www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 164, 2026 | DOI: 10.69849/g5e40w31

O impacto da computação quântica na segurança de dados

The impact of quantum computing on data security

Pedro Henrique Baltazar Louzada[1]
Rafael Martins Gomes dos Santos[2]
Emanuel de Azevedo Silva[3]

Resumo

Este artigo analisa os impactos da computação quântica sobre a segurança de dados em ambientes corporativos. Trata-se de uma pesquisa teórica, qualitativa e exploratório-descritiva, desenvolvida por meio de revisão bibliográfica narrativa. Inicialmente, são apresentados os fundamentos da segurança da informação e os padrões criptográficos simétricos e assimétricos mais utilizados atualmente. Em seguida, descreve-se o funcionamento da computação quântica e o modo como os algoritmos de Shor e de Grover afetam o RSA, o ECC e o AES. Também são discutidas duas soluções emergentes, a Criptografia Pós-Quântica (PQC), com destaque para os padrões ML-KEM e ML-DSA do NIST, e a Distribuição Quântica de Chaves (QKD). Com base na comparação entre essas abordagens, o trabalho propõe diretrizes para a transição da infraestrutura de TI corporativa, que envolvem o mapeamento do inventário criptográfico, a adoção de esquemas híbridos e a *crypto-agility*. Conclui-se que iniciar a migração com antecedência reduz os riscos e os custos associados à ameaça quântica.

Palavras-chave: Segurança de dados; Criptografia; Computação quântica; Criptografia pós quântica; Distribuição quântica de chaves.

[1] Centro Universitário Sul-Americano (UNIFASAM) – Goiânia – Goiás – Brasil. ORCID: https://orcid.org/0009- 0008-3215-6700
[2] Centro Universitário Sul-Americano (UNIFASAM) – Goiânia – Goiás – Brasil. ORCID: https://orcid.org/0009- 0005-1039-516X
[3] Centro Universitário Sul-Americano (UNIFASAM) – Goiânia – Goiás – Brasil. ORCID: https://orcid.org/0009- 0002-6411-3058

Abstract

This article analyzes the impacts of quantum computing on data security in corporate environments. It is a theoretical, qualitative, exploratory-descriptive study, conducted through a narrative literature review. It first presents the foundations of information security and the symmetric and asymmetric cryptographic standards most widely used today. It then describes how quantum computing works and how Shor's and Grover's algorithms affect RSA, ECC, and AES. Two emerging solutions are also discussed, Post-Quantum Cryptography (PQC), with emphasis on the NIST ML-KEM and ML-DSA standards, and Quantum Key Distribution (QKD). Based on a comparison between these approaches, the study proposes guidelines for the transition of corporate IT infrastructure, including cryptographic inventory mapping, the adoption of hybrid schemes, and crypto-agility. It concludes that starting the migration early reduces the risks and costs associated with the quantum threat.

Keywords: Data security; Cryptography; Quantum computing; Post-quantum cryptography; Quantum key distribution.

1 Introdução

No cenário contemporâneo, marcado pela constante evolução digital e pelo crescente volume de dados compartilhados e armazenados em ambiente virtual, a segurança da informação tornou-se um dos principais desafios enfrentados por organizações e usuários, ampliando a necessidade de mecanismos capazes de mitigar ataques cibernéticos, vazamentos e acessos indevidos. Segundo relatório divulgado pela IBM em 2024, o custo médio global de uma violação de dados atingiu aproximadamente US$ 4,8 milhões, um dos maiores valores já registrados para incidentes de segurança digital (IBM, 2024). Esse volume tende a crescer ainda mais nos próximos anos, acompanhando a expansão da inteligência artificial e da computação em nuvem.

Nesse cenário, a criptografia destaca-se como uma das principais ferramentas utilizadas para garantir a segurança de dados por meio dos princípios de confidencialidade, integridade e disponibilidade (STALLINGS, 2017). Diferentes padrões criptográficos vêm sendo empregados na atualidade, sendo fundamentais para a segurança de sistemas e múltiplas aplicações. Contudo, o avanço da computação

quântica tem levantado preocupações, pois sua capacidade de processamento pode comprometer algoritmos amplamente utilizados atualmente, tais como o RSA e a Criptografia de Curvas Elípticas (ECC) (NIELSEN; CHUANG, 2010).

Diferentemente da computação clássica, baseada em bits que assumem os estados 0 ou 1, a computação quântica utiliza *qubits*, capazes de explorar propriedades da mecânica quântica – como superposição, entrelaçamento e interferência – permitindo a realização de cálculos complexos de

maneira exponencialmente mais eficiente. Embora ainda seja uma tecnologia emergente e limitada a poucas organizações, discutir seus impactos sobre a proteção da informação e as estratégias de adaptação, como a criptografia pós-quântica já recomendada pelo National Institute of Standards and Technology (2024), torna-se necessário para capacitar as empresas a enfrentarem riscos futuros.

1.1 Justificativa

A crescente dependência de ecossistemas digitais tornou a segurança da informação indispensável para a continuidade das organizações no mercado. Grande parte dessa proteção é sustentada pela criptografia moderna, que resguarda infraestruturas e transações econômicas em escala global. Com o avanço da computação quântica, porém, os métodos de proteção tradicionais passam a ser vulneráveis, já que computadores quânticos criptograficamente relevantes poderão romper os padrões atuais em questão de horas. Por isso, é necessário compreender desde já os impactos e os riscos dessa transição para a segurança corporativa, para que as infraestruturas de TI sejam adaptadas antes que a criptografia clássica deixe de ser eficaz.

1.2 Objetivos

O objetivo geral deste trabalho é analisar os impactos da computação quântica sobre os sistemas de segurança de dados no ambiente corporativo, investigando as vulnerabilidades da criptografia e as soluções emergentes para a preservação da integridade informacional na era pós quântica. Especificamente, busca-se:

1. contextualizar a importância da criptografia simétrica e assimétrica na proteção de ativos digitais corporativos;
2. demonstrar como os algoritmos quânticos comprometem a eficácia dos padrões criptográficos vigentes;

3. avaliar as alternativas de defesa emergentes, incluindo os novos padrões de criptografia pós-quântica e as tecnologias de distribuição quântica de chaves (QKD);
4. propor diretrizes para o planejamento e a transição da infraestrutura de TI das empresas para um modelo de segurança resistente a ataques quânticos.

2 Revisão da Literatura

2.1 Segurança da Informação e Criptografia Clássica

A segurança da informação é definida pela norma ISO/IEC 27000 (ISO/IEC, 2014) como a preservação da confidencialidade, integridade e disponibilidade da informação, envolvendo ainda propriedades como autenticidade, responsabilidade e não repúdio. Segundo Anderson (2020), esses três pilares – confidencialidade, integridade e disponibilidade – precisam ser trabalhados em conjunto para que as organizações reconheçam vulnerabilidades, reduzam riscos e preservem a continuidade dos negócios em um ambiente cibernético eficaz.

