Segurança da Informação na Nuvem e Criptografia Pós-Quântica: Uma Revisão Bibliográfica

Alessandro Gabriel Pena Furtado[1], **Ana Karina D. S. de Oliveira**[2]

[1]Universidade Federal de Mato Grosso do Sul (UFMS)
Curso de Sistemas de Informação – Campo Grande, MS – Brasil

alessandro.furtado@ufms.br, ana.salina@ufms.br

Abstract. *The widespread adoption of cloud computing has transferred a security responsibility to users that is often underestimated. In the IaaS model, object storage repositories are exposed to misconfigurations, providers with access to stored content, and the threat of quantum computers capable of breaking the cryptographic algorithms currently in use. This work analyzes protection strategies for this environment in three layers. The first deals with confidentiality and access control via KP-ABE and PRE, techniques that allow the provider to operate on the data without ever seeing its content. The second addresses remote integrity verification through POR and PDP, which allow auditing the existence and completeness of files without needing to download them. The third examines post-quantum readiness, comparing the algorithms standardized by NIST with the QKD E91 protocol and the QuCloud hybrid framework, which combines both approaches to neutralize HNDL attacks. The analysis indicates that these techniques are not mutually exclusive: the choice between them depends on the risk profile of each organization, with sectors such as healthcare and government storing confidential data for decades, therefore they would have motivations to anticipate the post-quantum transition.*

Keywords: Cloud Computing, Object Storage, Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), Remote Integrity Auditing, Information Security.

Resumo. *A adoção massiva da computação em nuvem transferiu para os usuários uma responsabilidade de segurança que muitas vezes é subestimada. No modelo IaaS, os repositórios de armazenamento de objetos ficam expostos a configurações incorretas, a provedores com acesso ao conteúdo armazenado e à ameaça de computadores quânticos capazes de quebrar os algoritmos criptográficos em uso hoje. Este trabalho analisa estratégias de proteção para esse ambiente em três camadas. A primeira trata da confidencialidade e do controle de acesso via KP-ABE e PRE, técnicas que permitem ao provedor operar sobre os dados sem nunca enxergar seu conteúdo. A segunda aborda a verificação de integridade remota por meio de POR e PDP, que permitem auditar a existência e completude dos arquivos sem precisar baixá-los. A terceira examina a prontidão pós-quântica, comparando os algoritmos padronizados pelo NIST com o protocolo QKD E91 e o framework híbrido QuCloud, que combina ambas as abordagens para neutralizar o ataque HNDL. A análise indica que essas técnicas não são excludentes: a escolha entre elas depende do perfil de risco de*

cada organização, sendo que setores como saúde e governo armazenam dados sigilosos há décadas, portanto esses teriam motivações antecipar a transição pós-quântica.

Palavras-chave: Computação em Nuvem, *Buckets* de Armazenamento, Criptografia Pós-Quântica (PQC), Distribuição de Chaves Quânticas (QKD), Auditoria de Integridade (POR/PDP), Segurança da Informação.

1. Introdução

A adoção de sistemas baseados em nuvem tem demonstrado um crescimento exponencial nos últimos anos, impulsionada em grande parte pelo avanço da Inteligência Artificial (IA) e pela necessidade de infraestruturas que suportem o processamento em massa de dados. No cenário econômico atual, esse impacto é visível no valor de mercado de grandes provedores; um exemplo disso é a valorização recorde das ações da Oracle em 2025, motivada pela demanda por serviços de nuvem no setor de IA [1]. Além disso, observa-se que a computação em nuvem eliminou barreiras de entrada para pequenas e médias empresas, permitindo-lhes acessar recursos de supercomputação e armazenamento escaláveis a custos operacionais reduzidos. Embora o termo *Cloud Computing* possa sugerir uma inovação recente, o conceito de organizar a computação como um serviço público remonta à década de 1960. Conforme definido por [2], em uma perspectiva informal, a nuvem representa um passo à frente no acesso a serviços via internet, em que a gestão tecnológica é terceirizada em múltiplas dimensões e os recursos são disponibilizados por fornecedores de renome. Tecnicamente, essa estrutura é sustentada por uma rede global de *Data Centers*, que oferecem poder computacional sob demanda através de modelos de serviço conhecidos como IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) e SaaS (*Software as a Service*).

O paradigma da computação em nuvem fundamenta-se na oferta de recursos sem que a empresa precise investir em *hardware* próprio. De forma rigorosa, o modelo aceito pelo NIST [3] a define como um sistema que permite o acesso de qualquer lugar, conveniente e sob demanda a um pool compartilhado de recursos configuráveis, como redes, servidores e aplicações, que podem ser rapidamente provisionados com o mínimo esforço de gerenciamento.

Entretanto, as vantagens tecnológicas apresentadas na computação em nuvem trouxeram desafios críticos no âmbito da segurança da informação [4]. O aumento constante no número de ataques tem resultado em incidentes graves, que variam de vazamentos de dados proprietários a interrupções de serviços essenciais, gerando perdas financeiras substanciais. Nesse contexto, a proteção do ambiente de nuvem deixa de ser uma tarefa isolada para tornar-se uma responsabilidade compartilhada, exigindo um esforço combinado entre o provedor e o usuário, que deve garantir a segurança de suas aplicações e dados [5].

Este trabalho consiste em uma revisão bibliográfica que analisa estratégias de proteção para ambientes de armazenamento em nuvem, organizadas em três camadas progressivas de defesa: técnicas criptográficas clássicas avançadas para controle de acesso e auditoria de integridade; algoritmos de criptografia pós-quântica (PQC) padronizados pelo NIST; e arquiteturas híbridas que combinam PQC e Distribuição de Chaves Quânti-

cas (QKD) para neutralizar ataques do tipo *harvest-now, decrypt-later* (HNDL). O conhecimento consolidado destina-se a profissionais e estudantes de tecnologia que precisam de um mapa estruturado dessas técnicas, com análise de aplicabilidade e custo operacional para diferentes perfis de risco organizacional. Infraestruturas críticas como o sistema Pix e as urnas eletrônicas brasileiras já sinalizam que essa transição não pode ser reativa: dados protegidos hoje por algoritmos clássicos como RSA podem ser decifrados no futuro por adversários que os coletem agora e aguardem o amadurecimento das capacidades quânticas.

Para melhor fundamentação desse trabalho, seguimos a seguinte linha de pensamento: a seção 2 apresenta a metodologia adotada na seleção e organização das fontes consultadas; a seção 3 apresenta os trabalhos relacionados que fundamentam este estudo; a seção 4 apresenta uma revisão bibliográfica do Modelo do NIST; a seção 5 apresenta os Riscos e Desafios de Segurança na Nuvem; a seção 6 discute a segurança de longo prazo e a prontidão criptográfica pós-quântica; e a seção 7 fará a análise comparativa entre os algoritmos e técnicas mencionados, a aplicabilidade e o custo operacional dos mesmos.

2. Metodologia

Este trabalho foi desenvolvido a partir de uma abordagem qualitativa e exploratória, estruturado por meio de um mapeamento crítico da literatura. O objetivo central consistiu em identificar, analisar e sintetizar as principais técnicas de segurança aplicáveis ao armazenamento de dados em nuvem, traçando uma linha evolutiva que parte da criptografia clássica até alcançar as abordagens pós-quânticas contemporâneas.

A seleção das fontes foi conduzida a partir de três bases de dados primárias: a *IEEE Xplore Digital Library*, para artigos de conferências e periódicos de engenharia elétrica e ciência da computação, englobando estudos sobre controle de acesso e auditoria pública na nuvem [6, 7]; a *ACM Digital Library*, para publicações em segurança e criptografia aplicada, incluindo trabalhos fundamentais sobre provas de recuperabilidade de arquivos e complexidade de problemas em reticulados [8, 9, 10]; e o portal *MDPI*, para artigos de acesso aberto em computação e segurança da informação, com foco na integração de esquemas de autenticação pós-quântica [11].

Complementarmente, foram consultadas publicações oficiais do *National Institute of Standards and Technology* (NIST), contemplando as definições de arquitetura de nuvem e as diretrizes para a padronização da criptografia pós-quântica [3, 12, 13, 14]; da *Elsevier* — por meio do periódico *Journal of Information Security and Applications* — para a análise de segurança avançada em armazenamento em nuvem [15]; e de editoras de referência em computação teórica e engenharia [2, 4, 16].

No âmbito nacional, integraram-se os anais da Sociedade Brasileira de Computação (SBC) para avaliar bibliotecas criptográficas aplicadas ao cenário eleitoral [17], além de fontes institucionais nacionais, como comunicados oficiais da ABIN sobre segurança institucional [18] e relatórios do Banco Central do Brasil, especificamente focados na viabilidade de algoritmos pós-quânticos no sistema de pagamentos instantâneos [19].

Por fim, marcos regulatórios de proteção de dados [20, 21], documentações técnicas de plataformas de desenvolvimento e provedores de nuvem [22, 23, 24, 25, 26, 27, 28, 29, 30], bem como fontes de mídia especializada e guias setoriais [1, 5, 31, 32, 33, 34], fo-

ram utilizados exclusivamente para contextualização de mercado, arquitetura tecnológica e motivação da pesquisa.

O ponto de partida consistiu na explicação de conceitos como a computação em nuvem com base nas definições do modelo NIST. A partir disso, o mapeamento avançou para o exame de técnicas criptográficas clássicas e avançadas voltadas à proteção de repositórios de objetos (*buckets*). Nessa etapa, priorizou-se o controle de acesso granular via criptografia baseada em atributos (KP-ABE) e recriptografia por procuração (PRE) — conforme visto em [6] —, além de mecanismos que atestam a integridade e a disponibilidade dos dados remotamente, como os esquemas de Provas de Possessão de Dados (PDP) e Provas de Retreabilidade (PORs) [8, 7].

O escopo da pesquisa estendeu-se para a transição tecnológica imposta pela ameaça quântica. Logo, foram analisados os algoritmos finalistas do processo de padronização PQC conduzido pelo NIST [14, 11]. Por fim, a investigação alcançou o estado da arte na camada de aplicação ao avaliar arquiteturas híbridas de segurança, com foco central no recém-proposto *framework* QuCloud [15], que integra Criptografia Pós-Quântica e Distribuição de Chaves Quânticas (QKD).

Além da conceituação técnica, o estudo também buscou informações tanto na mídia como um todo, como sobre as reações do mercado frente ao surgimento dessas novas tecnologias. Esses dados auxiliaram na motivação da pesquisa, incorporando reportagens sobre a valorização de provedores impulsionada pela demanda de IA [1], levantamentos sobre a divisão de mercado em IaaS [31, 32] e guias setoriais de ferramentas de segurança [5]. Em complemento, tivemos fontes institucionais brasileiras [18, 35] que permitiram situar a aplicação prática dessas tecnologias no cenário nacional, discussão posteriormente aprofundada na Seção 6. A partir de todas essas análises, foi possível estabelecer comparações sobre as abordagens apresentadas, o custo operacional diante de sua eventual aplicação e o mapeamento dessas tecnologias e técnicas, que foram discutidas, no mercado como um todo.

