nuvem, equipamentos de clientes e relações com fornecedores. Algoritmos como RSA, Diffie-Hellman e curvas elípticas podem ser comprometidos por computadores quânticos criptograficamente relevantes, o que exige preparação antecipada para a transição à criptografia pós-quântica (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024a, 2024b, 2024c; EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE, 2023; GSM ASSOCIATION, 2024). Este trabalho propõe o MAT-CRIPTO-BR, um modelo preliminar de maturidade para apoiar operadoras brasileiras de telecomunicações nesse planejamento. A pesquisa é aplicada, exploratória e qualitativa, com construção de artefato inspirada em Design Science Research, revisão bibliográfica e documental, análise comparativa de modelos e demonstração conceitual com dados simulados (HEVNER et al., 2004; PEFFERS et al., 2007). O modelo organiza a avaliação em oito dimensões, vinte e seis indicadores, quatro níveis de maturidade, Índice Composto de Maturidade e Índice de Prioridade de Migração Pós-Quântica. Conclui-se que o MAT-CRIPTO-BR pode apoiar o diagnóstico inicial, a priorização de ações e a estruturação de evidências, embora ainda exija validação empírica.

Palavras-chave: criptografia pós-quântica; criptoagilidade; maturidade cibernética; telecomunicações; transição criptográfica.

ABSTRACT

Quantum computing challenges organizations that rely on public-key cryptography, especially in critical infrastructures. In telecommunications, cryptography underpins digital certificates, secure protocols, VPNs, network authentication, operating systems, cloud environments, customer equipment, and supplier relationships. Algorithms such as RSA, Diffie-Hellman, and elliptic curve cryptography may be compromised by cryptographically relevant quantum computers, which requires early preparation for the transition to post-quantum cryptography (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024a, 2024b, 2024c; EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE, 2023; GSM ASSOCIATION, 2024). This study proposes MAT-CRIPTO-BR, a preliminary maturity model to support Brazilian telecommunications operators in this planning. The research is applied, exploratory, and qualitative, with artifact construction inspired by Design Science Research, bibliographic and documentary review, comparative analysis of models, and conceptual demonstration using simulated data (HEVNER et al., 2004; PEFFERS et al., 2007). The model organizes the assessment into eight dimensions, twenty-six indicators, four maturity levels, a Composite Maturity Index, and a Post-Quantum Migration Priority Index. It is concluded that MAT-CRIPTO-BR can support initial diagnosis, action prioritization, and evidence structuring, although it still requires empirical validation.
Keywords: post-quantum cryptography; cryptoagility; cyber maturity; telecommunications; cryptographic transition.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

Não há figuras no corpo principal desta versão.

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

3GPP 3rd Generation Partnership Project

ABIN Agência Brasileira de Inteligência

AHP Analytic Hierarchy Process

AIVD Algemene Inlichtingen- en Veiligheidsdienst

Anatel Agência Nacional de Telecomunicações

CAMM Cryptographic Asset Management Maturity (conforme referência adotada neste trabalho)

CBOM Cryptographic Bill of Materials

CEPESC Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações

CMMI Capability Maturity Model Integration

CNCiber Comitê Nacional de Cibersegurança

COBIT Control Objectives for Information and Related Technology

COBR Fator de conformidade obrigatória

CRQC Computador Quântico Criptograficamente Relevante (Cryptographically Relevant Quantum Computer)

CRYSTALS-Kyber Cryptographic Suite for Algebraic Lattices - Kyber

CWI Centrum Wiskunde & Informatica

C2M2 Cybersecurity Capability Maturity Model

DSR Design Science Research

E-Ciber Estratégia Nacional de Cibersegurança

ECC Elliptic Curve Cryptography

ENSIC Estratégia Nacional de Segurança de Infraestruturas Críticas

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standards

GSMA GSM Association

GSI/PR Gabinete de Segurança Institucional da Presidência da República

HNDL Harvest Now, Decrypt Later

HSM Hardware Security Module

ICM Índice Composto de Maturidade

ICP-Brasil Infraestrutura de Chaves Públicas Brasileira

IPM-PQC Índice de Prioridade de Migração Pós-Quântica

ITI Instituto Nacional de Tecnologia da Informação

LGPD Lei Geral de Proteção de Dados Pessoais

LTE Long Term Evolution

MIL Maturity Indicator Level

ML-DSA Module-Lattice-Based Digital Signature Algorithm

ML-KEM Module-Lattice-Based Key-Encapsulation Mechanism

NIST National Institute of Standards and Technology

OSS/BSS Operations Support Systems / Business Support Systems

PKI Public Key Infrastructure

PLANSIC Plano Nacional de Segurança de Infraestruturas Críticas

PNCiber Política Nacional de Cibersegurança

PNSIC Política Nacional de Segurança de Infraestruturas Críticas

PQC Post-Quantum Cryptography

PPSI Programa de Privacidade e Segurança da Informação

Qev Fator de qualidade das evidências (variável do modelo)

R-Ciber Regulamento de Segurança Cibernética

SD-WAN Software-Defined Wide Area Network

SGD/MGI Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos

SIM Subscriber Identity Module

SISP Sistema de Administração dos Recursos de Tecnologia da Informação

SLH-DSA Stateless Hash-Based Digital Signature Algorithm

SmartVPN Serviço de rede privada virtual citado no white paper da SoftBank/SandboxAQ

TLS Transport Layer Security

TNO Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek

VPN Virtual Private Network

Σ Somatório

Pi Peso da dimensão i

MILi Nível médio normalizado da dimensão i

1 INTRODUÇÃO

A computação quântica representa desafio relevante para organizações que utilizam criptografia de chave pública. Algoritmos como RSA, Diffie-Hellman e curvas elípticas podem ser comprometidos por computadores quânticos criptograficamente relevantes, capazes de explorar algoritmos quânticos aplicáveis à fatoração de inteiros e ao problema do logaritmo discreto (SHOR, 1994; MOSCA, 2018). Embora a disponibilidade prática desses computadores ainda seja incerta, a preparação deve ser antecipada, especialmente em ambientes com ciclos longos de substituição tecnológica.

No setor de telecomunicações, a transição criptográfica envolve certificados digitais, protocolos seguros, redes privadas virtuais, autenticação de elementos de rede, sistemas OSS/BSS, nuvem, equipamentos de clientes e relações com fornecedores. Essa interdependência torna a migração para algoritmos resistentes a ataques quânticos um desafio técnico, organizacional, operacional e regulatório (EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE, 2023; GSM ASSOCIATION, 2024).

A publicação dos padrões FIPS 203, FIPS 204 e FIPS 205 pelo National Institute of Standards and Technology estabeleceu base técnica para o início da transição pós-quântica (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024a, 2024b, 2024c). Ainda assim, algoritmos padronizados não resolvem, por si sós, desafios de inventário criptográfico, priorização de ativos, gestão de risco, dependência de fornecedores e governança.

A literatura técnica e setorial indica que a transição tende a ser gradual, com inventário criptográfico, pilotos controlados, mecanismos híbridos, coordenação com fornecedores e monitoramento contínuo (3RD GENERATION PARTNERSHIP PROJECT, 2024; DEMIR; BILGIN; ONBASLI, 2025; GSM ASSOCIATION, 2024). Isso reforça que a preparação pós-quântica deve ser tratada como processo de maturidade institucional, e não como substituição pontual de algoritmo.

No contexto brasileiro, operadoras de telecomunicações estão sujeitas a requisitos de segurança cibernética, gestão de riscos, continuidade de negócios e conformidade, especialmente no Regulamento de Segurança Cibernética da Anatel (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2024). Além disso, o Programa de Privacidade e Segurança da Informação constitui referência indireta de maturidade para organizações que prestam serviços, processam dados ou integram soluções críticas utilizadas pela administração pública federal (SECRETARIA DE GOVERNO DIGITAL, 2025). Contudo, esses instrumentos não oferecem

modelo específico para avaliar a maturidade da preparação à transição criptográfica pós-quântica.

Diante dessa lacuna, este trabalho propõe o MAT-CRIPTO-BR, modelo preliminar de avaliação de maturidade para apoiar operadoras brasileiras de telecomunicações na preparação para a transição criptográfica pós-quântica. A proposta concentra-se na construção conceitual do artefato, na definição de dimensões, indicadores e mecanismos de pontuação e em demonstração com dados simulados. A validação empírica com especialistas e operadoras reais é etapa futura.

1.1 PROBLEMA DE PESQUISA

Esta subseção delimita a pergunta central que orienta a construção do modelo, convertendo a necessidade de preparação pós-quântica em desafio avaliável, mensurável e aderente ao contexto das operadoras brasileiras de telecomunicações.

Como avaliar, de forma estruturada e mensurável, a maturidade de operadoras brasileiras de telecomunicações na preparação para a transição criptográfica pós-quântica, considerando dimensões técnicas, organizacionais e regulatórias aplicáveis ao contexto nacional?

1.2 OBJETIVO GERAL

Esta subseção apresenta o objetivo geral da pesquisa, formulado para manter o escopo compatível com um TCC de especialização lato sensu e centrado na proposição conceitual do modelo, não em sua validação empírica.

Propor o MAT-CRIPTO-BR como modelo preliminar de avaliação de maturidade para apoiar operadoras brasileiras de telecomunicações na preparação para a transição criptográfica pós-quântica, integrando dimensões técnicas, organizacionais e regulatórias aplicáveis ao contexto nacional.