Os principais conceitos associados à segurança da informação são:

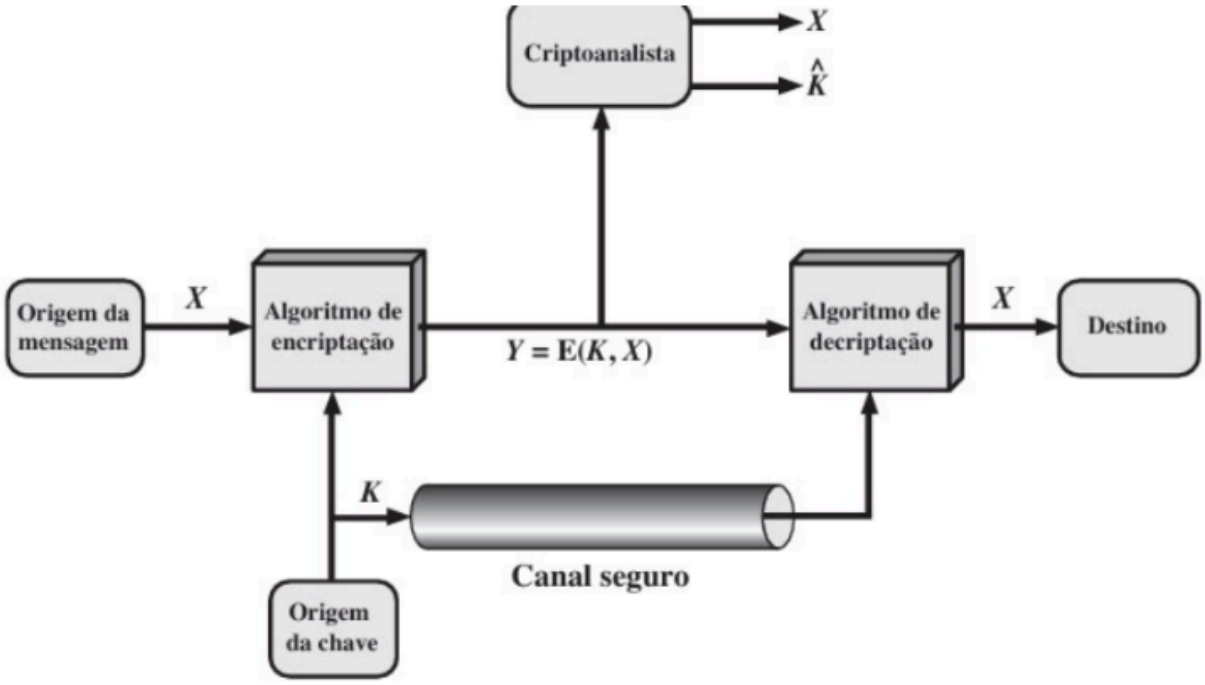
- **Sigilo:** refere-se ao efeito das ferramentas utilizadas para delimitar a quantidade de indivíduos que podem acessar uma informação específica.
- **Privacidade:** competência e/ou direito de preservar as próprias informações pessoais e de se proteger contra invasões ao espaço pessoal; pode se estender a famílias, mas não a entidades jurídicas.
- **Confidencialidade:** dever de cuidar dos segredos de uma pessoa ou organização quando se tem conhecimento deles.
- **Integridade:** garantia de que dados, informações e sistemas não sejam modificados sem autorização prévia ou de forma incorreta.
- **Disponibilidade:** garante que uma informação ou sistema esteja acessível a qualquer momento por um usuário autorizado.

A necessidade de proteger informações acompanha a humanidade desde as primeiras civilizações: segundo Singh (1999), já na Antiguidade existiam formas rudimentares de criptografia, como a escítala espartana. Um marco relevante foi a Cifra de César, na Roma antiga, uma cifra de substituição na qual cada letra é deslocada um número fixo de posições no alfabeto (DOOLEY, 2024). Além dos sistemas formais de cifragem, práticas de ocultação da informação também se desenvolveram

espontaneamente em contextos sociais específicos, funcionando como códigos linguísticos de resistência. Um exemplo brasileiro é a Linguagem de Camaco, manifestação linguística popular surgida entre trabalhadores das minas de Itabira, Minas Gerais, como forma de resistência à presença de garimpeiros na região (MARCHIORI, 2021). Seu funcionamento consiste na alteração da ordem dos fonemas das sílabas das palavras, criando um código sonoro compreensível apenas por seus falantes. Embora não se trate de um sistema criptográfico formal, a Linguagem de Camaco ilustra, em um contexto sociolinguístico, o mesmo princípio fundamental que rege a criptografia: a transformação estruturada de uma mensagem original em uma forma compreensível apenas por um grupo restrito de indivíduos. Já na Segunda Guerra Mundial, a criptografia passou por um período de grande evolução, destacando-se a máquina Enigma, utilizada pelas forças alemãs, e a máquina Bombe, desenvolvida por Alan Turing para automatizar a quebra de seus códigos (DOOLEY, 2024). Esse histórico evidencia como a criptografia evoluiu ao longo dos séculos, tornando-se cada vez mais complexa e resistente à quebra de códigos, até consolidar-se como um dos principais mecanismos de proteção da informação na atualidade.

A criptografia consolidou-se como um dos métodos mais relevantes para a proteção de dados, definida como o conjunto de técnicas científicas e matemáticas utilizadas para codificar informações, tornando-as incompreensíveis a pessoas não autorizadas (STALLINGS, 2017). Atualmente, sua evolução possibilitou o desenvolvimento de algoritmos altamente robustos, fundamentados em problemas matemáticos cuja resolução é computacionalmente inviável para computadores clássicos em tempo hábil, destacando-se a fatoração de grandes números inteiros e o cálculo de logaritmos discretos, empregados por algoritmos como RSA e ECC (MOBILON; ROSOLEM, 2024). Um sistema criptográfico simétrico utiliza uma única chave secreta tanto para cifrar quanto para decifrar a mensagem (Figura 1), enquanto um sistema assimétrico – ou de chave pública – emprega um par de chaves matematicamente relacionadas: a chave pública cifra a informação ou verificar assinaturas, e a chave privada a decifra ou assina, eliminando a necessidade de compartilhamento prévio de segredo entre as partes (Figura 2) (STALLINGS, 2014). Na prática, sistemas modernos adotam uma abordagem híbrida, combinando a criptografia assimétrica para o compartilhamento seguro da chave com a criptografia simétrica para proteger o restante dos dados.

Figura 1 – Modelo de criptossistema simétrico



Fonte: Adaptado de Stallings (2014).