3. Trabalhos relacionados

3.1. Mecanismos de Controle de Acesso Avançado e Confidencialidade de Dados

Os servidores da nuvem estão fora do domínio de confiança do usuário, dessa forma, algumas abordagens como a demonstrada por [6] auxiliam a manter a confidencialidade dos dados, de início assume-se um sistema composto por um *Data Owner*, muitos consumidores de dados, muitos servidores de nuvem e um auditor terceirizado, também assume-se que os canais de comunicação entre o proprietário dos dados/usuários e os Servidores de Nuvem estão protegidos sob protocolos de segurança existentes, como o SSL, o artigo de [6] não cita o TLS, mas o mesmo pode ser incluso nessa análise, pois assim com o SSL, o TLS sofreria do mesmo problema. Apesar dessa organização, considera-se que o provedor de nuvem é "honesto, mas curioso". Isso quer dizer que os servidores de nuvem seguirão, de maneira geral, o protocolo proposto, mas tentarão descobrir o máximo possível de informações secretas com base em suas entradas, estando mais interessados no conteúdo dos arquivos armazenados e nas informações de privilégios de acesso dos usuários.

A KP-ABE (criptografia baseada em atributos de política de chave) é uma criptografia de chave pública voltada para a comunicação de um para muitos. Ela é criada

pelo proprietário dos dados antes de ele enviá-los à nuvem. Os dados são associados a atributos e, para cada um deles, define-se um comportamento de chave pública. Cada usuário receberá uma estrutura de acesso, definida como uma árvore de acessos, em que os nós-folha estarão associados aos atributos e os nós internos às portas lógicas de limiar (*Threshold gates*). O usuário só conseguirá decifrar o texto cifrado se os atributos do arquivo satisfizerem a sua árvore de acesso. A KP-ABE é composta por quatro algoritmos, sendo esses:

Setup: O *Data Owner* escolhe o nível de segurança (parâmetro K) que servirá de base para criar o ambiente criptográfico; em seguida, define o conjunto de atributos que podem ser usados para descrever os dados no sistema. Com base nesses 'inputs' iniciais, o algoritmo de *setup* define uma *master key* e uma *public key*, que serão utilizadas em todo o sistema. A *public key* é enviada para os servidores de nuvem e é utilizada para consultas e execução, já a *master key* fica restrita ao *Data Owner* e é utilizada para criação de novos usuários e revogação de acessos, vale ressaltar que durante essa configuração inicial o *Data Owner* define o atributo Dummy, atributo fictício, esse incluido em todos os arquivos e chaves de usuário, servindo para a nuvem ajudar na atualização de chaves sem precisar descriptografar os dados sozinha.

Encryption: Após a configuração do sistema, o proprietário deseja subir um arquivo para seu sistema em nuvem, para isso ele utiliza uma criptografia híbrida, sendo o arquivo trancado por uma chave simétrica rápida (DEK), o algoritmo de Encryption tem como objetivo proteger essa chave, para isso o proprietário escolhe quais atributos esse arquivo possui e usa a PK para cifrar a DEK com eles. Portanto, o arquivo vai para a nuvem com uma identificação de quais atributos são necessários para abri-lo, porém o conteúdo real permanece ilegível para o servidor curioso.

Key Generation: Quando um novo usuário ingressa no sistema, o *Data Owner* define para ele uma estrutura de acesso personalizada, representada por uma árvore de decisão. Utilizando a *Master Key*, o algoritmo distribui segredos matemáticos por meio dessa árvore, do topo para a base, gerando componentes de chave secreta para cada atributo nas folhas. Uma característica vital para a escalabilidade deste modelo é que o *Data Owner* envia aos servidores na nuvem quase todos os componentes da chave secreta do usuário, exceto a parte correspondente ao atributo Dummy, que é entregue de forma privada apenas ao usuário. Dessa forma, o servidor consegue armazenar e atualizar essas chaves durante processos de revogação de outros usuários, mas nunca possui a chave completa necessária para realizar a descriptografia por conta própria.

Decryption: Esta fase é executada pelo usuário ao baixar um arquivo da nuvem para acesso. O algoritmo realiza o processo inverso da criptografia: utiliza o mapa bilinear para combinar os componentes da chave secreta do usuário com as chaves de atributos presentes no cabeçalho do arquivo. Por meio de uma técnica de interpolação polinomial, os resultados são agregados da base até o topo da árvore de acesso. Se os atributos do arquivo satisfizerem as condições lógicas da árvore do usuário, o "fator cego"que protege a chave simétrica é removido, permitindo a recuperação da DEK. Com a DEK liberada, o usuário consegue finalmente descriptografar o corpo do arquivo e acessar o conteúdo original

A Figura 1 ilustra como esse mecanismo funciona na prática. À esquerda, o pro-

prietário dos dados associa ao arquivo um conjunto de atributos descritivos: no exemplo, informações clínicas como doença (*Illness: diabetes*), hospital (*Hospital: A*), raça (*Race: asian*) e o atributo fictício *Dummy*. Esse arquivo cifrado é então enviado para os servidores de nuvem (seta superior). À direita, a estrutura de acesso do usuário é representada como uma árvore de decisão: o nó raiz impõe a condição `AND`, exigindo que dois ramos sejam satisfeitos simultaneamente. O ramo da esquerda exige os atributos *Illness: diabetes* e *Hospital: A*; o ramo da direita, outro `AND` com um `OR` aninhado, aceita tanto *Race: asian* quanto *Race: white*, além de um atributo fictício (*dummy attribute*). O usuário só consegue decifrar o conteúdo se os atributos que possui satisfazem todas as condições lógicas da árvore, de cima a baixo.

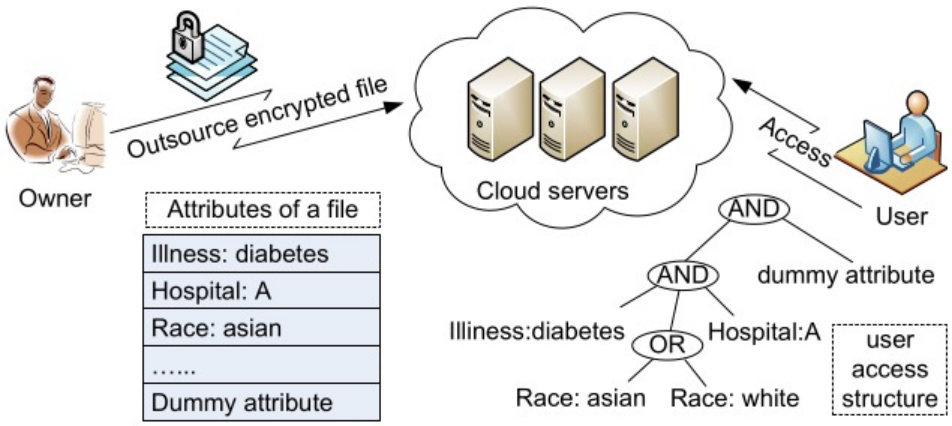

Figura 1. Esquema KP-ABE aplicado ao armazenamento em nuvem: o proprietário envia o arquivo cifrado com seus atributos descritivos para os servidores (esquerda); o usuário acessa o conteúdo apenas se seus atributos satisfizerem a estrutura de acesso em árvore (direita), onde nós internos representam portas lógicas (`AND`/`OR`) e folhas representam os atributos exigidos.

Fonte: [6].

O atributo *Dummy*, visível tanto na lista de atributos do arquivo quanto na árvore do usuário, desempenha um papel técnico central: como detalhado no algoritmo *Key Generation*, ele é a peça que o *Data Owner* retém para si e não entrega à nuvem, impedindo que o servidor, mesmo armazenando quase toda a chave do usuário, consiga realizar a descriptografia de forma autônoma.

Para viabilizar a sustentabilidade e a eficiência desse gerenciamento de chaves na nuvem, integram-se os mecanismos de PRE (*Proxy Re-Encryption*) e de *Lazy Re-Encryption*. O PRE permite que a nuvem altere o texto cifrado para uma nova versão atualizada, sem que o servidor consiga ler o conteúdo original. Já a estratégia de *Lazy Re-Encryption* adia a recriptografia real até que um novo dado seja postado ou modificado no sistema, economizando significativamente tempo de processamento. Ambas as operações são delegadas à nuvem, poupando o Data Owner do trabalho manual.

3.2. Verificação de Integridade e Auditoria de Dados por Entidades Terceiras

Como sistemas baseados em nuvem dependem de um provedor externo para o armazenamento dos dados, algumas técnicas visando manter a integridade, confidencialidade

e disponibilidade dos dados foram desenvolvidas, na subseção anterior foi visto como criptografias baseadas em atributos KP-ABE são úteis para manter a confidencialidade dos dados frente ao provedor, agora com as técnicas de POR e PDP, podemos assegurar a integridade dos dados e sua disponibilidade, além de sua confidencialidade frente às técnicas de auditoria de dados.

PORs (*Proofs of Retrievability for Large Files*) é descrito no artigo de Juels e Kalist [8], Essa técnica permite que um verificador, *Data Owner*, determine se um arquivo ou objeto de dados está em posse do provador, que seria O serviço de armazenamento desse arquivo, para ser feita essa constatação o Verificador utiliza sentinelas, que seria uma técnica utilizada para manter a integridade e a disponibilidade do arquivo armazenado, impedindo que o provador delete este, visando maior espaço de armazenamento. A Figura 2 resume a arquitetura do protocolo. O arquivo original F entra em um par de módulos: o *key generator* produz a chave de verificação K, que fica exclusivamente com o Verificador/Usuário (lado esquerdo); o *file encoder* gera a versão protegida $\tilde{F}$, que é enviada e mantida pelo Provador/Arquivo (lado direito), representando o serviço de armazenamento em nuvem. A auditoria acontece pelo protocolo de desafio-resposta indicado pelas setas centrais: o Verificador envia um desafio c apontando posições aleatórias no arquivo armazenado, e o Provador deve responder com r, os valores dos blocos naquelas posições, que incluem as sentinelas embutidas durante a codificação. Se qualquer bloco tiver sido deletado para economizar espaço, a chance de o Provador falhar ao revelar uma sentinela solicitada cresce a cada rodada, tornando a fraude estatisticamente detectável sem que o Verificador precise baixar o arquivo inteiro.