1.3 OBJETIVOS ESPECÍFICOS

Esta subseção desdobra o objetivo geral em etapas operacionais de pesquisa, indicando o percurso de fundamentação, construção, demonstração e delimitação do MAT-CRIPTO-BR.

1. Revisar conceitos essenciais sobre computação quântica, ameaça criptográfica, criptografia pós-quântica, criptoagilidade e modelos de maturidade aplicáveis à segurança cibernética.
2. Analisar requisitos técnicos e regulatórios relevantes para a transição criptográfica em operadoras brasileiras de telecomunicações.

3. Definir as dimensões, indicadores e escala de maturidade do MAT-CRIPTO-BR.
4. Propor mecanismos de pontuação e priorização, incluindo o Índice Composto de Maturidade e o Índice de Prioridade de Migração Pós-Quântica.
5. Demonstrar conceitualmente a aplicação do modelo por meio de cenário simulado.
6. Indicar limitações da proposta e caminhos para validação empírica futura.

1.4 JUSTIFICATIVA, DELIMITAÇÃO E ORGANIZAÇÃO

A transição para criptografia pós-quântica é estratégica para infraestruturas críticas porque dados cifrados hoje podem manter valor no futuro, criando risco de "colheita agora, decifra depois" (MOSCA, 2018; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024d). Em telecomunicações, a substituição de algoritmos envolve redes, sistemas legados, fornecedores, governança, continuidade operacional e conformidade.

A justificativa prática do estudo decorre da necessidade de converter recomendações técnicas e regulatórias em critérios verificáveis de maturidade. Inventário, priorização, criptoagilidade, governança, capacitação e gestão de fornecedores aparecem de forma recorrente como capacidades necessárias para uma transição sem ruptura operacional (BERNSTEIN et al., 2023; DEMIR; BILGIN; ONBASLI, 2025; GSM ASSOCIATION, 2024).

O estudo limita-se à proposição conceitual de um modelo preliminar para operadoras brasileiras de telecomunicações. Não abrange implementação de algoritmos pós-quânticos, testes de desempenho, avaliação empírica, construção de baseline setorial ou validação estatística, que ficam para pesquisas futuras.

O trabalho está organizado em seis capítulos: introdução, fundamentação teórica, metodologia, proposta do MAT-CRIPTO-BR, demonstração conceitual e discussão, e conclusão. Referências e apêndices reúnem materiais complementares e instrumentos preliminares para validação futura.

2 FUNDAMENTAÇÃO TEÓRICA E CONTEXTO DO PROBLEMA

Este capítulo reúne os fundamentos técnicos, conceituais e regulatórios que sustentam a proposta do MAT-CRIPTO-BR. A fundamentação está organizada de modo a conectar a ameaça quântica, a criptografia pós-quântica, a criptoagilidade, os modelos de maturidade e o contexto brasileiro de telecomunicações.

2.1 COMPUTAÇÃO QUÂNTICA, AMEAÇA CRIPTOGRÁFICA E CRIPTOGRAFIA PÓS-QUÂNTICA

A computação quântica explora propriedades como superposição e entrelaçamento para realizar certos cálculos com eficiência potencialmente superior à dos computadores clássicos. Na criptografia, o principal risco é comprometer problemas matemáticos que sustentam criptossistemas de chave pública.

O algoritmo de Shor mostra que um computador quântico suficientemente poderoso pode fatorar inteiros grandes e resolver o problema do logaritmo discreto em tempo polinomial, comprometendo RSA, Diffie-Hellman e criptografia de curvas elípticas (SHOR, 1994). A criptografia pós-quântica reúne algoritmos projetados para resistir a ataques clássicos e quânticos conhecidos. Os padrões FIPS 203, 204 e 205 do NIST estabelecem algoritmos pós-quânticos para encapsulamento de chaves e assinaturas digitais (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024a, 2024b, 2024c).

Operacionalmente, a padronização dos algoritmos é necessária, mas insuficiente. As organizações precisam identificar onde algoritmos vulneráveis são usados, avaliar dados de longa duração, mapear dependências de fornecedores e planejar substituições com baixo impacto sobre disponibilidade, desempenho, interoperabilidade e conformidade.

2.2 CRIPTOAGILIDADE E INVENTÁRIO CRIPTOGRÁFICO

Criptoagilidade é a capacidade de identificar, substituir e atualizar mecanismos criptográficos de forma controlada, tempestiva e com baixo impacto operacional, conforme Hoffman (2017). Essa capacidade depende de inventário criptográfico, registro de algoritmos, protocolos, bibliotecas, certificados, chaves, aplicações, equipamentos, fornecedores e dependências associadas ao uso de criptografia.

A criptoagilidade não se resume à troca de algoritmo. Em ambientes de telecomunicações, ela exige arquitetura modular, processos de mudança controlada, ambientes de teste, governança de exceções, políticas de ciclo de vida criptográfico e integração com fornecedores de software, hardware, SIM cards, HSMs, plataformas de nuvem, equipamentos de rede e sistemas de suporte à operação (DEMIR; BILGIN; ONBASLI, 2025; GSM ASSOCIATION, 2024).

A literatura distingue diferentes formas de criptoagilidade, úteis para detalhar a dimensão técnica do modelo. A agilidade de migração refere-se à capacidade de substituir um algoritmo por outro de forma controlada; a agilidade de conformidade refere-se à capacidade de reconfigurar a infraestrutura criptográfica para atender simultaneamente a diferentes exigências

regulatórias; e a agilidade de implementação refere-se à capacidade de substituir a própria implementação de um algoritmo (AIVD; CWI; TNO, 2024). A agilidade de conformidade é particularmente pertinente ao contexto brasileiro, no qual operadoras precisam conciliar padrões internacionais com exigências da ICP-Brasil e da regulação setorial da Anatel, podendo demandar configurações criptográficas distintas operando de forma concomitante.

Para operadoras de telecomunicações, o inventário criptográfico é pré-requisito para qualquer estratégia de transição pós-quântica. Sem visibilidade sobre ativos vulneráveis, dados de longa duração, conexões expostas e dependências externas, a organização não consegue priorizar adequadamente a migração. Nesse sentido, a noção de CBOM contribui ao tornar explícitos componentes, bibliotecas, algoritmos e dependências criptográficas, permitindo rastreabilidade e atualização contínua (BERNSTEIN et al., 2023).

Em termos práticos, o CBOM tem sido materializado como formato legível por máquina derivado do padrão CycloneDX de Software Bill of Materials, com suporte específico a ativos criptográficos a partir da versão 1.6 (AIVD; CWI; TNO, 2024). O formato permite registrar protocolos, algoritmos, chaves e certificados, com metadados como nível de segurança, parâmetros e dependências entre componentes. Cabe ressalvar, contudo, suas limitações: ferramentas de varredura nem sempre preenchem todos os campos e o formato não captura procedimentos de gestão do ciclo de vida de chaves, o que reforça a complementaridade entre as dimensões D2 e D5 do modelo proposto.

2.3 MODELOS DE MATURIDADE APLICÁVEIS À SEGURANÇA CIBERNÉTICA

Modelos de maturidade avaliam o grau de institucionalização de processos, capacidades e práticas. Em segurança cibernética, permitem diagnosticar lacunas, estabelecer metas e orientar melhorias. Para este trabalho, eles oferecem base conceitual para transformar a preparação pós-quântica em dimensões, indicadores, níveis e evidências. A Tabela 2.1 sintetiza as contribuições e limitações dos modelos de referência examinados, incluindo CMMI, C2M2, COBIT, ISO/IEC 21827, CAMM e modelos específicos de migração ou prontidão pós-quântica (CMMI INSTITUTE, 2018; U.S. DEPARTMENT OF ENERGY, 2022; ISACA, 2019; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2008; BERNSTEIN et al., 2023; AIVD; CWI; TNO, 2024; KONG; JANSSEN; BHAROSA, 2024).

Tabela 2.1 - Contribuições e limitações de modelos de referência para o MAT-CRIPTO-BR

Modelo	Contribuição	Limitação
CMMI	Evolução de processos e institucionalização	Não é específico para cibersegurança, criptografia ou telecom
C2M2	Maturidade em cibersegurança e escala MIL 0-3	Não trata especificamente de PQC nem do contexto brasileiro
COBIT	Governança, risco e controles de TI	Foco amplo em governança de TI
ISO/IEC 21827	Processos de engenharia de segurança	Não aborda PQC ou telecom
CAMM	Gestão de ativos criptográficos	Não contempla integralmente regulação brasileira e telecom
Modelo de Prontidão Organizacional QS (KONG; JANSSEN; BHAROSA, 2024)	Modelo de maturidade específico de PQC, com oito dimensões e cinco níveis de prontidão organizacional	Foco em ecossistema e PKI pública; não adaptado ao setor de telecom nem à regulação brasileira
PQC Migration Handbook (AIVD; CWI; TNO, 2024)	Abordagem faseada de migração (diagnóstico, inventário/CBOM, planejamento e execução), escore de risco quântico e personas de adoção	Guia de migração, não escala de maturidade por níveis; contexto regulatório europeu, não brasileiro

Fonte: Elaborado pelo autor.