Segundo Stallings (2014), um sistema criptográfico simétrico como o da Figura 1 é composto por cinco elementos: o **texto plano**, mensagem original antes da aplicação do algoritmo; o **algoritmo de criptografia**, que realiza as transformações matemáticas responsáveis por gerar o texto cifrado; a **chave secreta**, entrada independente do texto plano que determina as substituições aplicadas; o **texto cifrado**, mensagem de saída, que depende tanto do texto plano quanto da chave específica utilizada; e o **algoritmo de decriptação**, que reverte o processo de encriptação a partir do texto cifrado e da chave correspondente. Esse processo de cifragem pode ser representado pela Equação 1:

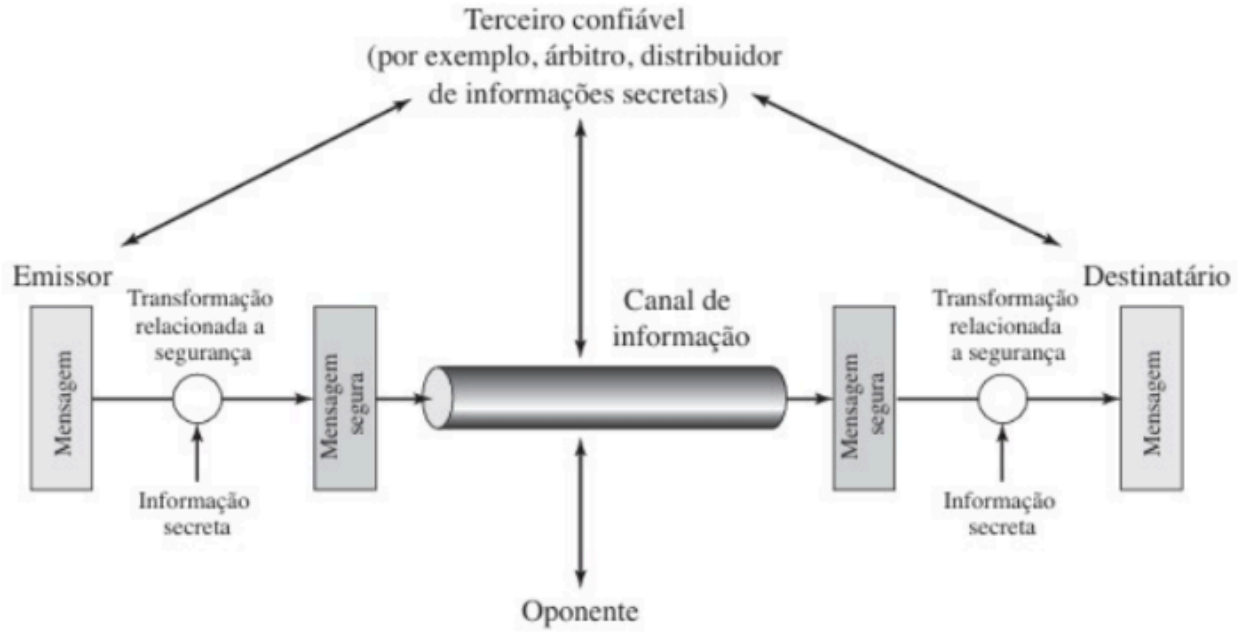
$$Y = E(K, X) \qquad (1)$$

em que X é o texto plano, K a chave criptográfica, E o algoritmo de criptografia e Y o texto cifrado resultante. Para recuperar a mensagem original, o destinatário aplica a chave correspondente ao algoritmo de decriptação, conforme a Equação 2:

$$X = D(K, Y) \qquad (2)$$

em que D representa o algoritmo de decriptação. Apenas quem possui a chave correta é capaz de recuperar o texto plano a partir do texto cifrado.

Figura 2 – Modelo de criptossistema assimétrico



Fonte: Adaptado de Stallings (2014).

2.2 Computação Quântica

A computação quântica pode ser definida como o modelo de computação baseado nos princípios da mecânica quântica, capaz de manipular informações e resolver determinados problemas de maneira mais eficiente que computadores clássicos (NIELSEN; CHUANG, 2010). O conceito remonta à proposta de Feynman (1982), formalizado por Deutsch (1985), e teve sua viabilidade física comprovada experimentalmente em 2001, quando um sistema baseado em Ressonância Magnética Nuclear fatorou o número 15 (VANDERSYPEN et al., 2001).

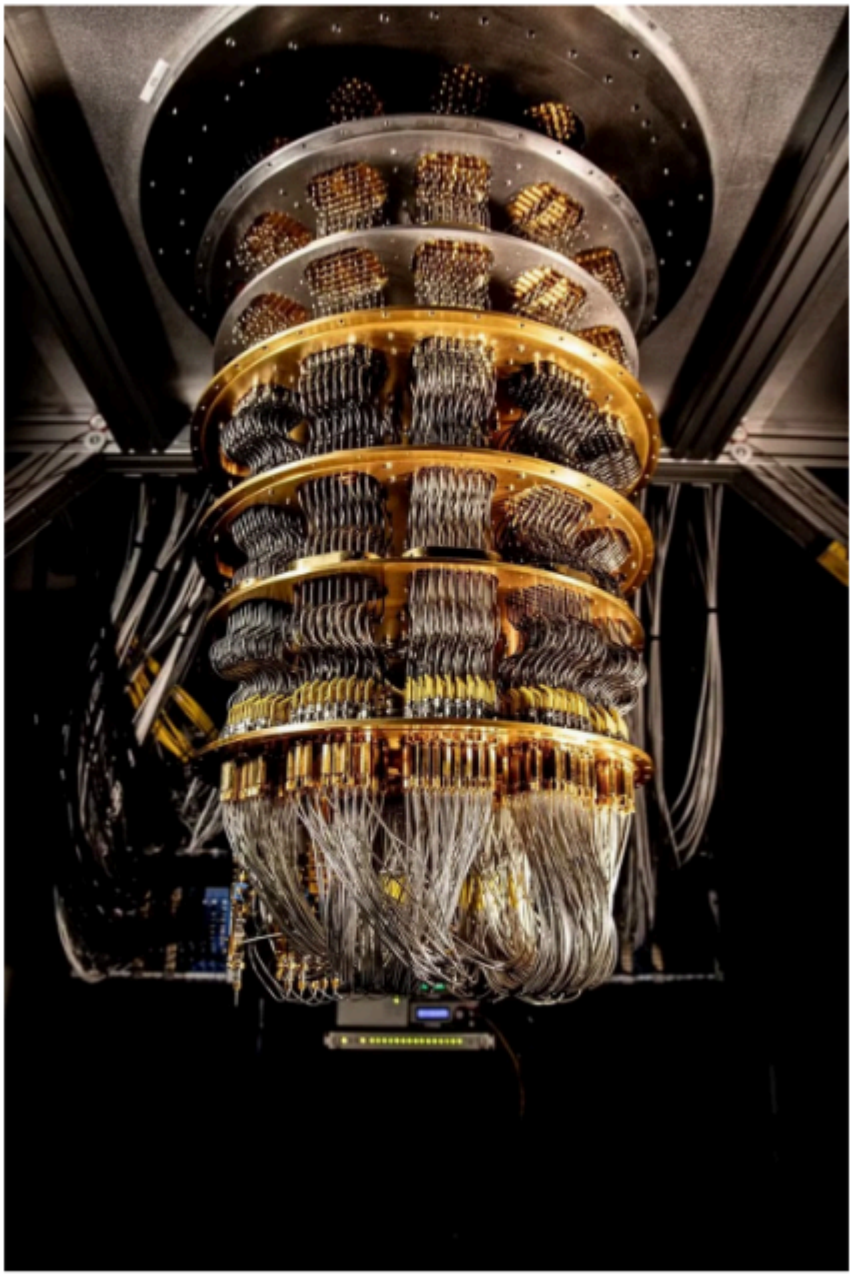
Segundo Bernhardt (2019), os principais conceitos por trás dos computadores quânticos são:

- **Qubits e superposição:** diferentemente do bit clássico (0 ou 1), o qubit pode assumir ambos os estados simultaneamente; um sistema de n qubits pode representar até 2^n combinações ao mesmo tempo.
- **Medição quântica:** quando um qubit é observado, a superposição desaparece e somente um resultado determinado é obtido, colapsando o estado quântico original. • **Emaranhamento e interferência:** estabelecem correlações entre qubits e permitem que amplitudes de probabilidade favoreçam resultados desejáveis, cancelando os indesejáveis.
- **Paralelismo quântico:** efeito direto da superposição, permite que vários estados sejam manipulados simultaneamente, resultando em múltiplos caminhos

computacionais explorados ao mesmo tempo.