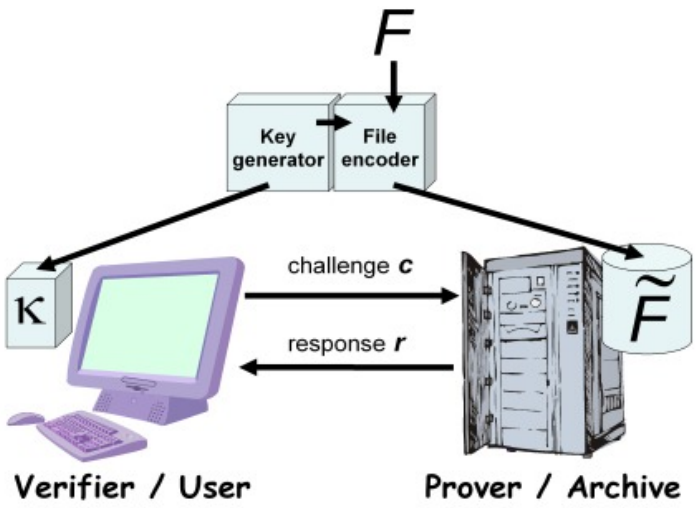

Figura 2. Arquitetura do protocolo POR: o arquivo F é processado em dois módulos que geram a chave de verificação K (retida pelo Verificador/Usuário) e a versão codificada $\tilde{F}$ (armazenada no Provador/Arquivo). A posse dos dados é auditada pelo par desafio c / resposta r, sem que o arquivo completo precise ser recuperado.

Fonte: [8].

Com essa arquitetura em mente, o funcionamento interno do protocolo torna-se mais claro: cada elemento do diagrama corresponde a uma etapa concreta do pipeline

de preparação do arquivo, descrita a seguir. De forma mais detalhada o arquivo original que será armazenado é subdividido em blocos conhecidos como *"Chunks"* (pedaços), aplica-se uma primeira camada de proteção na forma de um código de correção (ECC), o arquivo é criptografado, além de auxiliar na confidencialidade, a criptografia faz com que os blocos de dados sejam indistinguíveis dos blocos de sentinelas, por meio de permutação pseudoaleatória, todos os blocos de arquivos são "embaralhados"aleatoriamente, impedindo que o provedor saiba quais blocos são sentinelas; sem isso, o provedor poderia identificar e proteger apenas as sentinelas. As sentinelas são pequenos blocos de verificação inseridos em uma pequena fração do arquivo total, elas testam a disponibilidade do arquivo, o verificador desafia o provedor a revelar os valores de sentinelas em posições específicas, se o provedor deletou uma parte substancial do arquivo para economizar espaço, ele terá apagado alguma sentinela, falhando assim no desafio.

Para além da verificação realizada pelo *Data Owner*, como demonstrado na técnica de PORs, Wang ([7]) propõe o modelo PDP (Provable Data Possession), que se concentra na auditoria pública, permitindo que uma entidade externa verifique a integridade dos dados sem que o usuário precise estar online nem possuir uma cópia local do arquivo.

A Figura 3 apresenta os três atores do modelo e os fluxos que os conectam. Os **Usuários** (lado esquerdo), com seus diferentes dispositivos, interagem com o **Provedor de Serviço em Nuvem** (*Cloud Service Provider*, lado direito) por meio de um *Data Flow* bidirecional direto, que representa o tráfego normal de envio e recuperação de dados. Em paralelo, o **Auditor Terceirizado** (*Third Party Auditor*, centro superior) atua como intermediário de confiança: ele troca mensagens de segurança (*Security Message Flow*, setas tracejadas) tanto com os usuários quanto com o provedor, mas nunca participa do fluxo de dados em si. Essa separação é a propriedade central do modelo: o TPA pode desafiar o provedor e validar as respostas sem jamais ter acesso ao conteúdo real armazenado, o que é viabilizado pelos autenticadores homomórficos e pelo mascaramento aleatório descritos a seguir.

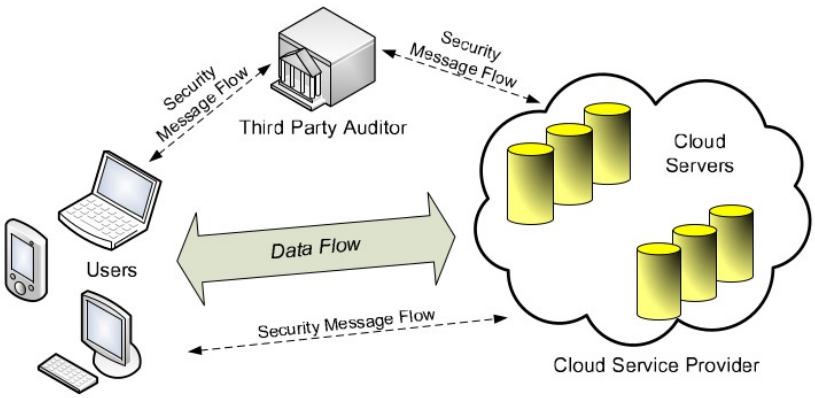

Figura 3. Modelo PDP com auditoria pública e preservação de privacidade: o fluxo de dados (*Data Flow*) permanece direto entre usuários e o Provedor de Nuvem, enquanto o Auditor Terceirizado (TPA) opera exclusivamente via fluxos de mensagens de segurança (*Security Message Flow*), validando a integridade dos dados sem acesso ao conteúdo em claro.

Fonte: [7].

Para que o TPA consiga cumprir esse papel sem comprometer a privacidade dos dados, os esquemas convencionais de PDP precisam ser aprimorados: Wang et al. identificam uma falha crítica neles e propõem a solução descrita a seguir. Os esquemas de PDP convencionais apresentam falhas que se evidenciam na exposição de combinações lineares de blocos ao auditor, permitindo que ele reconstrua o conteúdo original dos dados ao resolver sistemas de equações lineares. Contrapondo-se a técnicas convencionais Wang propõe a auditoria pública com a preservação de privacidade, que utiliza autenticadores homomórficos baseados em chave pública integrados a uma técnica de mascaramento aleatório (Random Mask), fazendo com que o servidor de nuvem utilize uma função pseudoaleatória para blindar a combinação linear dos blocos antes de enviá-la para a verificação dessa forma o auditor terceirizado (TPA) consegue validar a integridade dos dados por meio de propriedades bilineares sem nunca ter acesso à informação real ou às peças necessárias para derivar o conteúdo.

4. Modelo NIST

Desde o início, o conceito de computação em nuvem foi definido de diferentes maneiras por diferentes grupos de regulamentação, como o NIST (*National Institute of Standards and Technology*) [3], a ISO (*International Organization for Standardization*) [36], o ETSI (*European Telecommunications Standards Institute*) [37] e a CSA (*Cloud Security Alliance*) [38]. Dentre esses, destacou-se o NIST [3]. Sua definição de Computação em Nuvem é proposta através de cinco atributos essenciais, os quais incluem: Amplo Acesso à Rede, Elasticidade Rápida, Serviço Mensurável, Autosserviço Sob Demanda e Agrupamento de Recursos; três modelos de serviço, compostos por IaaS, PaaS e SaaS; e quatro modelos de implantação, sendo estes Nuvem Pública, Nuvem Privada, Nuvem Híbrida e Nuvem Comunitária, conforme apresentado na Figura 4.

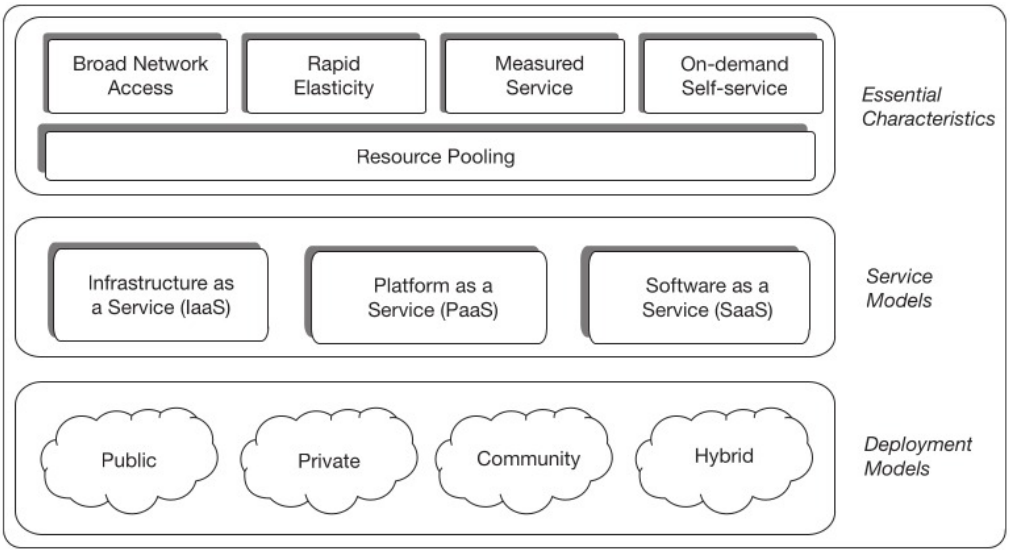

Figura 4. Modelo conceitual do NIST.
Fonte: NIST [3].

4.1. Características Essenciais

4.1.1. Amplo acesso à rede

A computação em nuvem possibilita que seus usuários tenham acesso aos seus serviços através da rede, não necessitando que o utilizador disponha de uma infraestrutura local de *data centers*. Como a infraestrutura física permanece sob a posse e gestão do provedor, é requerido apenas que o usuário possua conectividade com a rede de comunicação para usufruir dos recursos [2].

4.1.2. Elasticidade Rápida

Alguns sistemas computacionais podem sofrer mudanças bruscas no volume de requisições. A rápida elasticidade é a característica que permite que o sistema ajuste a capacidade computacional para cima ou para baixo de maneira dinâmica, a depender da demanda instantânea, com o objetivo de utilizar os recursos disponíveis da forma mais eficiente possível. Vale ressaltar que esse escalonamento segue diretrizes e políticas impostas pelo administrador do sistema, garantindo que o consumo de recursos permaneça dentro dos limites previstos [2].

4.1.3. Serviço Mensurável

O serviço mensurável assegura o controle e a otimização automática de recursos por meio de recursos de medição e monitoramento quantitativo. Essa medição ocorre em níveis de abstração adequados ao tipo de serviço (como volume de armazenamento, largura de banda ou poder de processamento), servindo de base para o faturamento e entrega automatizada no modelo *pay-per-use* (pagamento pelo uso), garantindo transparência por meio de relatórios detalhados de consumo tanto para provedores quanto para usuários [2].

4.1.4. Autosserviço Sob Demanda

O autosserviço sob demanda possibilita ao utilizador provisionar recursos computacionais, de forma unilateral e interativa, conforme a necessidade do sistema. Desse modo, a alocação de tempo de servidor ou armazenamento em rede é realizada de maneira automatizada, prescindindo de interação humana direta com o provedor do serviço [2].

4.1.5. Agrupamento de Recursos

Os recursos computacionais do provedor são agrupados em um modelo multiusuário (*multi-tenant*) para servir a múltiplos consumidores de forma dinâmica, onde diferentes recursos físicos e virtuais são atribuídos e realocados conforme a demanda. Sob essa perspectiva, o consumidor geralmente não possui controle ou conhecimento sobre a localização geográfica exata dos recursos fornecidos, possuindo apenas a especificação de termos mais amplos como o país ou a região de hospedagem [2].

4.2. Modelos de Implantação

Os modelos de implantação definidos pelo NIST são categorizados de acordo com o escopo de acesso, governança e a localização física ou lógica dos ativos de infraestrutura. Essa classificação estabelece limites claros sobre quem possui a propriedade dos recursos e como os perímetros de segurança são gerenciados [12].