O C2M2 é referência estrutural por sua aplicação a setores críticos e por utilizar escala MIL 0-3 (U.S. DEPARTMENT OF ENERGY, 2022). O CAMM é relevante por tratar de ativos criptográficos (BERNSTEIN et al., 2023). Nenhum dos modelos, contudo, atende simultaneamente a foco pós-quântico, mensuração por indicadores, adaptação ao setor brasileiro de telecomunicações e aderência regulatória nacional.

Mais próximos do escopo pós-quântico, dois esforços recentes merecem destaque. O PQC Migration Handbook, publicado pelas agências holandesas AIVD, CWI e TNO, estrutura a transição em etapas de diagnóstico de vulnerabilidade quântica, inventário criptográfico, planejamento e execução, incorporando escore de risco quântico, personas de adoção e orientação sobre criptoagilidade (AIVD; CWI; TNO, 2024). Trata-se, todavia, de guia de migração, e não de escala de maturidade organizada por níveis. Por sua vez, o Modelo de Prontidão Organizacional para Transição Quantum-Safe organiza a preparação em oito dimensões — colaboração, governança, política e regulação, conscientização, padrões de soluções quantum-safe, soluções híbridas, estratégias de criptoagilidade e conhecimento sobre a transição — cada uma com cinco níveis de prontidão (KONG; JANSSEN; BHAROSA, 2024). Esse modelo é o antecedente mais próximo da proposta deste trabalho, por ser especificamente voltado à transição pós-quântica e por adotar estrutura dimensional com escala de maturidade.

A convergência estrutural entre esses esforços e a proposta deste trabalho — organização em dimensões, escala de níveis e escore de risco multifatorial — valida as escolhas metodológicas adotadas. A contribuição original do MAT-CRIPTO-BR reside, portanto, não na criação de uma estrutura inédita de maturidade, mas em sua adaptação ao setor de telecomunicações e à realidade regulatória brasileira: ancorar as dimensões em obrigações da Anatel e da ICP-Brasil, incorporar mecanismos próprios de pontuação (ICM e IPM-PQC) e refletir as dependências típicas de operadoras, como fornecedores de equipamentos de rede, sistemas legados de suporte à operação e infraestrutura de chaves públicas. Nenhum dos

modelos internacionais examinados foi concebido para o setor de telecom brasileiro, o que delimita a lacuna que este trabalho busca preencher.

Além da ausência de foco específico em PQC, modelos genéricos de maturidade podem apresentar limitações de aplicabilidade prática quando empregados em ambientes heterogêneos, com tecnologias legadas, múltiplos fornecedores e diferentes níveis de capacidade organizacional. Revisões recentes sobre modelos de capacidade em cibersegurança apontam desafios de personalização, complexidade de autoavaliação, baixa conscientização organizacional e dificuldade de tradução dos resultados em ações de melhoria (LIYANAGE; ARACHCHILAGE; RUSSELLO, 2024).

2.4 TELECOMUNICAÇÕES COMO INFRAESTRUTURA CRÍTICA E RISCO QUÂNTICO

Redes de telecomunicações sustentam serviços públicos, atividades econômicas, comunicações governamentais, operações de emergência e infraestrutura digital. Seus componentes criptograficamente relevantes incluem certificados, interfaces de rede, sistemas de autenticação, túneis seguros, plataformas de gerenciamento, OSS/BSS, PKI, ambientes virtualizados, conexões com fornecedores e equipamentos de clientes. A gestão de risco quântico envolve identificar ativos vulneráveis, avaliar criticidade, exposição, vida útil da informação, dificuldade de substituição e dependências externas (EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE, 2023; GSM ASSOCIATION, 2024).

No contexto de 4G, 5G e evolução para 5G-Advanced e 6G, a transição criptográfica pode envolver redes de acesso, núcleo de rede, autenticação, interfaces de gerenciamento, sistemas de orquestração, APIs, redes privadas, funções virtualizadas e elementos de confiança digital. Orientações setoriais indicam que mecanismos híbridos, pilotos controlados e coordenação com organismos de padronização e fornecedores tendem a reduzir riscos de incompatibilidade durante a migração (3RD GENERATION PARTNERSHIP PROJECT, 2024; DEMIR; BILGIN; ONBASLI, 2025).

2.4.1 Evidências de Aplicação Real em Operadoras

Esta seção apresenta evidências documentais de aplicação ou experimentação de criptografia pós-quântica em operadoras de telecomunicações. Os casos selecionados não têm a finalidade de validar empiricamente o MAT-CRIPTO-BR, mas de demonstrar que as dimensões propostas no modelo correspondem a iniciativas já observáveis no setor. As evidências analisadas

derivam de comunicados institucionais, white papers técnicos e fonte jornalística especializada, razão pela qual devem ser interpretadas como indícios de movimento setorial, e não como resultados auditados de forma independente.

No Japão, a SoftBank, em parceria com a SandboxAQ, realizou prova de conceito de criptografia híbrida, combinando algoritmos clássicos, representados por criptografia de curvas elípticas, com algoritmos de criptografia pós-quântica. A iniciativa utilizou tráfego simulado entre handsets e servidores, avaliando métricas como latência, carga de CPU, uso de memória, taxa de conexão e volume de tráfego. Os resultados indicaram viabilidade prática da abordagem híbrida e impacto limitado sobre redes existentes (SOFTBANK CORP.; SANDBOXAQ, 2023). Em publicação técnica posterior, a SoftBank e a SandboxAQ detalharam cenários de teste envolvendo 5G, LTE, SmartVPN e Wi-Fi, além de algoritmos pós-quânticos estruturados baseados em reticulados, como ML-KEM e ML-DSA. Os resultados apontaram desempenho comparável ao de métodos tradicionais em dimensões críticas, como latência de conexão, carga de CPU e confiabilidade (SOFTBANK CORP.; SANDBOXAQ, 2025). Esse caso pode ser associado à dimensão de criptoagilidade técnica (D4), pois evidencia a capacidade de testar, combinar e avaliar alternativas criptográficas em ambientes de rede heterogêneos.

Na Coreia do Sul, a SK Telecom, em parceria com a Thales, testou uma solução de criptografia pós-quântica em ambiente de rede 5G standalone. A solução utilizou cartões SIM 5G PQC da Thales e o algoritmo CRYSTALS-Kyber para proteger a identidade do assinante contra ameaças quânticas futuras, incluindo ataques do tipo “coletar agora, decifrar depois” (SK TELECOM, 2023). O caso ilustra a priorização de um ativo crítico específico, a identidade do assinante, e pode ser relacionado às dimensões de inventário criptográfico (D2) e avaliação de risco e priorização (D3).

Nos Estados Unidos, a AT&T afirmou, por meio de declaração reportada por Liu (2022), ter em seu roadmap tornar-se “quantum ready” até 2025. A condição de prontidão quântica, conforme relatado pela fonte, não equivaleria a estar plenamente protegida contra ameaças quânticas, mas a ter realizado diligência preparatória, definido caminhos de ação e identificado soluções potenciais. A mesma fonte informa que a empresa vinha identificando ativos criptográficos, avaliando soluções de criptografia pós-quântica e conduzindo testes. Esse caso pode ser interpretado como evidência de capacidades iniciais de governança e estratégia (D1) e de inventário criptográfico (D2).

Em 2026, a AT&T Business anunciou um serviço de SD-WAN com criptografia pós-quântica, desenvolvido com a Cisco e baseado no Cisco 8000 Series Secure Router (AT&T, 2026). Segundo a empresa, a oferta incorpora capacidades de criptografia, autenticação e secure boot

resistentes a ameaças quânticas e alinhadas a padrões do NIST. Essa iniciativa indica avanço da fase de preparação para uma etapa de implementação comercial. Contudo, não permite concluir que toda a infraestrutura da AT&T tenha sido migrada ou esteja plenamente "quantum secured".

Em conjunto, os casos indicam diferentes graus de maturidade na preparação pós-quântica. A SoftBank evidencia experimentação técnica e criptoagilidade; a SK Telecom demonstra priorização de ativo crítico em rede 5G; e a AT&T ilustra a transição entre planejamento, inventário e oferta comercial. Tais evidências reforçam a relevância prática das dimensões do MAT-CRIPTO-BR, mas não constituem validação empírica do instrumento, etapa que permanece como limitação e desdobramento futuro desta pesquisa.

2.5 CONTEXTO REGULATÓRIO BRASILEIRO E LACUNA DE PESQUISA

O Brasil possui arcabouço regulatório aplicável à cibersegurança, à proteção de dados pessoais, à segurança da informação, às infraestruturas críticas e à infraestrutura de chaves públicas. Até o recorte desta pesquisa, entretanto, não se identifica norma setorial específica que estabeleça roteiro, prazos ou métricas de maturidade para a transição criptográfica pós-quântica em operadoras brasileiras de telecomunicações. Esta seção apresenta o contexto normativo e institucional brasileiro e delimita a lacuna que fundamenta a proposta do MAT-CRIPTO-BR.

2.5.1 Regulação Setorial de Telecomunicações

O Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução Anatel nº 740/2020 e alterado pela Resolução Anatel nº 767/2024, estabelece condutas e procedimentos para promoção da segurança nas redes e serviços de telecomunicações, incluindo segurança cibernética e proteção das infraestruturas críticas de telecomunicações (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2020; 2024). O regulamento contempla diretrizes relacionadas à gestão de riscos, proteção de dados pessoais, cooperação entre agentes, segurança de fornecedores, tratamento de incidentes, avaliação de vulnerabilidades e proteção de infraestruturas críticas.