- **Algoritmo de Shor:** proposto por Peter Shor em 1994, demonstra que um computador quântico suficientemente grande pode fatorar números inteiros em tempo polinomial, ameaçando diretamente a criptografia de chave pública (RSA, ECC).
- **Algoritmo de Grover:** reduz pela metade a segurança efetiva de chaves simétricas por meio de uma aceleração quadrática da busca exaustiva, sem quebrar diretamente algoritmos como o AES.

Figura 3 – Computador quântico supercondutor *Willow* e seu resfriador



Fonte: O Globo (2025).

A Figura 3 apresenta um dos principais avanços recentes da computação quântica.

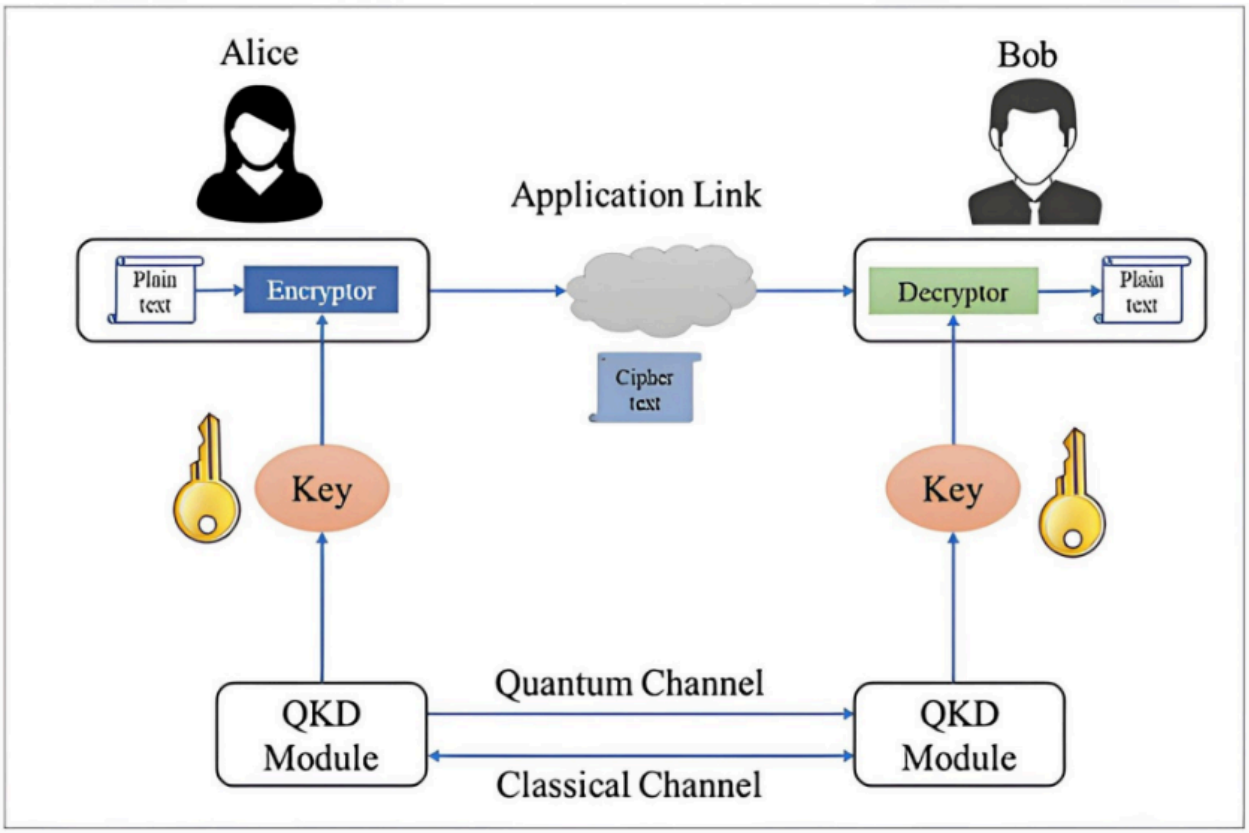
O computador quântico Willow demonstrou desempenho superior ao de supercomputadores clássicos em problemas computacionais específicos, evidenciando o potencial dessa tecnologia para determinadas classes de problemas. Diante desses avanços, cresce a preocupação com os impactos que computadores quânticos poderão causar.

2.3 Criptografia Pós-Quântica (PQC) e Distribuição Quântica de Chaves (QKD)

A Criptografia Pós-Quântica refere-se a algoritmos clássicos, executáveis na infraestrutura de TI atual, mas projetados para resistir a ataques de computadores clássicos e quânticos, fundamentados em estruturas matemáticas alternativas como reticulados algébricos, funções multivariadas e códigos lineares (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024). A segurança desses novos algoritmos depende de problemas matemáticos complexos, que os algoritmos quânticos conhecidos ainda não conseguem resolver de forma mais rápida, como o algoritmo de Shor faz com a fatoração. A padronização liderada pelo NIST consolidou dois algoritmos principais: o ML-KEM, derivado do *Kyber*, para encapsulamento de chaves, e o ML-DSA, para assinaturas digitais. Por serem compatíveis com a infraestrutura existente, esses algoritmos são a principal aposta para proteger sistemas operacionais, navegadores e protocolos de comunicação corporativos durante a transição pós-quântica (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024).

Já a Distribuição Quântica de Chaves (QKD) adota uma abordagem disruptiva, utilizando os princípios da física quântica – notadamente o Princípio da Incerteza de Heisenberg e o teorema da não clonagem – para garantir a confidencialidade na transmissão de chaves simétricas por meio de fótons de luz, transmitidos por canais de fibra óptica dedicados ou links de satélite (ELECTRONICS FOR YOU, 2024). O diferencial desta tecnologia reside na detecção imediata de intrusões: devido à natureza dos estados quânticos, qualquer tentativa de interceptação por parte de um agente malicioso altera as propriedades físicas dos fótons, alertando as partes antes do envio de dados sensíveis. Como ilustra a Figura 4, o arranjo envolve dois pontos legítimos de comunicação (Alice e Bob), interconectados por um canal quântico e um canal clássico de reconciliação.