4.2.1. Nuvem Pública

Nuvens públicas são aquelas em que recursos como servidores, armazenamento e redes são oferecidos por um provedor de serviço terceirizado. Nesse caso, observam-se vantagens como a ausência da necessidade de investir em recursos próprios de *hardware*, maior flexibilidade na administração de recursos, escalabilidade e acesso global por meio da rede. No entanto, o modelo apresenta algumas desvantagens, como a dependência do provedor, o aprisionamento tecnológico (*vendor lock-in*) e questões complexas de segurança [2].

Como apresentado na Figura 5, a infraestrutura da nuvem pública está localizada inteiramente no domínio do provedor (*Provider's Premises*). De acordo com o modelo de referência do NIST, os recursos computacionais são compartilhados de forma multiusuário e disponibilizados de maneira aberta para o público geral por meio da internet [12].

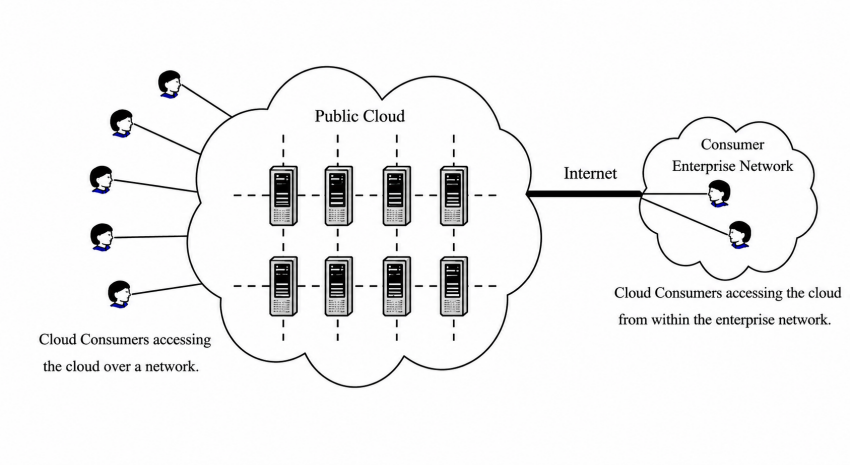

Figura 5. Arquitetura estrutural de uma Nuvem Pública.
Fonte: NIST [12, p. 20].

4.2.2. Nuvem Privada

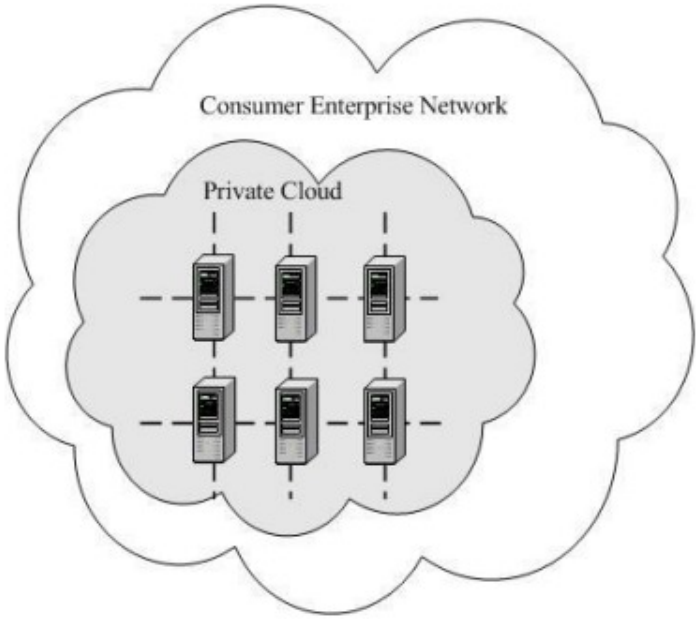

Figura 6. Arquitetura de uma Nuvem Privada local (*On-site*).
Fonte: NIST [12, p. 20].

As nuvens privadas ocorrem quando as organizações investem em toda uma estrutura dedicada de *hardware*, o que pode gerar altos custos de capital e operacionais para manter essa infraestrutura. Entretanto, a principal vantagem reside no maior nível de controle e na segurança dos dados, visto que os recursos computacionais são exclusivos daquela organização Segundo as especificações do NIST, na modalidade local (*On-site Private Cloud*),

exibida na Figura 6, a infraestrutura é implementada e operada estritamente dentro do perímetro físico e da rede local da própria organização consumidora (*Consumer's Premises*) [12]. O NIST prevê ainda uma variante terceirizada (*Outsourced Private Cloud*), hospedada nas instalações de um provedor externo, com isolamento lógico mantido por meio de redes privadas dedicadas (*Enterprise Network*) [12].

4.2.3. Nuvem Comunitária

A nuvem comunitária é um modelo de implantação organizado para servir a um grupo ou organizações que possuem interesses e preocupações em comum. Esses interesses compartilhados geralmente envolvem requisitos estritos de segurança, missões de negócio, políticas institucionais ou considerações de conformidade regulatória [2].

Com base no documento de arquitetura do NIST, na modalidade local (*On-site Community Cloud*), demonstrada na Figura 7, a infraestrutura é implantada nas dependências de uma ou mais organizações participantes do consórcio, que atuam provendo e gerenciando os recursos de nuvem locais para os demais membros autorizados [12]. O NIST prevê ainda uma variação terceirizada (*Outsourced Community Cloud*), em que os servidores são transferidos para o domínio de um provedor externo, mantendo acesso e governança restritos ao grupo comunitário por meio de canais de comunicação seguros isolados dos clientes públicos ordinários [12].

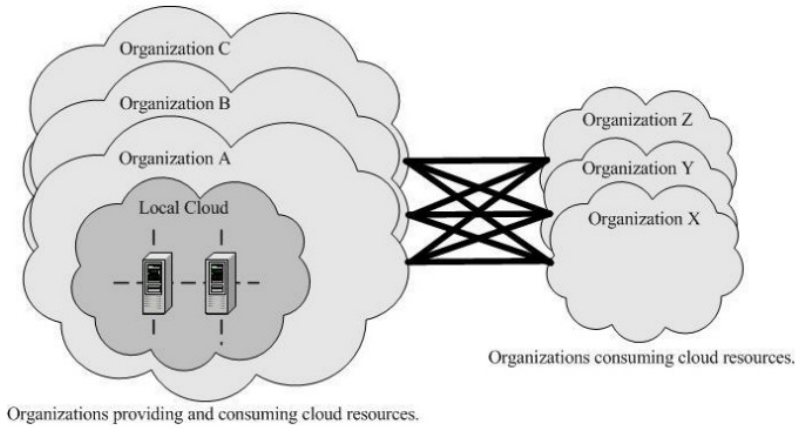

Figura 7. Arquitetura de uma Nuvem Comunitária local (*On-site*).
Fonte: NIST [12, p. 21].

4.2.4. Nuvem Híbrida

A nuvem híbrida consiste na combinação e orquestração das abordagens pública e privada, permitindo que as empresas aproveitem os benefícios de ambas as arquiteturas. Ela possibilita, por exemplo, manter dados altamente sensíveis em um ambiente privado e controlado, enquanto utiliza a nuvem pública para demandas menos críticas ou para absorver picos de escalabilidade adicional. Essa abordagem mitiga custos e eleva a flexibilidade, embora exija uma complexidade significativamente maior na gestão e na integração dos ambientes [2].

Como ilustrado na Figura 8, as diretrizes do NIST definem que a nuvem híbrida opera através da composição e federação de duas ou mais infraestruturas de nuvens distintas (públicas, privadas ou comunitárias). Esses ambientes mantêm suas identidades e características únicas originais, contudo, permanecem interligados por meio de tecnologias padronizadas ou proprietárias que viabilizam a portabilidade e a sincronização segura de dados e aplicações entre as fronteiras das nuvens [12].

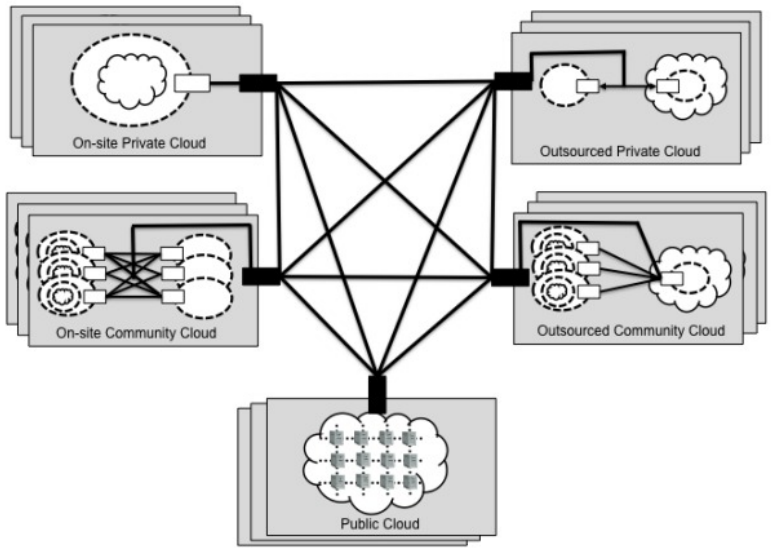

Figura 8. Modelo de federação e composição de uma Nuvem Híbrida.
Fonte: NIST [12, p. 22].

4.3. Modelos de Serviço

Como se observa na Figura 9, os modelos de serviço dividem as responsabilidades de gerenciamento do ambiente de forma hierárquica, mapeando as principais soluções de mercado aplicadas a cada nível tecnológico [2].

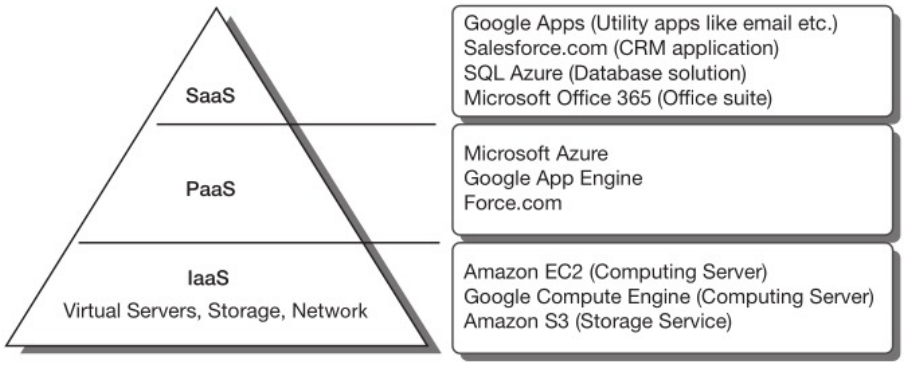

Figura 9. Hierarquia dos modelos de serviço em computação em nuvem (IaaS, PaaS e SaaS) e exemplos práticos.
Fonte: Bhowmik [2].