Embora a norma não trate especificamente da transição criptográfica pós-quântica, seus requisitos oferecem base regulatória para uma preparação estruturada. A identificação de infraestruturas críticas, a gestão de riscos, a avaliação de vulnerabilidades e o controle sobre fornecedores são elementos compatíveis com a construção de inventário criptográfico, análise de exposição e priorização de ativos. Nesse sentido, o MAT-CRIPTO-BR pode complementar

o regulamento setorial ao traduzir obrigações gerais de segurança cibernética em capacidades específicas de prontidão pós-quântica.

O Programa de Privacidade e Segurança da Informação (PPSI), atualizado pela Portaria SGD/MGI nº 9.511/2025, não constitui regulação setorial de telecomunicações. O programa aplica-se a órgãos e entidades da administração pública federal direta, autárquica e fundacional que possuem unidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Ainda assim, o PPSI 2.0 é relevante como referência nacional de maturidade em privacidade e segurança da informação, pois organiza controles e medidas em eixos como governança, maturidade, metodologia, pessoas e tecnologia (SECRETARIA DE GOVERNO DIGITAL, 2025).

A relevância do PPSI para o setor de telecomunicações é indireta. Ela se manifesta especialmente quando operadoras prestam serviços, processam dados ou integram soluções críticas utilizadas por órgãos públicos federais. Nesses casos, a existência de um programa governamental de maturidade em privacidade e segurança reforça a necessidade de instrumentos capazes de demonstrar controles, planos de evolução e critérios de priorização.

No âmbito da infraestrutura de chaves públicas, a Instrução Normativa ITI nº 35/2026 alterou o DOC-ICP-01.01 para acrescentar novos algoritmos criptográficos e certificados digitais, incluindo referências a algoritmos pós-quânticos como ML-DSA e ML-KEM no contexto da ICP-Brasil (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil), 2026). Essa alteração representa uma das evidências normativas brasileiras mais concretas de incorporação da criptografia pós-quântica. Seu escopo, entretanto, está relacionado à certificação digital e não estabelece, por si só, obrigação de migração criptográfica para redes de telecomunicações.

2.5.2 Proteção de Dados e Privacidade

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (BRASIL, 2018a). A LGPD não impõe, de forma geral, o uso de criptografia. Entretanto, a criptografia pode constituir medida técnica relevante para preservar confidencialidade, integridade e segurança de dados pessoais.

Operadoras de telecomunicações tratam dados pessoais de elevada relevância operacional, incluindo dados cadastrais, registros de chamadas, metadados, informações de localização, identificadores de rede e identidades de assinantes. Conforme o tratamento realizado, essas

organizações podem atuar como controladoras ou operadoras, nos termos da LGPD. A possibilidade de quebra futura de algoritmos criptográficos de chave pública por computadores quânticos criptograficamente relevantes cria risco específico para dados que devam permanecer confidenciais por longo período.

Nesse contexto, a preparação pós-quântica pode ser interpretada como componente prospectivo de conformidade com a LGPD. Essa preparação envolve identificar dados pessoais protegidos por criptografia vulnerável, estimar o período necessário de confidencialidade, mapear dependências criptográficas e priorizar a migração conforme risco e ciclo de vida dos dados. A ausência de orientação específica da LGPD ou da Autoridade Nacional de Proteção de Dados sobre criptografia pós-quântica, contudo, cria incerteza quanto a requisitos, prazos e critérios de suficiência.

2.5.3 Infraestruturas Críticas, Cibersegurança Nacional e Criptografia de Estado

As telecomunicações integram o contexto brasileiro de infraestruturas críticas em razão de sua importância para a continuidade de serviços essenciais, para a segurança do Estado e da sociedade e para o funcionamento de outros setores interdependentes. O Decreto nº 9.573/2018 aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC). Em seguida, o Decreto nº 10.569/2020 aprovou a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), e o Decreto nº 11.200/2022 aprovou o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC) (BRASIL, 2018b; 2020; 2022).

No campo da cibersegurança, o Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber) (BRASIL, 2023). Posteriormente, o Decreto nº 12.573/2025 instituiu a Estratégia Nacional de Cibersegurança (E-Ciber), consolidando diretrizes nacionais relacionadas à proteção de serviços essenciais, infraestruturas críticas, cooperação público-privada e soberania nacional (BRASIL, 2025a). Esse contexto indica tendência de fortalecimento da governança cibernética nacional, ainda que não estabeleça obrigação específica de transição pós-quântica para operadoras de telecomunicações.

Também se observa movimento institucional voltado à adoção de modelos de maturidade. A Resolução CNCiber nº 16/2025 instituiu grupo de trabalho temático para elaboração de modelos nacionais de maturidade em cibersegurança, incluindo modelo de avaliação nacional e modelo de avaliação institucional aplicável a instituições públicas ou privadas (COMITÊ NACIONAL DE CIBERSEGURANÇA, 2025). Essa iniciativa reforça a pertinência de instrumentos

estruturados de avaliação, como o MAT-CRIPTO-BR, especialmente em áreas de risco tecnológico emergente.

A Política Nacional de Segurança da Informação, instituída pelo Decreto nº 12.572/2025, também contribui para esse contexto. A norma estabelece diretrizes para governança da segurança da informação no âmbito da administração pública federal e atribui ao Gabinete de Segurança Institucional competências relacionadas à formulação de diretrizes, estratégias, planos, normativos e recomendações (BRASIL, 2025b). Embora seu escopo seja a administração pública federal, seus princípios de disponibilidade, integridade, confidencialidade e autenticidade dialogam diretamente com os desafios da transição criptográfica pós-quântica.

No âmbito da criptografia de Estado, a Agência Brasileira de Inteligência (ABIN), por meio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC), apresenta evidências públicas de atuação relacionada à criptografia pós-quântica. A ABIN informou o lançamento da biblioteca criptográfica Libharpia, composta por algoritmos pós-quânticos e utilizada no sistema eleitoral brasileiro (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2022; 2024). Essas evidências demonstram que a agenda pós-quântica já aparece em iniciativas brasileiras de criptografia de Estado. Contudo, elas não configuram roteiro público de migração pós-quântica para o setor de telecomunicações.

2.5.4 Marcos Regulatórios em Construção

O contexto brasileiro de cibersegurança encontra-se em processo de modernização normativa. Além da PNCiber, da E-Ciber, da Política Nacional de Segurança da Informação e das atualizações setoriais da Anatel, há discussões sobre uma Lei Geral de Cibersegurança, sobre governança nacional do tema e sobre requisitos mínimos para provedores e operadores de serviços essenciais e infraestruturas críticas. Resoluções e documentos do CNCiber indicam a criação de grupos de trabalho voltados a temas como maturidade, serviços essenciais, infraestruturas críticas e anteprojeto de lei geral de cibersegurança (COMITÊ NACIONAL DE CIBERSEGURANÇA, 2025).

Esses movimentos ainda não estabelecem obrigação específica de migração para criptografia pós-quântica em telecomunicações. Entretanto, indicam tendência de maior formalização de requisitos relacionados à gestão de riscos, proteção de ativos críticos, segurança de fornecedores, resiliência cibernética e demonstração de maturidade institucional. Em cenário de evolução regulatória, tais requisitos podem passar a incorporar, direta ou indiretamente, preocupações relacionadas à ameaça quântica.

2.5.5 Lacuna de Pesquisa

Apesar da multiplicidade de normas, políticas e iniciativas institucionais, não se identifica instrumento estruturado, mensurável e adaptado ao contexto nacional que permita a operadoras brasileiras de telecomunicações diagnosticar e priorizar sua preparação para a transição criptográfica pós-quântica. Essa lacuna torna-se mais relevante porque a preparação exige considerar, simultaneamente, obrigações setoriais da Anatel, proteção de dados pessoais, segurança de infraestruturas críticas, maturidade em privacidade e segurança da informação, infraestrutura de chaves públicas, criptografia de Estado e modernização regulatória em curso.
A complexidade técnica do setor reforça essa lacuna. Operadoras de telecomunicações possuem ambientes heterogêneos, tecnologias legadas, múltiplos fornecedores, dependências de cadeia de suprimentos, restrições orçamentárias, requisitos de continuidade operacional e necessidade permanente de capacitação. Esses fatores dificultam a conversão de recomendações internacionais genéricas em roteiro mensurável e compatível com a realidade brasileira.
Dessa forma, identifica-se a necessidade de um instrumento estruturado, mensurável e adaptado ao contexto nacional para avaliar a maturidade de operadoras brasileiras na preparação para a transição criptográfica pós-quântica. O MAT-CRIPTO-BR busca preencher essa lacuna ao organizar capacidades de governança, inventário criptográfico, avaliação de risco, criptoagilidade, gestão de fornecedores, implementação técnica, monitoramento e conformidade em um roteiro compatível com o ambiente regulatório brasileiro e com a evolução normativa em curso.

3 METODOLOGIA

Este estudo caracteriza-se como pesquisa aplicada, exploratória e qualitativa, com construção de artefato inspirada em Design Science Research. A metodologia contempla revisão bibliográfica e documental, análise comparativa de modelos de maturidade, definição de dimensões e indicadores, construção de mecanismos de pontuação e demonstração conceitual com dados simulados.