Figura 4 – Arquitetura da Distribuição Quântica de Chaves (QKD)



Fonte: Adaptado de Electronics For You (2024).

3 Metodologia

Este estudo caracteriza-se como uma pesquisa teórica, qualitativa e exploratório-descritiva, desenvolvida por meio de revisão bibliográfica narrativa, com base em livros de referência, artigos científicos, relatórios técnicos e normas internacionais relacionados à segurança da informação, à criptografia clássica e pós-quântica e à computação quântica, priorizando fontes recentes e de reconhecida relevância acadêmica ou institucional.

A fundamentação sobre criptografia clássica e segurança de redes baseou-se principalmente nas obras *Cryptography and Network Security*, de Stallings (2017), e *History of Cryptography and Cryptanalysis*, de Dooley (2024), além do levantamento histórico apresentado por Singh (1999) sobre a evolução dos métodos de ocultação de informação desde a Antiguidade até a era digital. Os princípios de segurança da informação e seus pilares fundamentais foram embasados na norma ISO/IEC 27000 (ISO/IEC, 2014) e na obra *Security Engineering*, de Anderson (2020).

Para a fundamentação sobre computação quântica, foram utilizadas a obra *Quantum Computation and Quantum Information*, de Nielsen e Chuang (2010), referência clássica na área, e *Quantum Computing for Everyone*, de Bernhardt (2019),

empregada para a explicação didática de conceitos. Os marcos históricos da área foram sustentados pelos trabalhos de Feynman (1982) e Deutsch (1985), bem como pelo experimento de comprovação física de Vandersypen et al. (2001), referente à primeira fatoração experimental utilizando ressonância magnética nuclear. Quanto às ameaças e soluções emergentes, foram consultados os materiais técnicos disponibilizados pelo National Institute of Standards and Technology (2024), órgão responsável pela padronização mundial dos algoritmos de Criptografia Pós-Quântica, e o artigo de Mobilon e Rosolem (2024), que discute a evolução e as perspectivas de uso em larga escala da criptografia quântica e pós-quântica. Complementarmente, utilizou-se o relatório *Cost of a Data Breach Report*, da IBM (2024), para contextualização dos impactos econômicos das violações de dados, e a publicação técnica da Electronics For You (2024) para a descrição da arquitetura de Distribuição Quântica de Chaves (QKD).

4 Resultados e Discussão

4.1 Impactos sobre a Criptografia Atual

A ameaça que a computação quântica representa para os sistemas criptográficos atuais está ligada, sobretudo, à eficiência matemática dos algoritmos quânticos. Como destacado por Nielsen e Chuang (2010), a segurança clássica se apoia na complexidade computacional, já que determinados problemas matemáticos exigem recursos que crescem exponencialmente com o tamanho da chave. Para alguns desses problemas, os algoritmos quânticos reduzem drasticamente esse custo, o que compromete a base da segurança atual.

O impacto mais grave recai sobre a criptografia assimétrica de chave pública. Os sistemas baseados em RSA, cuja segurança é fundamentada na intratabilidade da fatoração de grandes inteiros, e os baseados em ECC, que dependem do problema do logaritmo discreto em curvas elípticas, tornam-se obsoletos sob a aplicação do Algoritmo de Shor (MOBILON; ROSOLEM, 2024). Na prática, uma chave RSA-2048, que demandaria bilhões de anos para ser decifrada por supercomputadores clássicos por meio de métodos de força bruta ou crivos matemáticos, poderia ter seus fatores primos encontrados por um computador quântico tolerante a falhas em questão de horas.

Já a criptografia simétrica e as funções de hash sofrem um impacto menos devastador. Como preconizado por Stallings (2017), a segurança do AES não contém estrutura matemática vulnerável ao Algoritmo de Shor, mas sofre degradação pelo

Algoritmo de Grover, que reduz pela metade o espaço de chave efetivo de um sistema simétrico. Consequentemente, o AES-128 passa a oferecer segurança equivalente a meros 64 bits no ambiente quântico, tornando-se suscetível a ataques, enquanto o AES-256 mantém um nível de segurança de 128 bits, patamar considerado computacionalmente seguro mesmo diante de capacidades quânticas (Tabela 1).

Tabela 1 – Impacto da computação quântica nos algoritmos criptográficos atuais

Algoritmo	Tipo	Impacto quântico
RSA / ECC	Assimétrico	Totalmente quebrado (Shor)
AES-128	Simétrico	Segurança reduzida a 64 bits (inseguro)
AES-256	Simétrico	Segurança reduzida a 128 bits (seguro)
SHA-256/3	Hash	Colisões mais rápidas

Fonte: Adaptado de National Institute of Standards and Technology (2024).

No ambiente corporativo, a quebra das técnicas assimétricas gera um efeito cascata na infraestrutura: protocolos fundamentais de comunicação segura na internet, como o Transport Layer Security (TLS/HTTPS), dependem da criptografia assimétrica para a etapa de troca de chaves e autenticação de identidade. Sem chaves públicas seguras, ficam comprometidos a integridade de assinaturas digitais e contratos eletrônicos e o sigilo dos dados em trânsito. Esse cenário também favorece ataques do tipo *Store Now, Decrypt Later* (armazene agora, decripte depois), nos quais agentes maliciosos capturam hoje o tráfego cifrado para decifrá-lo no futuro, quando houver computadores quânticos com capacidade suficiente.

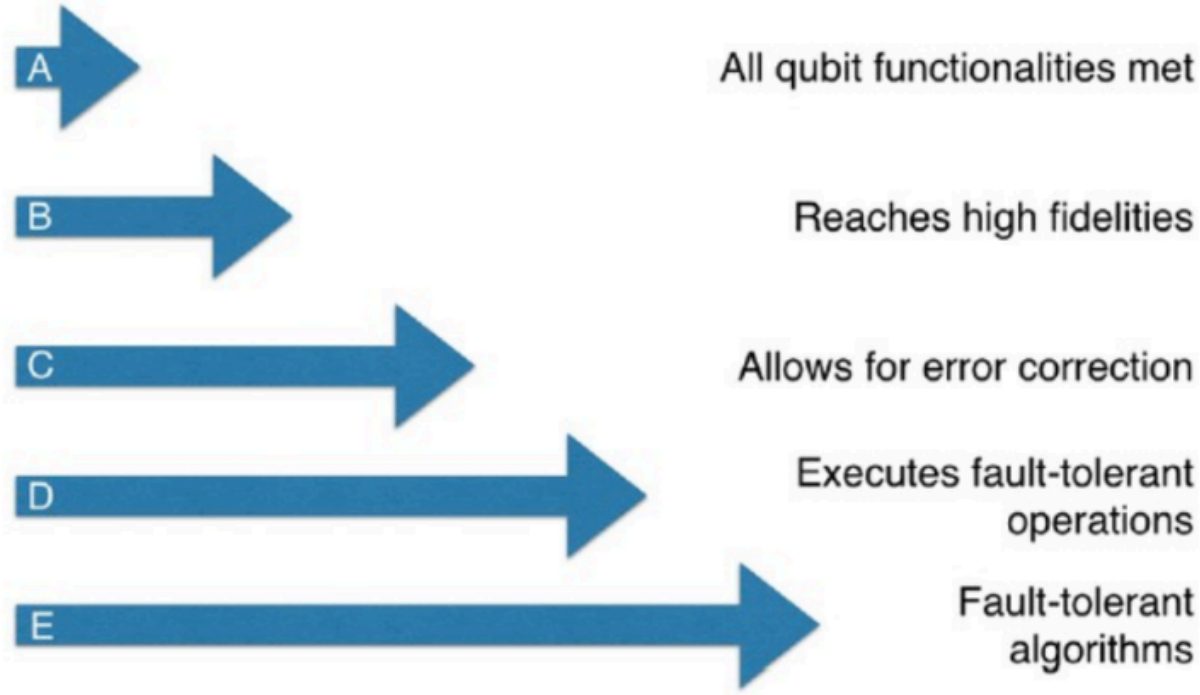
4.2 Estudos de Caso e Relatórios Técnicos