Essa transição de responsabilidades operacionais torna-se ainda mais evidente ao analisar a pilha de componentes gerenciados. Conforme ilustrado na Figura 10, à medida que se avança da infraestrutura tradicional para as modalidades IaaS, PaaS e SaaS, o provedor assume progressivamente o controle desde os ativos físicos até as camadas de aplicação, redefinindo o escopo de governança e segurança do cliente [4].

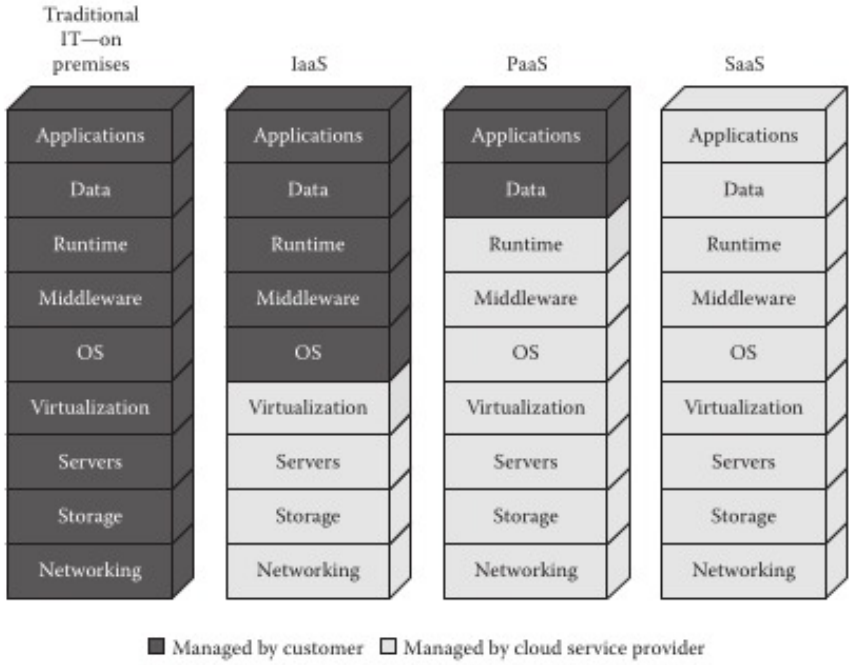

Figura 10. Divisão de escopo e responsabilidades entre cliente e provedor nas camadas de serviço computacionais.

Fonte: Vacca [4].

4.3.1. IaaS

Infraestrutura como Serviço (IaaS) é o modelo em que o provedor oferece recursos computacionais básicos, como processamento, redes e armazenamento, incluindo tanto discos virtuais quanto buckets de objetos. O consumidor detém controle sobre o sistema operacional e as aplicações implantadas, no entanto, seu controle é limitado em componentes de rede de baixo nível. No modelo IaaS, o usuário é responsável por gerenciar tudo acima da camada de virtualização, o que inclui a segurança do SO e a configuração de acesso aos dados armazenados nos buckets. Portanto, como o usuário possui maior nível de controle e liberdade de configuração, há maior probabilidade de falha humana, como a exposição acidental de um bucket público. Como exemplo de serviços de IaaS temos a *Amazon Web Services* (AWS), *Microsoft Azure*, *Google Cloud Platform*, *Huawei Cloud*, entre outros [31] [32].

4.3.2. PaaS

Plataforma como Serviço (PaaS) oferece um ambiente preparado para que o usuário implante aplicações criadas ou adquiridas. O usuário controla as configurações do ambiente de hospedagem e interage com recursos de armazenamento, como buckets, por meio de APIs fornecidas pela plataforma, mas não terá autonomia para gerenciar a Infraestrutura subjacente, como servidores, redes ou sistemas operacionais. Como exemplos práticos de soluções PaaS voltadas para a implantação de aplicações, destacam-se o *AWS Elastic Beanstalk* [22], o *Google App Engine* [23] e o *Heroku* [24]. Adicionalmente, a Huawei Cloud oferece o *ServiceStage* [26], uma plataforma PaaS voltada para o ciclo de vida completo de aplicações e microsserviços. Nessas plataformas, o desenvolvedor apenas faz o envio do código-fonte ou do contêiner, enquanto o provedor gerencia automaticamente o provisionamento, o balanceamento de carga e o escalonamento.

Além disso, o modelo PaaS engloba bancos de dados totalmente gerenciados, como o *Amazon RDS*, o *Google Cloud SQL* [25] e o *Huawei GaussDB* [27], um ecossistema de banco de dados nativo em nuvem. Nestes serviços, tarefas complexas como replicação, aplicação de patches de segurança e backups automatizados são abstraídas, permitindo que o usuário interaja apenas com a camada de dados através de APIs.

4.3.3. SaaS

Software como Serviço (SaaS) é o nível de maior abstração, no qual o usuário consome aplicações completas que rodam na infraestrutura do provedor. O usuário tem o mínimo de controle possível; toda a gestão de dados e o armazenamento em buckets são invisíveis para ele, e a aplicação é acessada por meio de interfaces thin client, como o navegador web. A experiência do usuário é totalmente gerenciada pelo provedor, que decide onde e como os dados serão armazenados. Como exemplos amplamente difundidos desse modelo, destacam-se suítes de produtividade e colaboração baseadas inteiramente na nuvem, como o *Microsoft 365* [28] e o *Google Workspace* [29]. Nessas plataformas, o usuário final cria documentos, planilhas e gerencia e-mails sem qualquer visibilidade sobre os servidores ou bancos de dados que sustentam a operação.

No ambiente de desenvolvimento e engenharia de software, ferramentas de gerenciamento de repositórios e esteiras de CI/CD como o *GitHub* [30] também operam majoritariamente no modelo SaaS, centralizando o código-fonte e o histórico de revisões em uma interface web totalmente gerenciada pelo provedor.

4.4. Unidade de Armazenamento de Objetos: Buckets e a Camada IaaS

O armazenamento na nuvem consiste na virtualização de recursos físicos, permitindo que os dados sejam geridos em pools lógicos de acordo com as necessidades de desempenho e de organização da aplicação. A segurança em buckets deriva da capacidade de distinguir as três principais técnicas de armazenamento: arquivos, blocos e objetos, ilustradas na Figura 11.

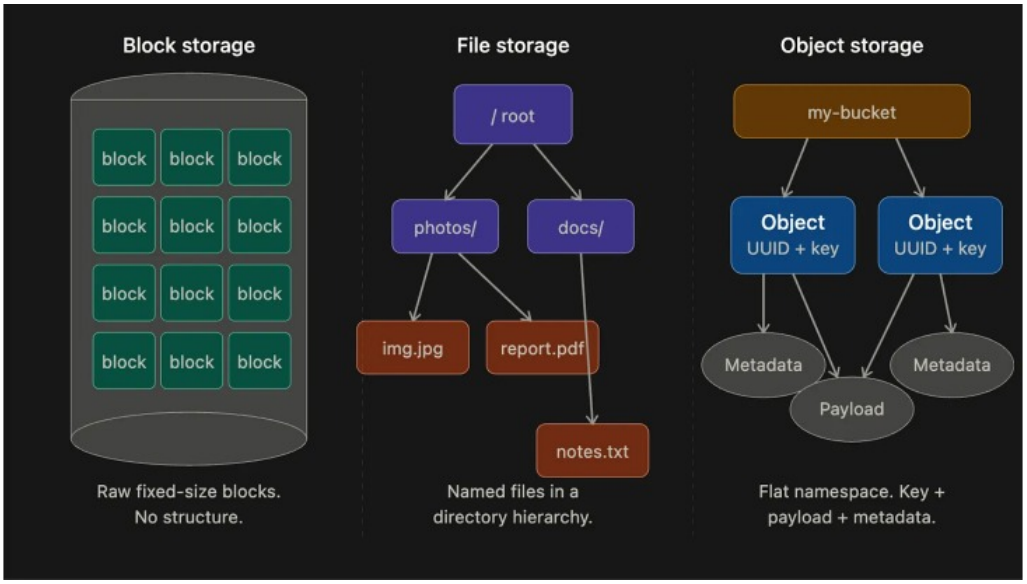

Figura 11. Diferenciação estrutural e conceitual entre os modelos de armazenamento em bloco (*Block*), arquivo (*File*) e objeto (*Object*).
Fonte: [33].

O armazenamento em arquivos (File Storage) é o módulo mais familiar, organizando os dados em uma hierarquia tradicional de diretórios e pastas; essa metodologia encontra espaço em equipes pequenas por meio de serviços como o Google Drive ou o OneDrive. O armazenamento em blocos (Block Storage) é uma técnica que particiona arquivos volumosos em blocos de tamanho fixo, distribuindo-os em volumes de armazenamento bruto que funcionam como discos rígidos não formatados. Há controle total para particionar e formatar esses volumes, utilizando sistemas de arquivos tradicionais, como NTFS e Ext4, amplamente utilizados em máquinas virtuais e em bancos de dados relacionais. O armazenamento em objetos (Object Storage) é a abordagem mais moderna para gerir volumes massivos de dados não estruturados em escala global. O Object Storage opera em um endereçamento plano (Flat Space), no qual cada dado é tratado como um objeto que contém o próprio arquivo. Esses objetos são armazenados em contêineres lógicos conhecidos como buckets, que incluem seus metadados descritivos e um identificador para recuperação rápida.

5. Riscos e Desafios de Segurança na Nuvem

A segurança da informação é regida pela tríade CIA (Confidencialidade, Integridade e Disponibilidade). Na nuvem, garantir que os dados estejam protegidos contra alterações não autorizadas e permaneçam acessíveis é um desafio crítico [4]. A migração de infraestruturas tradicionais para infraestruturas baseadas em nuvem traz vantagens como acesso fácil e redução de custos, porém, expande a superfície de ataque [2]. Esta refere-se às vulnerabilidades em redes, aplicações e dispositivos que podem ser exploradas. Caso a empresa utilize nuvens públicas ou híbridas, a segurança passa a ser compartilhada com o provedor, e quanto maior a integração com outras aplicações, maior será essa exposição [12].

5.1. Configurações de Nuvem Incorretas

Muitos dos incidentes de segurança na nuvem ocorrem devido a configurações inadequadas, tais como configurações de IAM (*Identity and Access Management*), que ocorrem quando se definem políticas de acesso de maneira incorreta, concedendo privilégios excessivos a usuários ou grupos, permitindo ações não autorizadas [4]. Outro erro grave envolve os *buckets* de armazenamento: quando definidos como públicos, em vez de privados, expõem dados confidenciais diretamente na rede [33]. Além disso, a falta de criptografia adequada coloca em risco os dados, tanto em repouso quanto em trânsito [4].

5.2. Vulnerabilidades em contêineres

Contêineres são pacotes de *software* que contêm o código de uma aplicação, suas bibliotecas e outras dependências de que ela precisa para ser executada na nuvem. As vulnerabilidades nos contêineres podem ocorrer devido a imagens corrompidas ou a vulnerabilidades no ambiente de execução (como o Kubernetes) [5]. É fundamental que o alcance de um aplicativo seja limitado para que ele não comprometa o sistema de seu ambiente conteinerizado [4].