A pesquisa é aplicada porque busca produzir conhecimento voltado à solução de problema prático: a ausência de modelo estruturado para avaliar a maturidade de operadoras brasileiras na preparação pós-quântica. É exploratória porque aborda tema em consolidação técnica e regulatória. É qualitativa porque se baseia na interpretação de literatura técnica, documentos normativos, modelos de maturidade e requisitos setoriais.

A construção do MAT-CRIPTO-BR é inspirada em Design Science Research, abordagem adequada à criação de artefatos voltados a problemas organizacionais e tecnológicos relevantes (HEVNER et al., 2004; PEFFERS et al., 2007). O artefato corresponde ao próprio modelo, composto por dimensões, indicadores, escala, critérios de pontuação, ICM e IPM-PQC.

A revisão bibliográfica contemplou computação quântica, ameaça criptográfica, criptografia pós-quântica, criptoagilidade, inventário criptográfico, modelos de maturidade e gestão de risco cibernético. A análise documental examinou padrões técnicos, orientações institucionais e documentos regulatórios de organizações como NIST, ETSI, GSMA, 3GPP, Anatel e ICP-Brasil.

A construção do artefato ocorreu de forma analítica e iterativa: definição de dimensões, seleção de indicadores, escala de maturidade, regras de pontuação, ICM, IPM-PQC, critérios exemplificativos de evidência e demonstração com dados simulados. A pesquisa anexada ao processo de revisão foi utilizada como subsídio para reforçar a fundamentação das dimensões, especialmente inventário, criptoagilidade, gestão de fornecedores, capacitação e monitoramento contínuo.

Não houve coleta de dados reais em operadoras; instrumentos como questionário, roteiro de entrevista, matriz AHP e guia de remediação são tratados como materiais de apoio para validação futura. A principal limitação metodológica é a ausência de validação empírica com operadoras reais. Como a demonstração utiliza dados simulados, os resultados não podem ser generalizados para o setor. Também se reconhecem limitações na definição analítica dos pesos, na rápida evolução das fontes técnicas e normativas e no viés de construção por autor único. Essas limitações justificam validação posterior com especialistas e aplicações reais.

4 PROPOSTA DO MAT-CRIPTO-BR

O MAT-CRIPTO-BR é modelo preliminar de avaliação de maturidade para preparação à transição criptográfica pós-quântica em operadoras brasileiras de telecomunicações. O modelo busca apoiar diagnóstico inicial, priorização de ações e estruturação de evidências, sem substituir modelos amplos como C2M2, COBIT ou CMMI.

4.1 LÓGICA DE CONSTRUÇÃO DO MODELO

A lógica do MAT-CRIPTO-BR pode ser sintetizada em três eixos complementares. O primeiro eixo é inventário e priorização: antes de migrar, a organização precisa saber onde a criptografia vulnerável está presente, quais ativos protegem informações de longa duração e

quais dependências aumentam o risco de exposição. Esse eixo sustenta principalmente as dimensões D2 e D3.

O segundo eixo é implementação faseada e criptoágil. A transição pós-quântica tende a exigir pilotos, testes, mecanismos híbridos, atualização de bibliotecas, substituição controlada de certificados e coordenação com fornecedores. Esse eixo sustenta principalmente as dimensões D4, D5 e D6.

O terceiro eixo é governança, capacitação e conformidade. A preparação pós-quântica exige responsabilidades definidas, patrocínio executivo, alinhamento com segurança cibernética, compras, jurídico, arquitetura, operação e conformidade regulatória. Esse eixo sustenta principalmente as dimensões D1, D7 e D8 (BERNSTEIN et al., 2023; DEMIR; BILGIN; ONBASLI, 2025; GSM ASSOCIATION, 2024).

4.2 ESTRUTURA GERAL E DIMENSÕES

O modelo é composto por oito dimensões de maturidade, vinte e seis indicadores, escala MIL 0-3, Índice Composto de Maturidade e Índice de Prioridade de Migração Pós-Quântica. As dimensões refletem capacidades consideradas essenciais para a preparação organizacional à transição pós-quântica. A Tabela 4.1 apresenta a estrutura geral do modelo, com dimensões, indicadores e pesos propostos.

Tabela 4.1 - Estrutura geral do MAT-CRIPTO-BR

Dimensão	Nome	Indicadores	Peso
D1	Governança e Estratégia	MCB.01-MCB.03	0,15
D2	Inventário Criptográfico	MCB.04-MCB.07	0,18
D3	Avaliação de Risco e Priorização	MCB.08-MCB.11	0,18
D4	Criptoagilidade Técnica	MCB.12-MCB.14	0,15
D5	Gestão de Chaves e PKI	MCB.15-MCB.17	0,12
D6	Fornecedores	MCB.18-MCB.20	0,10
D7	Prontidão Organizacional	MCB.21-MCB.23	0,04
D8	Conformidade Regulatória	MCB.24-MCB.26	0,08

Fonte: Elaborado pelo autor.

D1 avalia política, plano de transição, papéis e governança executiva. D2 avalia algoritmos, certificados, chaves, protocolos, bibliotecas, aplicações, sistemas e fornecedores. D3 avalia risco quântico, criticidade, exposição, vida útil da informação e priorização. D4 avalia capacidade técnica de substituição, testes, modularidade e mudança controlada. D5 avalia ciclo de vida de chaves, certificados, HSM e PKI. D6 avalia dependências externas, contratos, aquisições e roadmaps de fornecedores. D7 avalia capacitação e integração entre áreas. D8 avalia alinhamento com obrigações regulatórias e evidências de conformidade.

A distribuição de pesos prioriza as capacidades que condicionam tecnicamente o início da transição. Inventário criptográfico (D2) e avaliação de risco e priorização (D3) recebem os maiores pesos (0,18 cada) por constituírem pré-requisitos para qualquer migração estruturada.

Governança (D1) e criptoagilidade técnica (D4) recebem peso intermediário (0,15). Prontidão organizacional (D7) recebe o menor peso (0,04) não por baixa relevância conceitual — a capacitação aparece de forma recorrente na fundamentação como capacidade habilitadora —, mas por ser, neste modelo, uma capacidade de suporte transversal cujos efeitos se materializam por meio das demais dimensões, e não um eixo de migração em si. Ressalva-se que essa ponderação é analítica e preliminar, devendo ser calibrada por painel de especialistas e métodos como Delphi ou AHP em validação futura.

4.3 ESCALA E INDICADORES DE MATURIDADE

A escala de maturidade possui quatro níveis, de MIL 0 a MIL 3, buscando equilíbrio entre simplicidade e capacidade de diferenciação entre estágios de preparação. A Tabela 4.2 define os níveis utilizados, enquanto a Tabela 4.3 sintetiza os indicadores e o foco de avaliação de cada dimensão.

Tabela 4.2 - Escala de maturidade do MAT-CRIPTO-BR

MIL	Denominação	Descrição
0	Inexistente	Ausência de capacidade estabelecida, processos, políticas ou evidências.
1	Inicial	Capacidade incipiente, parcial ou ad hoc.
2	Definido	Capacidade documentada, formalizada e parcialmente implementada.
3	Gerenciado	Capacidade monitorada, integrada à gestão e sujeita a melhoria contínua.

Fonte: Elaborado pelo autor.

Tabela 4.3 - Síntese dos indicadores por dimensão

Dimensão	Indicadores	Foco da avaliação
D1	MCB.01-MCB.03	Política, papéis, plano e governança
D2	MCB.04-MCB.07	Algoritmos, certificados, chaves, protocolos e sistemas
D3	MCB.08-MCB.11	Risco quântico, criticidade, exposição e priorização
D4	MCB.12-MCB.14	Substituição, testes, modularidade e adaptação
D5	MCB.15-MCB.17	Chaves, certificados, HSM, PKI e testes
D6	MCB.18-MCB.20	Contratos, fornecedores e requisitos de aquisição
D7	MCB.21-MCB.23	Capacitação, responsabilidades e comunicação
D8	MCB.24-MCB.26	Conformidade, regulação e reporte institucional

Fonte: Elaborado pelo autor.

4.4 ÍNDICE COMPOSTO DE MATURIDADE

O Índice Composto de Maturidade sintetiza a avaliação em escala de 0 a 100 pontos, permitindo comunicação executiva, acompanhamento temporal e identificação de dimensões prioritárias. O cálculo utiliza a média normalizada por dimensão, pesos, fator de conformidade obrigatória e fator de qualidade de evidências. A Tabela 4.4 apresenta as faixas de classificação adotadas para interpretação do índice.

$$ICM = (\Sigma\ Pi \times MILi) \times COBR \times Qev \times 100$$

Nessa formulação, Pi representa o peso da dimensão i, conforme a Tabela 4.1, sendo Σ Pi = 1,00. MILi corresponde ao nível médio normalizado da dimensão i, obtido pela média aritmética dos níveis MIL atribuídos aos indicadores daquela dimensão, dividida por 3, de modo

que MILi assume valores no intervalo [0; 1] (por exemplo, MIL 2 corresponde a 2/3 ≈ 0,67 e MIL 1 a 1/3 ≈ 0,33). O produto Σ Pi × MILi resulta, portanto, em valor entre 0 e 1, posteriormente convertido para a escala de 0 a 100 pela multiplicação por 100.