O trabalho do *Federal Office for Information Security* (BSI) cataloga estudos de caso e relatórios técnicos que evidenciam o avanço da computação quântica e seus impactos na segurança da informação. Ao longo de sucessivas edições, o estudo de Wilhelm et al. (2025) avalia a evolução das tecnologias de hardware e algoritmos quânticos, e o *Quantum Threat Timeline Report* do Global Risk Institute (MOSCA; PIANI, 2024) complementa essa análise consultando especialistas internacionais. Ambos indicam avanço constante rumo à relevância criptoanalítica.

O relatório do BSI introduziu um modelo de evolução para categorizar os níveis de maturidade dessas tecnologias, desde o cumprimento das funcionalidades básicas de um qubit até a execução de algoritmos plenamente tolerantes a falhas (Figura 5). Esse modelo evidencia que a maturidade de uma plataforma quântica não se resume à

quantidade de qubits disponíveis, mas também à qualidade das operações realizadas e à capacidade de correção de erros.

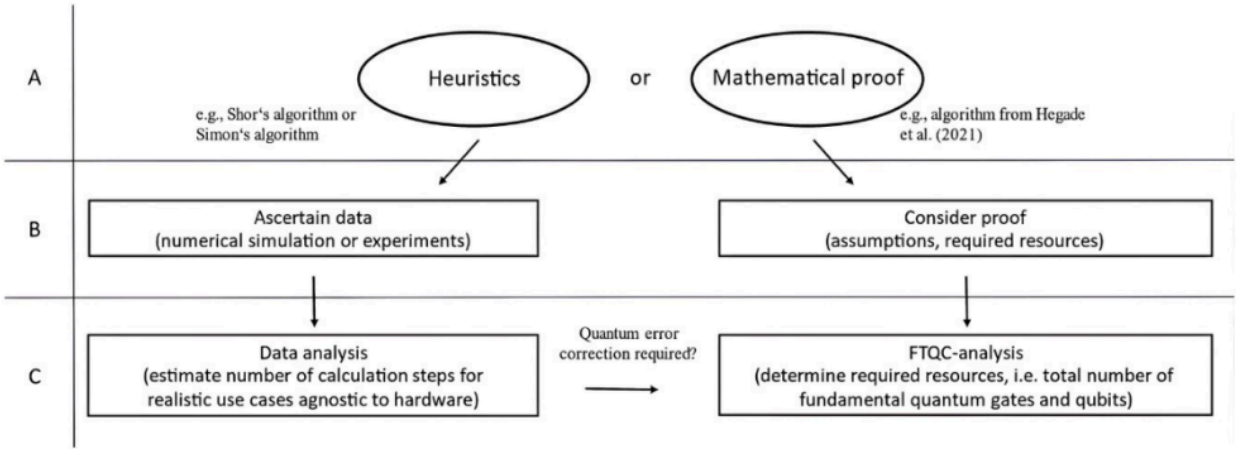
Figura 5 – Níveis de desenvolvimento para um computador quântico



Fonte: Adaptado de Federal Office for Information Security (2025).

Em sua segunda versão, o estudo aprofundou esse modelo para analisar o domínio dos algoritmos no paradigma NISQ (*Noisy Intermediate-Scale Quantum*), avaliando se cada algoritmo depende de heurísticas ou de provas matemáticas formais, e quais recursos de hardware – como correção de erros e tolerância a falhas – são necessários para sua execução (Figura 6).

Figura 6 – Esquema de avaliação para algoritmos quânticos: tolerante a falhas (direita) e NISQ (esquerda)

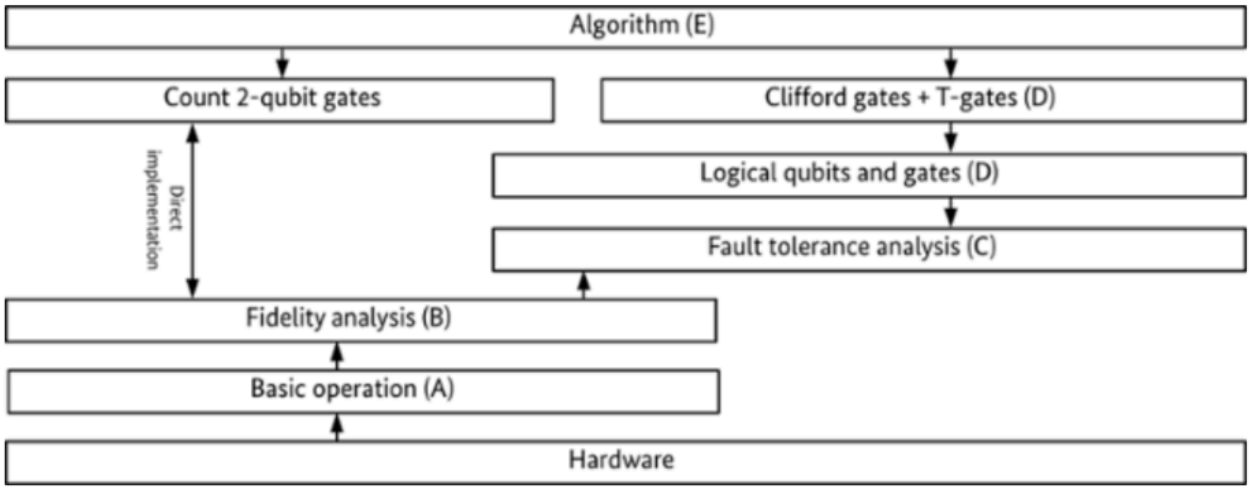


Fonte: Adaptado de Federal Office for Information Security (2025).

A Figura 7 ilustra o mapeamento de dependências entre algoritmos quânticos e as diferentes plataformas de hardware avaliadas nesses relatórios, evidenciando quais

combinações já demonstram maior maturidade tecnológica.

Figura 7 – Dependência entre algoritmos quânticos e plataformas de hardware



Fonte: Adaptado de Federal Office for Information Security (2025).