5.3. Modelo de Responsabilidade Compartilhada

A computação em nuvem opera em um modelo de responsabilidade compartilhada, em que a segurança é responsabilidade tanto do provedor do serviço quanto da empresa que o utiliza [12]. O provedor assumirá a responsabilidade pela infraestrutura física, por todas as redes e pelas camadas de virtualização. Já o usuário é responsável por tudo o que gere acima disso, isto é, controles de acesso, configurações de segurança e a proteção dos dados [4]. Pelo fato de o usuário deter esse maior nível de controle, há uma maior probabilidade de falha humana [38].

5.4. Desafios da Conformidade com as Regulamentações

A conformidade refere-se à necessidade de a organização atender a leis, regulamentos e padrões de segurança, como a LGPD (Lei Geral de Proteção de Dados) no Brasil [20] ou o GDPR na Europa [21]. Na computação em nuvem, um dos maiores desafios é a soberania dos dados, pois os provedores possuem *data centers* espalhados por diversas regiões do mundo [38]. O usuário deve garantir que o armazenamento de dados esteja em conformidade com as leis locais, o que se torna complexo em arquitetura de nuvem pública, na qual o controle físico sobre a localização do servidor é inexistente [12]. Além disso, a empresa contratante precisa auditar se o provedor cumpre as certificações de segurança prometidas, uma vez que a responsabilidade legal sobre os dados dos clientes finais permanece sendo da empresa, e não do provedor [38].

5.5. Falta de Visibilidade da Nuvem

A falta de visibilidade ocorre quando a organização não consegue monitorar ou controlar totalmente os recursos utilizados em sua infraestrutura na nuvem [5]. Diferente de um ambiente local (*on-premises*), onde o controle físico é total, na nuvem é comum o surgimento do *shadow IT*, em que usuários criam instâncias, *buckets* ou bancos de dados sem o conhecimento da equipe de segurança [38]. Sem ferramentas de monitoramento centralizadas, torna-se difícil identificar, em tempo real, atividades suspeitas, acessos não autorizados ou configurações incorretas [5]. Essa "cegueira"operacional aumenta drasticamente o tempo de resposta a incidentes, permitindo que uma vulnerabilidade seja explorada por longos períodos antes de ser detectada [4].

6. Segurança de Longo Prazo e Prontidão Criptográfica Pós-Quântica

Com o alvorecer da computação quântica, os algoritmos criptográficos modernos, embora eficazes em contextos de computação clássica, tornam-se vulneráveis. O algoritmo de Shor é capaz de fatorar inteiros grandes e resolver problemas de logaritmo discreto em tempo polinomial, o que coloca em risco esquemas amplamente utilizados, como o RSA e a criptografia de curvas elípticas (ECC) [14]. De forma semelhante, os algoritmos de chave simétrica são desafiados pelo algoritmo de Grover, que otimiza a busca por força bruta e reduz a segurança efetiva das chaves pela metade (ex.: uma chave de 256 bits passa a oferecer o nível de segurança de 128 bits) [11]. Segundo [11], a mitigação dessas vulnerabilidades exige uma fase de transição dos algoritmos clássicos para a criptografia pós-quântica (PQC), garantindo resistência a ataques quânticos de forma simultânea. Paralelamente, protocolos de Distribuição de Chaves Quânticas (QKD) utilizam os princípios da mecânica quântica, como o princípio da incerteza de Heisenberg e o teorema da não clonagem, para realizar a troca segura de chaves físicas [15].

Desde 2017, o NIST conduz um processo global de padronização para selecionar os algoritmos PQC mais robustos [13]. Inicialmente, foram avaliadas 82 propostas em um processo colaborativo e aberto à comunidade criptográfica internacional. Em agosto de 2024, o NIST publicou os primeiros padrões oficiais definitivos baseados nos finalistas anunciados em 2023 [14], consolidando o CRYSTALS-Kyber (padronizado como ML-KEM), o CRYSTALS-Dilithium (ML-DSA) e o SPHINCS+. O algoritmo FALCON (FN-DSA) também foi selecionado para padronização subsequente [14].

Todavia, na análise de [11], foram considerados apenas o Kyber, o Dilithium e o Falcon. Embora o SPHINCS+ ofereça alta segurança por basear-se puramente em funções *hash* de segurança bem compreendida, ele gera assinaturas digitais extensas e apresenta desempenho computacional consideravelmente mais lento. Para a transmissão rápida e contínua exigida em canais QKD, o impacto computacional do SPHINCS+ comprometeria o desempenho do sistema [11]. Em contrapartida, os algoritmos baseados em redes (*lattices*) exibem baixa complexidade de implementação e alta prontidão de mercado, constituindo soluções puramente baseadas em *software* capazes de executar em infraestruturas clássicas existentes [16]. Essa padronização priorizou esquemas cuja segurança fundamenta-se em problemas matemáticos de difícil resolução tanto para computadores clássicos quanto quânticos, com destaque para o Problema do Vetor Mais Curto (SVP, *Shortest Vector Problem*), conforme a proposição clássica de Ajtai [9].

O SVP constitui o desafio matemático fundamental e a base de segurança para a criptografia baseada em reticulados. Geometricamente, o problema consiste em encontrar o vetor não nulo mais próximo da origem (ou seja, o de menor norma linear) em uma grade de pontos multidimensional infinita, mapeada originalmente por Regev [10] (Figura 12). A segurança dos algoritmos decorre do fato de que, à medida que a dimensão dessa grade é ampliada para centenas de variáveis, a busca pelo vetor mais curto sofre com a explosão combinatória [16]. Desse modo, para que um computador atacante consiga quebrar a criptografia e deduzir a chave privada a partir da chave pública interceptada, ele é obrigatoriamente induzido a resolver uma instância do SVP de alta dimensão [9]. Como não existem algoritmos clássicos ou quânticos eficientes conhecidos capazes de solucionar o SVP em tempo polinomial, o problema atua como uma barreira computacional intransponível, garantindo a imunidade quântica de algoritmos como o ML-KEM e o ML-DSA

[10, 11].

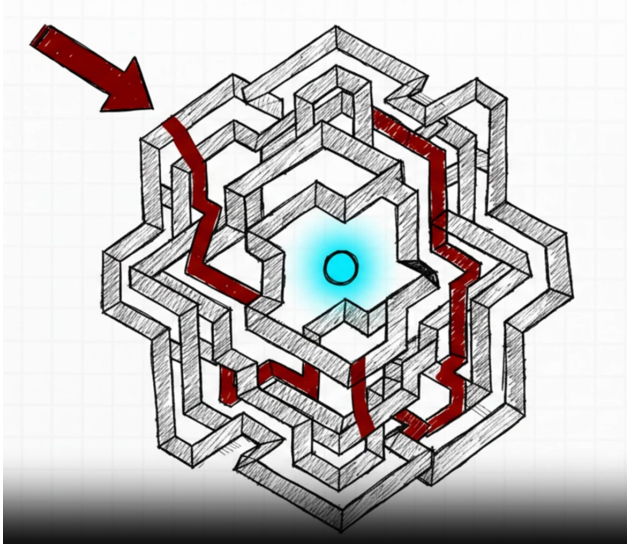

Figura 12. Analogia visual do Problema do Vetor Mais Curto (SVP) representada como um labirinto geométrico tridimensional.

Fonte: O autor, gerada com suporte de Google NotebookLM [34].

A aplicação prática do SVP e de suas variantes algébricas — como o problema do Aprendizado com Erros Baseado em Módulos (MLWE, *Module Learning with Errors*) — reflete-se diretamente nas funções específicas desempenhadas pelos três algoritmos de transição selecionados pelo NIST [14], conforme sintetizado na Tabela 1.

Tabela 1. Quadro comparativo dos algoritmos pós-quânticos em destaque pelo NIST.

Algoritmo	Nome Padrão	Tipo de Função	Características Principais
CRYSTALS-Kyber	ML-KEM	Encapsulamento (KEM)	Alta eficiência, tamanhos de chaves otimizados e foco no estabelecimento de chaves simétricas.
CRYSTALS-Dilithium	ML-DSA	Assinatura Digital	Equilíbrio ideal entre velocidade de processamento, tamanho do artefato e segurança.
Falcon	FN-DSA	Assinatura Digital	Assinaturas extremamente curtas, ideal para IoT e *hardware* restrito, porém maior complexidade.

Fonte: NIST [14] e Ghashghaei [11].

CRYSTALS-Kyber (ML-KEM): Atua como um Mecanismo de Encapsulamento de Chave (KEM, *Key-Encapsulation Mechanism*). Sua função primordial é permitir o

estabelecimento seguro de uma chave simétrica compartilhada entre duas entidades por meio de um canal público, sendo o único padrão KEM selecionado, em primeira instância, pelo NIST devido à sua alta eficiência e aos tamanhos de chave otimizados [14].

CRYSTALS-Dilithium (ML-DSA): Projetado como um esquema primário de assinatura digital. Destina-se a garantir a integridade dos dados e a autenticidade da origem da informação. O NIST o recomenda como a escolha principal para assinaturas eletrônicas devido ao excelente equilíbrio técnico entre segurança, velocidade de processamento e tamanho do artefato criptográfico gerado [14].

Falcon (FN-DSA): Também é configurado como um esquema de assinatura digital, porém focado estritamente na economia de espaço em banda e memória. Ele produz as assinaturas mais curtas entre todos os finalistas avaliados, tornando-se ideal para dispositivos com severas restrições de *hardware*, como microcontroladores e dispositivos IoT, embora apresente maior complexidade matemática e lentidão na geração das chaves iniciais quando comparado ao Dilithium [11].

Por outro lado, diferentemente da abordagem algorítmica do PQC, o QKD utiliza as leis da física para garantir a segurança, tornando qualquer tentativa de violação da confidencialidade dos dados detectável devido à alteração dos estados quânticos [11]. A seguir, apresentam-se dois protocolos fundamentais utilizados pela tecnologia QKD:

BB84: É um protocolo de "preparação e medição"que utiliza fótons polarizados para transmitir bits. Por exemplo, um usuário chamado Alice envia qubits em bases aleatórias, e um segundo usuário, chamado Bob, os mede. Após a troca, eles comparam uma parcela das bases para detectar erros que indicariam a presença de um terceiro usuário espião chamado de Eve [11].

E91: Baseia-se no emaranhamento quântico (pares de Bell). Alice e Bob recebem partículas emaranhadas de uma fonte central e realizam medições independentes. A segurança é verificada por meio da desigualdade de CHSH; se os resultados das medições violarem os limites da física clássica, a segurança do canal é confirmada [15]. As principais diferenças entre os dois protocolos serão mostradas na Tabela 2.

Tabela 2. Quadro comparativo dos protocolos de Distribuição Quântica de Chaves (QKD).

Protocolo	Ano	Princípio Físico	Mecanismo de Detecção de Espionagem
BB84	1984	Preparação e medição de fótons polarizados em bases aleatórias (Alice prepara, Bob mede).	Comparação pública de parte das bases utilizadas; divergências estatísticas revelam a presença de um espião (Eve).
E91	1991	Emaranhamento quântico (pares de Bell) distribuídos por uma fonte central a Alice e Bob.	Verificação da desigualdade de CHSH; a violação dos limites da física clássica confirma a segurança do canal.