O fator de conformidade obrigatória (COBR) é um multiplicador no intervalo [0; 1] que penaliza a ausência de capacidades consideradas obrigatórias por exigência regulatória. Atribui-se COBR = 1,0 quando todos os indicadores de caráter obrigatório atingem, no mínimo, o nível exigido; valores inferiores a 1,0 são aplicados proporcionalmente à quantidade de requisitos obrigatórios não atendidos, refletindo que deficiências regulatórias devem reduzir a maturidade agregada independentemente do desempenho nas demais dimensões. O fator de qualidade das evidências (Qev), também no intervalo [0; 1], ajusta o resultado conforme a robustez das evidências documentais que sustentam as pontuações: evidências completas, formalizadas e verificáveis aproximam Qev de 1,0, enquanto evidências parciais, informais ou não verificáveis reduzem o fator. Ambos os fatores são paramétricos e devem ser calibrados em validação futura; os valores adotados na demonstração conceitual são ilustrativos.

Tabela 4.4 - Classificação do ICM

ICM	**Classificação**	**Interpretação**
0-19	Inexistente	Ausência de capacidades estruturadas
20-39	Inicial	Iniciativas pontuais ou ad hoc
40-59	Emergente	Capacidades parcialmente formalizadas
60-79	Estabelecido	Processos definidos e evidências consistentes
80-100	Otimizado	Capacidades gerenciadas e continuamente aprimoradas

Fonte: Elaborado pelo autor.

4.5 ÍNDICE DE PRIORIDADE DE MIGRAÇÃO PÓS-QUÂNTICA

O Índice de Prioridade de Migração Pós-Quântica (IPM-PQC) é um instrumento complementar ao Índice Composto de Maturidade, concebido para apoiar a ordenação de ativos, sistemas ou processos segundo a urgência relativa de sua migração criptográfica. Enquanto o ICM expressa o grau agregado de preparo organizacional, o IPM-PQC opera em nível analítico mais específico, voltado à priorização operacional de elementos cuja exposição à ameaça quântica possa exigir tratamento antecipado. Sua finalidade é oferecer critério sintético e comparável para subsidiar decisões iniciais de planejamento em contextos caracterizados por grande volume de ativos e restrições de tempo, orçamento e capacidade técnica.

$$IPM\text{-}PQC = C + E + D + V + M$$

Cada fator (C, criticidade; E, exposição; D, dificuldade de migração; V, vulnerabilidade; M, maturidade atual da gestão criptográfica associada ao ativo) é pontuado em escala de 1 a 5, resultando em valores agregados no intervalo de 5 a 25. Diferentemente do ICM, que pondera dimensões por meio de pesos, o IPM-PQC adota soma simples e não ponderada. Essa opção é

deliberada e justifica-se por seu propósito distinto: enquanto o ICM mede maturidade organizacional agregada, o IPM-PQC é um instrumento de triagem rápida para ordenar muitos ativos em cenários de recursos limitados, no qual a simplicidade e a transparência do cálculo são priorizadas sobre a precisão relativa entre fatores. A atribuição de pesos diferenciados aos cinco fatores é posicionada como aprimoramento para validação futura, preferencialmente por meio de calibração com especialistas.

A seleção desses fatores dialoga com abordagens consolidadas de avaliação de risco quântico. O PQC Migration Handbook propõe escore de risco quântico que combina fraqueza criptográfica, impacto e esforço de migração, mapeando-os em uma escala final por meio de tabela de correspondência, em vez de soma direta (AIVD; CWI; TNO, 2024). Os fatores de impacto e esforço de migração daquele modelo correspondem, aproximadamente, às noções de exposição e dificuldade de migração adotadas no IPM-PQC. A escolha por soma simples, e não por tabela de correspondência, é uma opção de transparência operacional, reconhecendo-se a alternativa como caminho de refinamento.

A dimensão temporal da priorização pode ser ancorada na desigualdade de Mosca, que estabelece a condição $X + Y < Z$, na qual X é o tempo durante o qual a informação deve permanecer segura, Y é o tempo necessário para concluir a migração e Z é o tempo estimado até a disponibilidade de um computador quântico criptograficamente relevante (MOSCA, 2018). Quanto mais $X + Y$ se aproxima de Z, mais urgente é a migração. Essa relação fundamenta a inclusão de fatores associados à vida útil da informação e à dificuldade de migração no IPM-PQC, reforçando que a priorização não depende apenas da criticidade atual, mas também do horizonte temporal de exposição. A Tabela 4.5 apresenta as faixas de classificação do IPM-PQC.

Tabela 4.5 - Classificação do IPM-PQC

Pontuação	**Prioridade**	**Interpretação**
20-25	Crítica	Prioridade máxima de migração
15-19	Alta	Planejamento de curto prazo
10-14	Média	Monitoramento e planejamento
5-9	Baixa	Tratamento em ciclo posterior

Fonte: Elaborado pelo autor.

4.6 PORTE DA OPERADORA E EVIDÊNCIAS

A interpretação dos resultados deve considerar porte, complexidade, exposição regulatória e dependência de fornecedores. Pequenas operadoras podem adotar metas iniciais

mais realistas, enquanto grandes operadoras tendem a exigir maturidade mais elevada. Essas faixas são indicativas e não representam baseline setorial validado. A Tabela 4.6 apresenta exemplos de evidências que podem sustentar a pontuação em cada dimensão.

Tabela 4.6 - Exemplos de evidências por dimensão

Dimensão	**Exemplos de evidências**
D1	Política, plano, atas de comitê e responsabilidades
D2	Inventário de algoritmos, certificados, chaves, protocolos e sistemas
D3	Relatório de risco quântico e matriz de criticidade
D4	Testes de substituição, arquitetura modular e registros de mudança
D5	Políticas de chaves, registros de certificados, HSM e testes
D6	Cláusulas contratuais, questionários e roadmaps
D7	Plano de capacitação, treinamentos e matriz de responsabilidades
D8	Relatórios de conformidade e evidências regulatórias

Fonte: Elaborado pelo autor.

O ICM e o IPM-PQC não devem ser interpretados como medidas absolutas de segurança. São instrumentos preliminares para diagnóstico, priorização e planejamento, sujeitos a validação e calibração futuras.

O IPM-PQC e o ICM constituem, conjuntamente, os dois instrumentos centrais do MAT-CRIPTO-BR. Enquanto o ICM expressa o grau agregado de maturidade organizacional para a transição pós-quântica, o IPM-PQC oferece mecanismo de triagem para ordenar ativos segundo urgência relativa de migração. A complementaridade entre os dois índices é intencional: o diagnóstico organizacional e a priorização de ativos são dimensões distintas, mas interdependentes, de um mesmo processo de preparação. O capítulo seguinte apresenta demonstração conceitual do modelo, ilustrando o cálculo do ICM, a análise de lacunas e a aplicação do IPM-PQC a um conjunto de ativos simulados.

5 DEMONSTRAÇÃO CONCEITUAL E DISCUSSÃO

A demonstração conceitual utiliza dados simulados, sem correspondência com operadora real. Seu objetivo é ilustrar o funcionamento do MAT-CRIPTO-BR, demonstrando cálculo do ICM, análise de lacunas e uso do IPM-PQC. Os resultados não constituem estudo de caso, validação empírica ou baseline setorial.

5.1 CENÁRIO E CÁLCULO DEMONSTRATIVO

Considera-se uma operadora fictícia de grande porte, com infraestrutura nacional, múltiplos fornecedores, sistemas OSS/BSS, PKI, VPNs, plataformas em nuvem e dependência de certificados digitais. Assume-se que a organização possui práticas gerais de segurança, mas baixa maturidade específica para transição pós-quântica. A Tabela 5.1 apresenta a aplicação demonstrativa do ICM por dimensão.

Tabela 5.1 - Aplicação demonstrativa do ICM por dimensão

Dimensão	Peso	MIL	Normalizado	Contribuição
D1 Governança	0,15	2	0,67	0,100
D2 Inventário	0,18	1	0,33	0,059
D3 Risco	0,18	1	0,33	0,059
D4 Criptoagilidade	0,15	1	0,33	0,050
D5 Chaves/PKI	0,12	2	0,67	0,080
D6 Fornecedores	0,10	1	0,33	0,033
D7 Prontidão	0,04	2	0,67	0,027
D8 Conformidade	0,08	2	0,67	0,054
Total	1,00	-	-	0,462

Fonte: Elaborado pelo autor.

Aplicando-se COBR = 1,0 e Qev = 0,95, obtém-se ICM = 43,9, correspondente à maturidade Emergente. O resultado indica capacidades parcialmente formalizadas, mas lacunas relevantes em inventário, risco quântico, criptoagilidade e fornecedores.

5.2 ANÁLISE DE LACUNAS

Esta subseção interpreta os resultados simulados a partir da diferença entre o nível atual e o nível-alvo de maturidade. A análise de lacunas permite identificar quais dimensões exigiriam tratamento prioritário em um plano de preparação pós-quântica. A Tabela 5.2 apresenta a lacuna demonstrativa por dimensão.

Tabela 5.2 - Análise demonstrativa de lacunas por dimensão

Dimensão	Atual	Alvo	Gap	Prioridade
D1 Governança	2	3	1	Média
D2 Inventário	1	3	2	Crítica
D3 Risco	1	3	2	Crítica
D4 Criptoagilidade	1	2	1	Alta
D5 Chaves/PKI	2	3	1	Média
D6 Fornecedores	1	2	1	Alta
D7 Prontidão	2	2	0	Nenhuma
D8 Conformidade	2	3	1	Baixa

Fonte: Elaborado pelo autor.