Em suas edições mais recentes, o estudo também avalia comparativamente as principais tecnologias físicas candidatas à construção de computadores quânticos tolerantes a falhas. Os resultados indicam um avanço constante da computação quântica, demonstrando a aplicabilidade do Algoritmo de Shor em sistemas tolerantes a falhas por meio de arquiteturas supercondutoras e de íons aprisionados.

4.3 Impactos e Prazos da Ameaça Quântica

Para parametrizar a urgência da migração, utiliza-se a Desigualdade de Mosca:

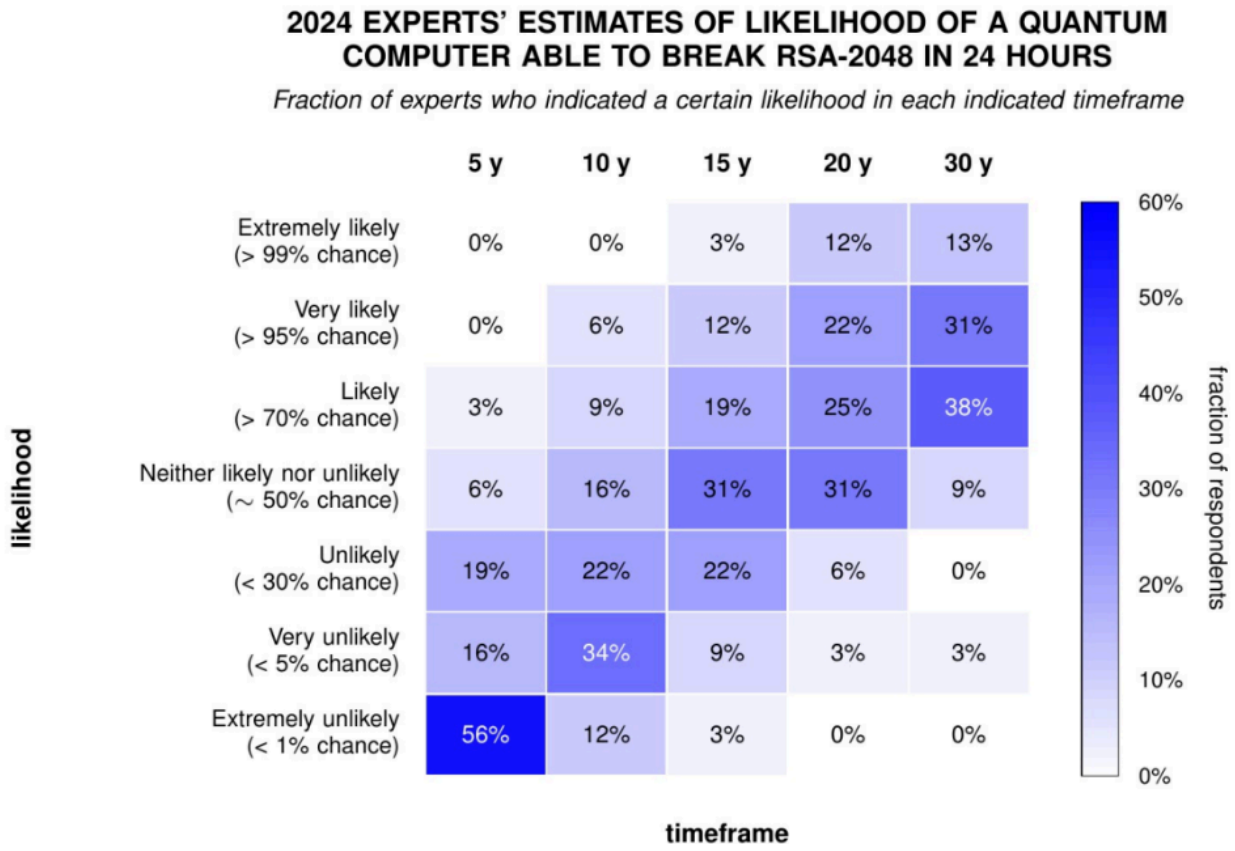
$$X + Y > Z \tag{3}$$

em que X é o tempo de sigilo exigido para os dados, Y o tempo necessário para a transição criptográfica e Z o tempo estimado até o surgimento de um computador quântico criptograficamente relevante. Por exemplo, para uma instituição que necessita de $X = 15$ anos de confidencialidade e $Y = 5$ anos de transição, uma estimativa $Z < 20$ anos já exige o início imediato da migração.

O *Quantum Threat Timeline Report* (MOSCA; PIANI, 2024) consultou especialistas internacionais para estimar a probabilidade de surgimento, em diferentes janelas temporais, de um computador quântico capaz de quebrar uma chave RSA-2048 em até 24 horas (Figura 8). A distribuição das respostas evidencia divergência entre especialistas quanto ao horizonte exato, mas convergência quanto à tendência de risco

crescente ao longo das próximas décadas, reforçando a necessidade de planejamento antecipado por parte das organizações.

Figura 8 – Distribuição das estimativas de probabilidade de especialistas



Fonte: Adaptado de Mosca e Piani (2024).

4.4 Avaliação Comparativa entre PQC e QKD

Embora PQC e QKD sejam frequentemente discutidas em conjunto, as duas abordagens atendem a necessidades e contextos diferentes, e compreender essa diferença é importante para os gestores de TI que precisam decidir qual caminho seguir. Para a maioria das organizações, a PQC tende a ser o caminho mais viável, pois seus algoritmos funcionam sobre a infraestrutura existente e a padronização do NIST oferece uma referência regulatória clara, embora exija chaves maiores e mais processamento. A QKD, por sua vez, tem a segurança garantida por princípios físicos e não é afetada por avanços computacionais futuros. No entanto, o custo da infraestrutura dedicada e as limitações de distância restringem seu uso a segmentos de alta criticidade, como instituições financeiras. As duas tecnologias tendem a se complementar, cada uma aplicada ao contexto em que é mais adequada.

4.5 Diretrizes para a Transição da Infraestrutura de TI

Dessa avaliação derivam três diretrizes práticas para a transição da infraestrutura de TI corporativa:

Mapeamento do inventário criptográfico. Identificar onde e como RSA, ECC e AES-128 são usados exige entender o papel de cada algoritmo em cada sistema. Uma assinatura digital em um contrato eletrônico, por exemplo, possui efeitos diferentes de uma chave usada para criptografar um banco de dados em repouso. É comum que esse levantamento revele criptografia obsoleta em sistemas legados que já não recebem manutenção, o que torna necessário um esforço inicial de documentação (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024).

Adoção de esquemas híbridos. A migração não deve ocorrer de uma só vez. Uma estratégia que vem ganhando espaço é a implementação de esquemas híbridos, nos quais um algoritmo clássico e um pós-quântico operam em paralelo durante o período de transição, como na combinação de ECDHE com ML-KEM no estabelecimento de sessões TLS (KWIATKOWSKI et al., 2026). Dessa forma, a comunicação continua protegida mesmo que uma das camadas seja comprometida, e as equipes técnicas podem se familiarizar com os novos algoritmos em um ambiente controlado.