Fonte: Ghashghaei [11] e Zarin [15].

O *framework* QuCloud representa um avanço estratégico ao integrar as defesas matemáticas da criptografia Pós-Quântica (PQC) às leis fundamentais da mecânica quântica para blindar o armazenamento de dados em nuvem. Enquanto as propostas de transição direta focam no canal de comunicação, o QuCloud é uma arquitetura híbrida multicamadas que combina o protocolo de Distribuição de Chaves Quânticas (QKD) E91, o algoritmo baseado em redes Kyber-512 e uma camada inovadora de Recriptografia por Procuração (PRE) customizada [15].

A Figura 13 detalha o pipeline criptográfico dessa arquitetura, dividido em três módulos de cores distintas. O **módulo de cifragem** (bloco amarelo à esquerda) recebe o arquivo em claro (*Plaintext*) enviado pelo remetente. Dentro dele, a chave passa por uma expansão de 256 bits com *salt hash* (*Key expansion*), seguida de 13 rodadas completas de AES (`SubBytes`, `ShiftRows`, `MixColumns`, `AddRound`) e uma 14ª rodada final sem `MixColumns`, produzindo o *Ciphertext*. O **módulo de re-criptografia** (bloco azul ao centro) representa a camada da nuvem: a PRE customizada do QuCloud recebe o texto cifrado e o re-criptografa usando uma *proxy key* efêmera, gerando um *Re-encrypted ciphertext* armazenado nos servidores. O **módulo de decifragem** (bloco amarelo à direita) é executado pelo receptor: ele usa um subconjunto da chave E91 como *proxy key* para desfazer a PRE e, em seguida, aplica os passos inversos do AES-256 com o *salt hash*, recuperando o arquivo original. Em nenhum ponto desse fluxo a nuvem possui a chave E91 completa, apenas a *proxy key* derivada dela, o que é exatamente o que torna o sistema resistente ao ataque HNDL.

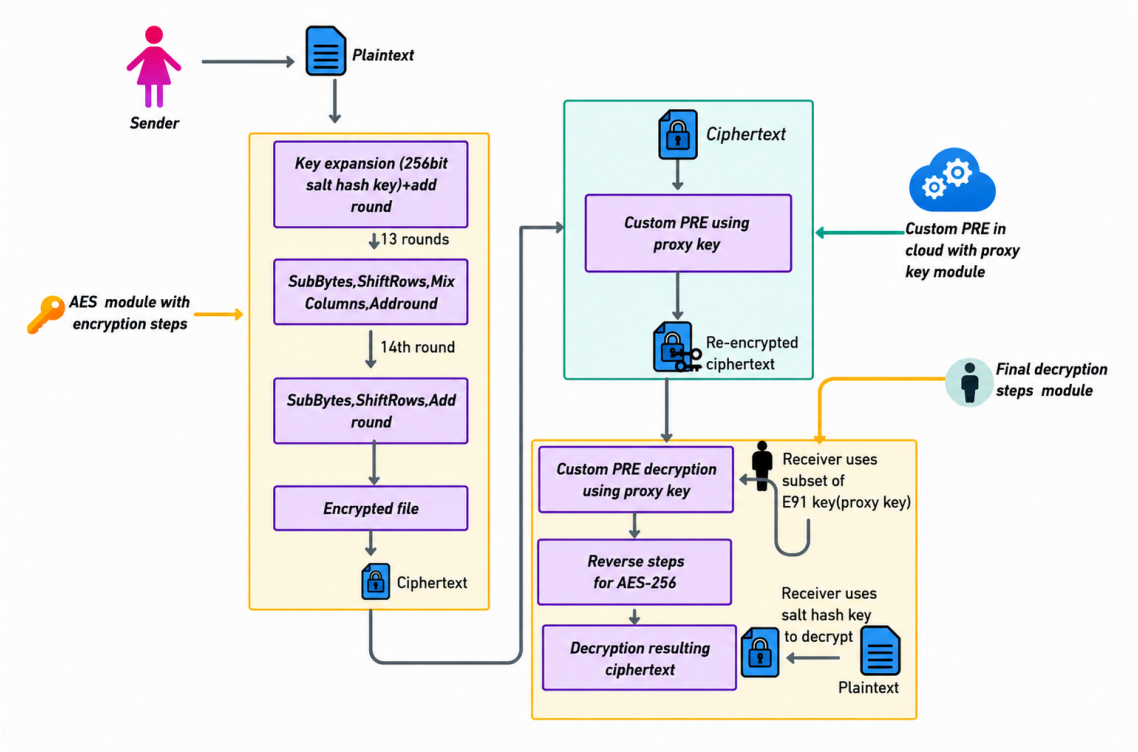

Figura 13. Pipeline criptográfico do QuCloud: módulo AES-256 com expansão de chave *salted* (bloco amarelo à esquerda); Re-criptografia por Procuração customizada executada na nuvem com *proxy key* efêmera derivada do protocolo E91 (bloco azul ao centro); decifragem pelo receptor via reversão AES-256 e *salt hash* (bloco amarelo à direita).

Fonte: [15].

A origem da *proxy key* efêmera utilizada nesse pipeline, e o motivo pelo qual ela muda a cada sessão, é explicada pelo protocolo de estabelecimento de chaves ilustrado na Figura 14.

A Figura 14 mostra como Alice (remetente, lado esquerdo) e Bob (receptor, lado direito) estabelecem a chave efêmera que alimenta o pipeline da Figura 13. Uma fonte central chamada **Charlie** emite pares de fótons emaranhados (seta vermelha no topo, *Entangle Photons*): Alice e Bob recebem cada um um fóton do par pelo canal quântico (*Quantum Channel*) e realizam medições independentes (*Measurement*). Após a comparação clássica das bases (*BASIS MATCH CLASSICALLY*), ambos derivam a mesma **Chave Simétrica Final E91 (KEY 1)**. A partir daí, o fluxo se divide em dois caminhos paralelos. No **caminho do material de chave** (lado esquerdo): Alice aplica *hashing* com *salt* sobre a KEY 1 para gerar uma *hashed key* salted, que é criptografada com a chave pública Kyber-PKE de Bob (*USING KYBER public key (A,t)*) e enviada a ele pelo canal clássico; Bob decifra com sua chave privada Kyber e recupera a *hashed key*. Alice também escolhe uma sequência específica de bits da KEY 1 para gerar a ***proxy key***, que é compartilhada com Bob e com o proxy de nuvem (seta tracejada ao centro). No **caminho dos dados** (parte inferior): Alice usa a *hashed key* para cifrar os arquivos com AES e os envia à nuvem, onde são re-criptografados com a *proxy key*. Bob recebe os arquivos

re-criptografados, desfaz a PRE com a *proxy key* e decifra o resultado final com a *salt hash key*, obtendo o arquivo original.

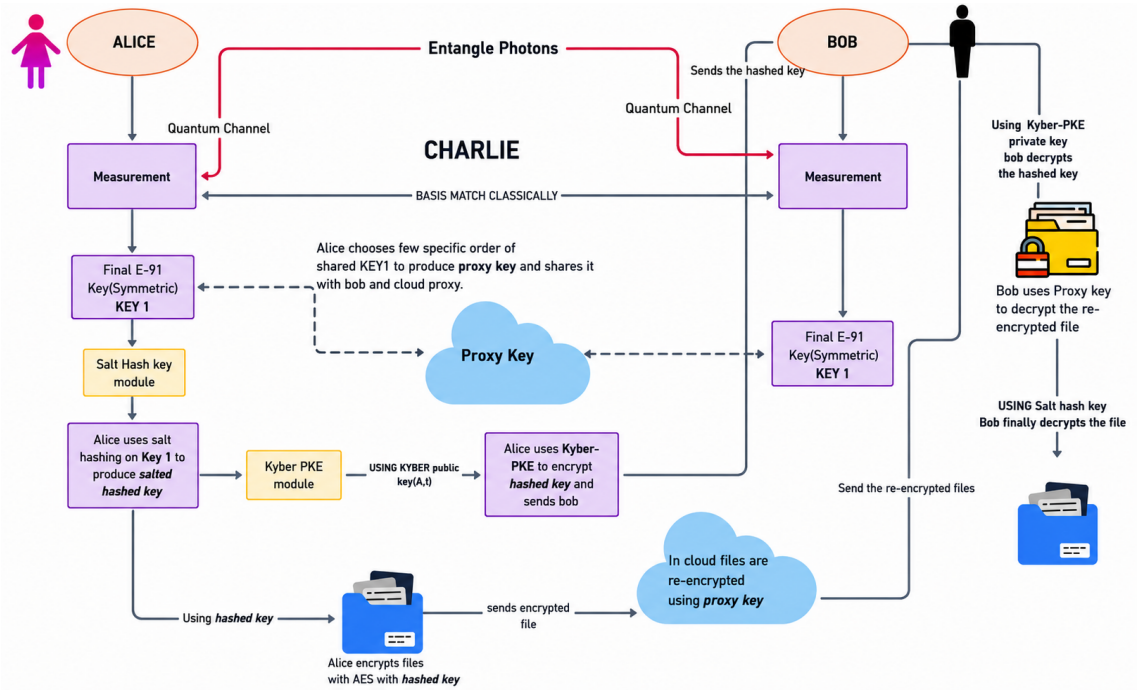

Figura 14. Fluxo completo de estabelecimento de chaves no QuCloud: Alice e Bob geram a Chave Simétrica E91 (KEY 1) via emaranhamento quântico mediado por Charlie; Alice protege a *hashed key* com Kyber-PKE e a envia a Bob; a *proxy key* derivada da KEY 1 é compartilhada com a nuvem, que re-criptografa os arquivos sem jamais ter acesso à KEY 1 completa, neutralizando o ataque HNDL.
Fonte: [15].

Com os dois fluxos estabelecidos, o pipeline criptográfico (Figura 13) e o protocolo de distribuição de chaves (Figura 14), a contribuição central do QuCloud torna-se evidente: a chave de re-criptografia nunca é fixa nem de longa duração, pois depende diretamente da aleatoriedade quântica produzida pelo emaranhamento E91 a cada sessão.

A principal contribuição desse sistema é a mitigação definitiva da ameaça *"harvest-now, decrypt-later"* (HNDL), na qual adversários interceptam e armazenam *"blobs"* de dados e chaves protegidas por RSA/ECC para descriptografá-los posteriormente. O diferencial técnico do QuCloud reside no fato de que sua camada de recriptografia não depende de chaves matemáticas de longa duração, mas sim de uma "fatia"de 128 bits extraída diretamente da chave bruta e efêmera gerada pelo processo quântico de emaranhamento do protocolo E91. Ao utilizar a aleatoriedade de sessão dependente da física quântica, o sistema garante que as chaves de recriptografia mudem constantemente, tornando os dados coletados hoje inúteis para ataques futuros [15].