As maiores lacunas concentram-se em D2 e D3. Essa conclusão é coerente com a lógica do modelo: antes de migrar algoritmos, a organização precisa identificar onde a criptografia vulnerável está presente e quais ativos devem ser priorizados. D4 e D6 também são relevantes porque a migração depende de capacidade técnica de mudança e coordenação com fornecedores.

5.3 EXEMPLO DE APLICAÇÃO DO IPM-PQC

Esta subseção exemplifica o uso do IPM-PQC para ordenar ativos, sistemas ou processos conforme a urgência de migração. O objetivo é demonstrar como o modelo pode apoiar decisões iniciais de priorização quando há muitos ativos criptograficamente relevantes e recursos limitados. A Tabela 5.3 apresenta exemplo de aplicação do índice a ativos e sistemas selecionados.

Tabela 5.3 - Exemplo demonstrativo de aplicação do IPM-PQC

Ativo ou sistema	C	E	D	V	M	IPM-PQC	Prioridade
PKI interna	5	4	4	5	4	22	Crítica
VPN acesso remoto	4	5	3	4	3	19	Alta
Certificados de rede	5	3	4	4	3	19	Alta
OSS/BSS legado	5	3	5	3	4	20	Crítica
Portal interno	3	2	2	3	2	12	Média
Treinamento interno	2	1	1	2	2	8	Baixa

Fonte: Elaborado pelo autor.

No exemplo, PKI interna e OSS/BSS legado aparecem como prioridades críticas. A PKI concentra funções de confiança digital, enquanto sistemas OSS/BSS legados combinam alta criticidade e dificuldade de migração. O IPM-PQC não substitui análise técnica detalhada, mas oferece mecanismo inicial de ordenação para ambientes com muitos ativos e recursos limitados.

5.4 DISCUSSÃO, LIMITAÇÕES E VALIDAÇÃO FUTURA

A demonstração indica que o MAT-CRIPTO-BR pode apoiar diagnóstico agregado, identificação de lacunas e priorização de ativos. Também evidencia que maturidade geral em segurança cibernética não equivale, necessariamente, à maturidade específica para transição pós-quântica.

A leitura dos resultados reforça três contribuições práticas. A primeira é explicitar que inventário e risco devem anteceder pilotos técnicos. A segunda é destacar que criptoagilidade depende de arquitetura e processos de mudança, não apenas de bibliotecas criptográficas. A terceira é tornar visível que fornecedores, contratos e roadmaps tecnológicos condicionam o ritmo real da transição em telecomunicações.

As limitações decorrem do uso de dados simulados, da definição analítica dos pesos, da ausência de avaliação independente e da evolução contínua de padrões técnicos e normativos. Assim, os resultados não podem ser generalizados para o setor.

Como validação futura, recomenda-se aplicação piloto em uma ou mais operadoras brasileiras, coleta de evidências documentais, entrevistas estruturadas, painel de especialistas, calibração de pesos por Delphi ou AHP e construção de baseline setorial com dados reais anonimizados.

6 CONCLUSÃO

Este trabalho propôs o MAT-CRIPTO-BR como modelo preliminar de avaliação de maturidade para apoiar operadoras brasileiras de telecomunicações na preparação para a transição criptográfica pós-quântica. A proposta foi motivada pelos impactos potenciais da computação quântica sobre algoritmos de chave pública e pela necessidade de planejamento antecipado em infraestruturas críticas.

A principal contribuição foi organizar capacidades técnicas, organizacionais e regulatórias em oito dimensões, vinte e seis indicadores, escala MIL 0-3, Índice Composto de Maturidade e Índice de Prioridade de Migração Pós-Quântica. O ICM apoia diagnóstico agregado, enquanto o IPM-PQC auxilia a priorização de ativos e sistemas que demandam migração.

A fundamentação do modelo conecta suas dimensões a achados sobre inventário criptográfico, criptoagilidade, modelos híbridos, gestão de fornecedores, capacitação, monitoramento contínuo e limitações de modelos genéricos de maturidade. Essa articulação fortalece a justificativa das dimensões e dos mecanismos de avaliação, sem alterar o escopo preliminar da proposta.

A construção do modelo foi fundamentada em revisão bibliográfica e documental, análise de modelos de maturidade e referências técnicas sobre criptografia pós-quântica, criptoagilidade, gestão de ativos criptográficos, segurança cibernética em infraestrutura crítica e regulação aplicável ao setor brasileiro de telecomunicações.

A demonstração conceitual com dados simulados permitiu ilustrar o cálculo do ICM, a análise de lacunas e a aplicação do IPM-PQC. O cenário demonstrativo indicou que inventário criptográfico, avaliação de risco quântico, criptoagilidade técnica e gestão de fornecedores tendem a ser dimensões críticas para o início da preparação.

A principal limitação é a ausência de validação empírica com operadoras reais. Portanto, o MAT-CRIPTO-BR deve ser compreendido como proposta preliminar, sujeita a refinamento posterior. Pesos, critérios, evidências e escalas devem ser avaliados por especialistas e testados em aplicações reais.

Como trabalhos futuros, recomenda-se aplicar o modelo em operadoras brasileiras, submeter dimensões e indicadores a painel de especialistas, calibrar pesos por métodos como Delphi ou AHP, avaliar concordância entre avaliadores, comparar o modelo com C2M2, COBIT ou CAMM e desenvolver baseline setorial com dados reais anonimizados.

Conclui-se que o MAT-CRIPTO-BR oferece estrutura inicial para que operadoras brasileiras possam compreender, medir e planejar sua preparação para a transição criptográfica pós-quântica. Embora dependa de validação empírica, o modelo contribui ao traduzir um problema técnico emergente em dimensões avaliáveis, indicadores observáveis, critérios de maturidade e mecanismos de priorização.

REFERÊNCIAS

3RD GENERATION PARTNERSHIP PROJECT. 3GPP TR 33.703: Study on Post-Quantum Cryptography for 5G. [S.l.]: 3GPP, 2024.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. ABIN lança criptografia com algoritmos pós-quânticos para as eleições. Brasília, DF: ABIN, 14 set. 2022. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/abin-lanca-criptografia-com-algoritmos-pos-quanticos-para-as-eleicoes>. Acesso em: 10 jun. 2026.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. Decifre o papel da ABIN na criptografia das urnas eletrônicas em novo episódio do ABINCast. Brasília, DF: ABIN, 28 ago. 2024. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/decifre-o-papel-da-abin-na-criptografia-das-urnas-eletronicas-em-novo-episodio-do-abincast>. Acesso em: 10 jun. 2026.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Resolução nº 740, de 21 de dezembro de 2020. Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Brasília, DF: Anatel, 2020. Disponível em: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740>. Acesso em: 10 jun. 2026.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Resolução nº 767, de 7 de agosto de 2024. Altera o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Brasília, DF: Anatel, 2024. Disponível em: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2024/1965-resolucao-767>. Acesso em: 10 jun. 2026.

ALGEMENE INLICHTINGEN- EN VEILIGHEIDSDIENST; CENTRUM WISKUNDE & INFORMATICA; NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK. The PQC Migration Handbook: **guidance** for migrating to post-quantum cryptography. [S.l.]: AIVD; CWI; TNO, 2024.

AT&T. Preparing for The Quantum Era: AT&T Business Debuts Post-Quantum Cryptography Secure SD-WAN, Powered by Cisco. AT&T News, Dallas, 11 maio 2026. Disponível em: <https://about.att.com/story/2026/cisco-post-quantum-cryptography.html>. Acesso em: 10 jun. 2026.

BERNSTEIN, D. J.; HOFFMAN, P. E.; HOPWOOD, D.; LENSTRA, A. K.; MOSCA, M.; PERIN, G. Cryptographic Asset Management Maturity (CAMM) Framework. [S.l.], 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018a. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 jun. 2026.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2018b. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9573.htm>. Acesso em: 10 jun. 2026.

BRASIL. Decreto nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm>. Acesso em: 10 jun. 2026.

BRASIL. Decreto nº 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm>. Acesso em: 10 jun. 2026.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm>. Acesso em: 10 jun. 2026.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2025a. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm>. Acesso em: 10 jun. 2026.

BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. Brasília, DF: Presidência da República, 2025b. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12572.htm>. Acesso em: 10 jun. 2026.

CMMI INSTITUTE. CMMI for Development, Version 2.0. Pittsburgh, PA: CMMI Institute, 2018.

COMITÊ NACIONAL DE CIBERSEGURANÇA. Resolução CNCiber nº 16, de 13 de outubro de 2025. Institui grupo de trabalho temático para elaboração de modelos nacionais de maturidade em cibersegurança. Brasília, DF: GSI/PR, 2025. Disponível em:

<https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber/resolucoes/resolucao-cnciber-no-16-de-13-de-outubro-de-2025.pdf>. Acesso em: 10 jun. 2026.

DEMIR, E. D.; BILGIN, B.; ONBASLI, M. C. Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms. **arXiv**, Ithaca, arXiv:2503.12952 [cs.CR], 2025. Disponível em: <https://arxiv.org/abs/2503.12952>. Acesso em: 10 jun. 2026.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. ETSI TR 103 744: Quantum-Safe Cryptography; Quantum-Safe Threat Assessment. Sophia Antipolis: ETSI, 2023.