***Crypto-agility* como princípio de projeto.** Migrações criptográficas tendem a ser custosas quando os algoritmos estão enraizados no código. A transição de RSA e ECC para os novos padrões pós-quânticos ilustra bem esse problema, pois sistemas que isolaram a lógica criptográfica desde o início enfrentam uma migração mais simples do que aqueles em que o algoritmo está espalhado por toda a base de código. Por isso, recomenda-se que novos sistemas sejam projetados com *crypto agility*, isto é, com a capacidade de substituir primitivas criptográficas causando o mínimo impacto na arquitetura. Para isso, a lógica criptográfica deve ficar concentrada em módulos que possam ser substituídos, o algoritmo utilizado deve ser definido por configuração, em vez de fixado no código, e devem ser evitadas dependências diretas de implementações específicas.

5 Conclusão

Este trabalho analisou os principais impactos que a computação quântica pode ter sobre a segurança de dados em ambientes corporativos, desde a demonstração das fraquezas da criptografia atual até a exemplificação de soluções emergentes, cumprindo

o objetivo geral estabelecido. Evidenciou-se que a criptografia simétrica e assimétrica é a base da segurança de informações atual, e que algoritmos quânticos, aliados a computadores quânticos especializados, poderiam quebrar os sistemas mais utilizados hoje.

A contribuição deste trabalho está no reconhecimento da computação quântica como uma tecnologia emergente com grande potencial para beneficiar a sociedade, mas que precisa ser cuidadosamente estudada e observada para que os possíveis riscos envolvendo seus usos indevidos sejam mitigados. Demonstrou-se como o uso combinado de algoritmos criptográficos pós quânticos e das diretrizes de transição propostas pode reduzir consideravelmente esses riscos.

Constatou-se também que não há uma solução única para a transição pós-quântica. PQC e QKD atendem a perfis de risco distintos, e a escolha entre uma delas, ou a combinação de ambas, depende do contexto de cada organização. As diretrizes propostas (mapeamento, hibridização e *crypto-agility*) se complementam e priorizam a redução de riscos, ainda que isso torne a implementação mais gradual. Assim, iniciar a transição o quanto antes tende a reduzir tanto os custos quanto os riscos envolvidos.

Para trabalhos futuros, propõe-se a realização de estudos comparativos entre a capacidade de defesa da criptografia pós-quântica e da criptografia atual frente a um computador quântico especializado, aprofundando a compreensão das diferenças de segurança entre os algoritmos.

Referências

ANDERSON, Ross. **Security engineering**: a guide to building dependable distributed systems. 3. ed. Indianapolis: Wiley, 2020. DOI: https://doi.org/10.1002/9781119644682.

BERNHARDT, Chris. **Quantum computing for everyone**. Cambridge, MA: MIT Press, 2019.

DEUTSCH, David. Quantum theory, the Church-Turing principle and the universal quantum computer. **Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences**, London, v. 400, n. 1818, p. 97-117, 1985. DOI: https://doi.org/10.1098/rspa.1985.0070.

DOOLEY, John F. **History of cryptography and cryptanalysis**: codes, ciphers, and their algorithms. 2. ed. Cham: Springer, 2024. DOI: https://doi.org/10.1007/978-3-031-67485-3.

ELECTRONICS FOR YOU. **Quantum key distribution**: the future of secure

communication. [*S. l.*], 2024. Disponível em: https://www.electronicsforu.com/technology-trends/quantum-key distribution-future-secure-communication. Acesso em: 9 jul. 2026.

FEDERAL OFFICE FOR INFORMATION SECURITY. **Entwicklungsstand Quantencomputer**. Bonn: BSI, 2025. Disponível em: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand Quantencomputer/entwicklungsstand-quantencomputer_node.html. Acesso em: 6 ago. 2026.

FEYNMAN, Richard P. Simulating physics with computers. **International Journal of Theoretical Physics**, [*S. l.*], v. 21, n. 6-7, p. 467-488, 1982. DOI: https://doi.org/10.1007/BF02650179.

IBM. **Cost of a data breach report 2024**. Armonk: IBM, 2024. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 25 maio 2026.

ISO/IEC. **ISO/IEC 27000**: information technology – security techniques – information security management systems – overview and vocabulary. Geneva: ISO, 2014. Disponível em: https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/c063411_ISO_IEC_27000_2014 .pdf. Acesso em: 1 jun. 2026.

KWIATKOWSKI, Kris et al. **Post-quantum hybrid ECDHE-MLKEM key agreement for TLSv1.3**. [*S. l.*]: IETF, 2026. Internet-Draft. Disponível em: https://datatracker.ietf.org/doc/draft ietf-tls-ecdhe-mlkem/. Acesso em: 19 ago. 2026.

MARCHIORI, Geuderson T. **A linguagem de Camaco**: identidade, memória e reexistência. Ouro Preto: UFOP, 2021. Disponível em: https://www.repositorio.ufop.br/items/12b03a34-5713- 40bc-8748-99c4f695f2fc. Acesso em: 16 jun. 2026.

MOBILON, Eduardo; ROSOLEM, João B. Criptografia quântica e pós-quântica: evolução e perspectivas de uso em larga escala. **Revista SBFoton**, [*S. l.*], 2024. Disponível em: https://revista.sbfoton.org.br/artigos/criptografia-quantica-e-pos-quantica-evolucao-e perspectivas-de-uso-em-larga-escala/. Acesso em: 11 jun. 2026.

MOSCA, Michele; PIANI, Marco. **Quantum threat timeline report 2024**. Toronto: Global Risk Institute, 2024. Disponível em: https://globalriskinstitute.org/publication/2024-quantum-threat timeline-report/. Acesso em: 6 ago. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Post-quantum cryptography**. Gaithersburg: NIST, 2024. Disponível em: https://www.nist.gov/pqcrypto. Acesso em: 25 maio 2026.

NIELSEN, Michael A.; CHUANG, Isaac L. **Quantum computation and quantum information**. 10th anniversary ed. Cambridge: Cambridge University Press, 2010. DOI: https://doi.org/10.1017/CBO9780511976667.

O GLOBO. Multiverso? Entenda visão dos cientistas sobre processador quântico do Google que permitiria acessar mundos paralelos. **O Globo**, Rio de Janeiro, 12 fev. 2025. Disponível em: https://oglobo.globo.com/economia/tecnologia/noticia/2025/02/12/multiverso-entenda-visao-dos cientistas-sobre-processador-quantico-do-google-que-permitiria-acessar-mundos-paralelos.ghtml. Acesso em: 29 set. 2026.

SINGH, Simon. **The code book**: the science of secrecy from ancient Egypt to quantum cryptography. New York: Anchor Books, 1999.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson, 2014.

STALLINGS, William. **Cryptography and network security**: principles and practice. 7. ed. Boston: Pearson, 2017.

VANDERSYPEN, Lieven M. K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. **Nature**, London, v. 414, p. 883-887, 2001. DOI: https://doi.org/10.1038/414883a.

WILHELM, Frank K. et al. **Status of quantum computer development**: version 2.2. Bonn: BSI, 2025. Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_2.html. Acesso em: 6 ago. 2026.