GSM ASSOCIATION. Post-Quantum Telco Network Task Force: Recommendations. London: GSMA, 2024.

HEVNER, A. R.; MARCH, S. T.; PARK, J.; RAM, S. Design science in information systems research. MIS Quarterly, v. 28, n. 1, p. 75-105, 2004.

HOFFMAN, P. E. The Transition from Classical to Post-Quantum Cryptography. [S.l.], 2017. Internet-Draft. Disponível em: <https://datatracker.ietf.org/doc/draft-hoffman-c2pq/02/>. Acesso em: 10 jun. 2026.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil). Instrução Normativa ITI nº 35, de 30 de janeiro de 2026. Acrescenta novos algoritmos criptográficos e certificados digitais ao documento Padrões e Algoritmos Criptográficos da ICP-Brasil — DOC-ICP-01.01. Brasília, DF: ITI, 2026. Disponível em: <https://repositorio.iti.gov.br/instrucoes-normativas/IN2026_35_DOC_ICP_01.01_PQC.htm>. Acesso em: 10 jun. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 21827: Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model (SSE-CMM). Geneva: ISO, 2008.

ISACA. COBIT 2019 Framework: Introduction and Methodology. Rolling Meadows: ISACA, 2019.

KONG, I.; JANSSEN, M.; BHAROSA, N. Navigating Through the Unknowns: Organizational Readiness Assessment Model for Quantum-Safe Transition. In: JANSSEN, M.; CROMPVOETS, J.; GIL-GARCÍA, J. R.; LEE, H.; LINDGREN, I.; NIKIFOROVA, A.; PEREIRA, G. V. (org.). **Electronic Government: 23rd IFIP WG 8.5 International Conference, EGOV 2024, Ghent-Leuven, Belgium, September 3-5, 2024, Proceedings**. Cham: Springer, 2024. p. 438-453.

LINSTONE, H. A.; TUROFF, M. The Delphi Method: Techniques and Applications. Reading: Addison-Wesley, 1975.

LIU, Nancy. AT&T Aims to be 'Quantum Ready' by 2025. SDxCentral, 5 out. 2022. Disponível em: <https://www.sdxcentral.com/news/att-aims-to-be-quantum-ready-by-2025/>. Acesso em: 10 jun. 2026.

LIYANAGE, L.; ARACHCHILAGE, N. A. G.; RUSSELLO, G. SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). **arXiv**, Ithaca, arXiv:2408.16140 [cs.CR], 2024. Disponível em: <https://arxiv.org/abs/2408.16140>. Acesso em: 10 jun. 2026.

MOSCA, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? **IEEE Security & Privacy**, Los Alamitos, v. 16, n. 5, p. 38-41, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Gaithersburg, MD: NIST, 2024a. Federal Information Processing Standards Publication FIPS 203.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Module-Lattice-Based Digital Signature Standard. Gaithersburg, MD: NIST, 2024b. Federal Information Processing Standards Publication FIPS 204.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Stateless Hash-Based Digital Signature Standard. Gaithersburg, MD: NIST, 2024c. Federal Information Processing Standards Publication FIPS 205.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Transition to Post-Quantum Cryptography Standards. Gaithersburg, MD: NIST, 2024d. NIST Internal Report 8547, initial public draft.

PEFFERS, K.; TUUNANEN, T.; ROTHENBERGER, M. A.; CHATTERJEE, S. A design science research methodology for information systems research. Journal of Management Information Systems, v. 24, n. 3, p. 45-77, 2007.

SAATY, T. L. The Analytic Hierarchy Process. New York: McGraw-Hill, 1980.

SECRETARIA DE GOVERNO DIGITAL. Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025. Institui o Programa de Privacidade e Segurança da Informação 2.0 no âmbito do SISP. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2025. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455>. Acesso em: 10 jun. 2026.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, 35., 1994. Proceedings [...]. [S.l.]: IEEE, 1994.

SK TELECOM. SK Telecom and Thales Collaborate on Post-Quantum Cryptography to Enhance Users' Protection on 5G Network. SK Telecom Newsroom, Seul, 19 dez. 2023. Disponível em: <https://news.sktelecom.com/en/628>. Acesso em: 10 jun. 2026.

SOFTBANK CORP.; SANDBOXAQ. SoftBank Corp. and SandboxAQ Jointly Verify Hybrid Mode Quantum-safe Technology. SoftBank Research Institute of Advanced Technology, Tóquio, 28 fev. 2023. Disponível em: <https://www.softbank.jp/en/corp/technology/research/topics/008/>. Acesso em: 10 jun. 2026.

SOFTBANK CORP.; SANDBOXAQ. Designing a Hybrid Path to PQC Built for the Real World. Tóquio: SoftBank Research Institute of Advanced Technology, 2025. White paper. Disponível em: <https://www.softbank.jp/en/corp/set/data/technology/research/news/076/pdf/WhitePaper_PQC_SB_SAQ_250425_en.pdf>. Acesso em: 10 jun. 2026.

U.S. DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2), Version 2.1. Washington, DC: U.S. Department of Energy, 2022.

APÊNDICE A - INSTRUMENTO PRELIMINAR DE AVALIAÇÃO DO MAT-CRIPTO-BR

Apêndice reservado à matriz operacional de avaliação por indicador, com campo para pontuação MIL 0-3, evidência, justificativa e responsável pela validação. O instrumento deve ser aplicado em etapa futura de validação, preferencialmente com coleta de evidências documentais e avaliação independente por especialistas.

APÊNDICE B - ROTEIRO PRELIMINAR DE ENTREVISTA PARA VALIDAÇÃO FUTURA

Apêndice reservado ao roteiro de entrevista ou questionário estruturado para avaliar clareza, relevância, completude e aplicabilidade do modelo. Recomenda-se que a validação futura utilize perguntas fechadas, escala de concordância e espaço controlado para observações, reduzindo o esforço dos respondentes e preservando a finalidade metodológica.

APÊNDICE C - MATRIZ PRELIMINAR DE CALIBRAÇÃO DE PESOS

Apêndice reservado à matriz de calibração de pesos por métodos como Delphi ou AHP em estudos futuros. A matriz deve permitir comparação entre dimensões, registro de justificativas e cálculo de consistência quando aplicável.

APÊNDICE D - GUIA SINTÉTICO DE REMEDIAÇÃO POR DIMENSÃO

Este apêndice sintetiza ações de remediação associadas às dimensões do MAT-CRIPTO-BR. As ações não constituem prescrição exaustiva, mas servem como roteiro inicial para transformar os resultados da avaliação em plano de melhoria. O Quadro D.1 apresenta recomendações e evidências mínimas esperadas por dimensão.

Quadro D.1 - Guia sintético de remediação por dimensão

Dimensão	Ações recomendadas	Evidências mínimas esperadas
D1 Governança e Estratégia	Formalizar política de transição PQC, definir responsável executivo, criar plano de transição e integrar o tema à gestão de riscos.	Política aprovada, plano de transição, atas de comitê, matriz de responsabilidades.
D2 Inventário Criptográfico	Mapear algoritmos, certificados, chaves, protocolos, bibliotecas, PKI, VPNs, sistemas legados e dependências de fornecedores.	Inventário criptográfico, CBOM, registros de certificados, mapeamento de aplicações e fornecedores.
D3 Avaliação de Risco e Priorização	Classificar ativos por criticidade, exposição, vida útil da informação, dificuldade de migração e vulnerabilidade quântica.	Matriz de risco quântico, critérios de priorização, lista de ativos críticos e plano de tratamento.
D4 Criptoagilidade Técnica	Realizar pilotos, testar mecanismos híbridos, avaliar modularidade criptográfica e estabelecer processo de mudança controlada.	Relatórios de teste, registros de mudança, arquitetura-alvo, plano de rollback e evidências de homologação.
D5 Gestão de Chaves e PKI	Revisar ciclo de vida de chaves e certificados, avaliar HSMs, dependências ICP/PKI e prontidão para ML-KEM, ML-DSA e SLH-DSA.	Política de chaves, registros de certificados, inventário de HSMs, plano de renovação e testes de compatibilidade.
D6 Fornecedores	Exigir roadmap PQC, cláusulas contratuais de atualização criptográfica, questionários de prontidão e evidências de suporte a padrões.	Contratos, questionários respondidos, roadmaps de fornecedores, requisitos de aquisição e SLA de atualização.
D7 Prontidão Organizacional	Capacitar equipes técnicas, segurança, arquitetura, jurídico, compras e operação; definir comunicação interna sobre riscos PQC.	Plano de capacitação, registros de treinamento, matriz RACI e materiais de comunicação.
D8 Conformidade Regulatória	Monitorar Anatel, ICP-Brasil, NIST, ETSI, GSMA e 3GPP; associar evidências do modelo a obrigações regulatórias e auditorias.	Relatórios de conformidade, matriz de aderência, evidências de auditoria e registros de acompanhamento normativo.

Fonte: Elaborado pelo autor.

A priorização das ações deve considerar o resultado do ICM, o IPM-PQC dos ativos críticos, a disponibilidade de fornecedores e o calendário de atualização tecnológica da operadora. Em ambientes com recursos limitados, recomenda-se iniciar por inventário, risco e dependências externas, pois essas dimensões condicionam as demais etapas da transição.