Além da confidencialidade, o QuCloud reforça a segurança através da detecção ativa de intrusos no canal quântico por meio do teste da desigualdade CHSH; em cenários de espionagem, a perturbação nos estados quânticos causa uma queda acentuada (cerca de 62,6%) no valor de CHSH, o que aciona um aborto imediato do protocolo. Para o trans-

porte seguro do material-chave entre Alice e Bob, o sistema utiliza o Kyber-512, aproveitando sua eficiência e textos cifrados compactos de 768 bytes. Resultados experimentais demonstram que essa abordagem é viável para o mercado de nuvem atual, processando um *pipeline* completo de segurança para arquivos de 10 MB em 45,78 segundos, com um *overhead* de recriptografia de apenas 0,23 segundos, mantendo o desempenho próximo a implementações puramente clássicas [15].

7. Análise Comparativa, Aplicabilidade e Custo Operacional

As técnicas discutidas nas seções anteriores não competem entre si, pois cada uma foi desenvolvida para resolver um problema específico dentro do ambiente de nuvem. Esta seção analisa essas abordagens sob três ângulos complementares: a Seção 7.1 compara o que cada técnica faz na prática e qual problema resolve; a Seção 7.2 examina o custo operacional real de implementá-las, decomposto em processamento, armazenamento e tráfego de rede; e a Seção 7.3 discute em quais contextos de mercado esse investimento se justifica, considerando que nem toda organização tem a mesma necessidade ou capacidade de adoção.

7.1. Análise das Abordagens e suas Implementações

O ponto de partida fundamental para as abordagens discutidas nesta seção é o reconhecimento de que os servidores de nuvem operam fora do domínio de confiança do usuário. Embora protocolos como SSL/TLS sejam amplamente utilizados, eles protegem apenas o canal de comunicação durante o trânsito, o que é insuficiente para salvaguardar os dados contra "provedores curiosos"interessados no conteúdo armazenado.

Na tabela a seguir teremos um quadro comparativo das frentes de segurança em nuvem e suas implementações Tabela 3:

Tabela 3. Quadro comparativo das frentes de segurança em nuvem e suas implementações.

Abordagem	Objetivo Principal	Mecanismo Técnico Prático	Referência
Confidencialidade e Escalabilidade	Controle de acesso granular em nuvem	Uso de KP-ABE delegado ao servidor via PRE e mascaramento por "Atributo *Dummy*".	[6]
Verificação de Retratibilidade	Garantir posse do dado sem fazer *download*	Auditoria contínua baseada em blocos "sentinelas"aleatórios e Códigos de Correção de Erros (ECC).	[8]
Auditoria Pública com Privacidade	Verificação independente por terceiros (TPA)	Autenticadores homomórficos acoplados a técnicas de mascaramento aleatório de dados.	[7]
Prontidão Pós-Quântica	Imunidade contra o algoritmo de Shor e ataques HNDL	Integração de algoritmos baseados em *lattices* (Kyber) com chaves efêmeras geradas via QKD E91.	[11, 15]

O KP-ABE [6] resolve a confidencialidade sem exigir que o usuário confie no provedor. A ideia central é que o servidor pode armazenar e processar as chaves dos usuários, mas nunca possui a peça que completa a descriptografia, o Atributo Dummy, retido exclusivamente pelo Data Owner. O provedor realiza o trabalho computacional sem nunca enxergar o conteúdo real.

O POR [8] resolve um problema diferente: como verificar se o provedor está guardando o arquivo inteiro sem precisar baixá-lo. As sentinelas embaralhadas entre os blocos reais funcionam como uma armadilha. Se o provedor apagar parte dos dados para economizar espaço, eventualmente apagará uma sentinela e será detectado no próximo desafio de auditoria.

O PDP [7] complementa o POR ao permitir que essa auditoria seja conduzida por um terceiro independente, sem que esse auditor precise acessar o conteúdo dos arquivos. Isso é útil em cenários onde o próprio usuário não pode estar online para verificar seus dados.

A prontidão pós-quântica, por sua vez, não resolve um problema de confiança no provedor atual, mas um problema de prazo. O RSA e o ECC são seguros hoje, porém tornam-se vulneráveis à medida que computadores quânticos evoluem [11]. O QuCloud [15] antecipa essa ameaça combinando Kyber com chaves efêmeras geradas via QKD E91, de forma que dados interceptados hoje não possam ser decifrados no futuro, neutralizando o ataque HNDL.

O que essas quatro frentes têm em comum é que nenhuma é suficiente sozinha. Um sistema que usa KP-ABE mas não audita a integridade dos dados pode ter sua confidencialidade preservada enquanto os arquivos são silenciosamente apagados. Um sistema com POR mas sem proteção pós-quântica pode ter sua auditoria comprometida no futuro. A escolha de quais técnicas adotar depende menos de qual é a melhor e mais de quais ameaças são prioritárias para cada organização.

7.2. Componentes de Custo Operacional

O custo operacional de arquiteturas de segurança em nuvem é o ponto de partida para estimar seu impacto financeiro, já que os provedores cobram com base no consumo de recursos — como armazenamento por gigabyte-mês e volume de transferência de dados. Por isso, as métricas de tempo de processamento, espaço adicional e tráfego de rede apresentadas na Tabela 4 funcionam como indicadores diretos do custo que cada abordagem efetivamente adiciona à fatura na nuvem.

Tabela 4. Quadro comparativo dos componentes de custo operacional e impactos de desempenho.

Pilar de Custo	Tecnologia / Cenário	Métrica / Impacto Operacional Prático
Processamento (*Overhead* Computacional)	Criptografia Pós-Quântica	Kyber-512 realiza encapsulamento em 0,06 s e gera chaves em 31,2 ms (significativamente mais veloz que os 334,34 ms do RSA-3072).
	Gargalo Quântico	Protocolo QKD E91 responde por 97% do tempo total de execução (39,59 s para 500 pares de fótons).
	Acesso e Auditoria	KP-ABE possui complexidade de revogação de $\mathcal{O}(N)$; auditoria em lote reduz operações de *pairing* de $2K$ para $K + 1$.
Armazenamento (*Overhead* de *Storage*)	Redundância para Integridade	Implementações de PoRs geram fator de expansão de arquivo modesto de cerca de 15% devido a ECC e "sentinelas".
	Metadados Criptográficos	Cabeçalhos KP-ABE crescem linearmente; assinaturas Falcon ocupam apenas 356 B contra 2420 B do Dilithium-2.
Rede e Tráfego (*Data Transfer Out*)	Eficiência na Auditoria	Autenticadores homomórficos garantem tamanho de resposta constante, independente do número de blocos amostrados.
	Compactação de Chaves	Kyber-512 gera textos cifrados compactos de 768 B; PRE customizada adiciona apenas 0,23 s de latência (contra 1,8 s em Java).

Fonte: Yu et al. [6], Wang [7], Ghashghaei [11] e Zarin [15].

A tabela acima evidencia uma assimetria importante: o custo operacional das técnicas discutidas neste trabalho não se distribui uniformemente entre os três pilares.

No processamento, o gargalo não está onde se esperaria. Os algoritmos PQC, tanto o Kyber na cifragem quanto o KP-ABE no controle de acesso, operam na casa dos milissegundos. O problema está na camada física do QKD: o protocolo E91 consome sozinho 97% do tempo total de execução, com 39,59 segundos para processar 500 pares de fótons [15]. Isso significa que, em sistemas híbridos como o QuCloud, otimizar o software criptográfico tem impacto marginal. O investimento em desempenho precisa ir para o canal quântico.

No armazenamento, o impacto é modesto e administrável. As sentinelas dos PORs

geram uma expansão de aproximadamente 15% no tamanho dos arquivos, e os metadados do KP-ABE crescem linearmente com o número de atributos. Para a maioria dos casos de uso, esse overhead não representa um custo relevante na fatura do provedor.

No tráfego de rede, a criptografia baseada em reticulados apresenta uma vantagem concreta: textos cifrados compactos de 768 bytes no Kyber-512 e latência de recriptografia de apenas 0,23 segundos na PRE customizada do QuCloud [15]. Para operações em escala, essa compactação reduz diretamente o volume de transferência cobrado pelo provedor.

A conclusão prática é que a PQC pode ser adotada com baixo impacto operacional, já que roda puramente em software sobre infraestrutura existente. O QKD é outro cenário: exige hardware especializado, tempo de processamento significativo e infraestrutura de rede dedicada. Essa diferença de custo é o principal fator que hoje separa a adoção ampla da PQC da adoção restrita do QKD a setores específicos.

7.3. Mapeamento de Aplicabilidade no Mercado de Nuvem

A decisão de adotar uma ou mais das técnicas discutidas neste trabalho não é puramente técnica. Ela depende do perfil de risco de cada organização, do tipo de dado que precisa proteger e do horizonte de tempo em que essa proteção precisa ser válida. Esta subseção mapeia essa relação entre custo e contexto para os três segmentos identificados na Tabela 5.

Tabela 5. Quadro comparativo do mapeamento de aplicabilidade das tecnologias quânticas no mercado de nuvem.

Segmento / Modelo	Caso de Uso na Nuvem	Mecanismo Técnico Associado
Infraestrutura (IaaS) e Armazenamento	Provedores de Armazenamento	Esquemas de POR (*Proofs of Retrievability*) para garantias reais de SLA e integridade de dados.
	Buckets de dados públicos e privados	Criptografia Baseada em Atributos (KP-ABE) e PQC para neutralizar administradores "curiosos".
Setores de Alta Regulação	Saúde (Registros *HIPAA*)	Hibridização (PQC + QKD) para salvaguardar dados confidenciais de longa retenção por décadas.
	Governo e Defesa Nacional	Proteção imediata contra espionagem e ataques do tipo *"harvest-now, decrypt-later"* (HNDL).
Delegação e Compartilhamento Seguro	Fluxos de trabalho *multiusuário*	Camada de Re-criptografia por Procuração (*Proxy Re-Encryption* – PRE) customizada.
	Nuvem Corporativa Colaborativa	Delegação segura de acesso a arquivos sem revelar chaves mestras ou dados originais ao servidor.

Para provedores de armazenamento como o Amazon S3, o caso de uso mais imediato é o POR. Garantias de SLA são promessas — o POR é a forma de torná-las verificáveis, provando que os dados continuam acessíveis e íntegros sem que o usuário precise baixá-los para conferir. Dentro dos buckets, o KP-ABE, combinado com algoritmos PQC, endereça o risco mais recorrente discutido neste trabalho: a exposição de dados a administradores curiosos ou a configurações incorretas de acesso público.

Em setores de alta regulação, o horizonte de tempo muda o cálculo. Hospitais e órgãos governamentais lidam com dados que precisam permanecer sigilosos por décadas. Para esses casos, a ameaça HNDL deixa de ser hipotética: um adversário que colete dados criptografados hoje e os decifre daqui a dez ou vinte anos causa um dano irreversível. A hibridização entre PQC e QKD é, nesses contextos, a única abordagem que endereça esse risco de forma estrutural.

No Brasil, esse movimento já é visível em infraestruturas críticas. A ABIN desenvolve criptografia PQC de caráter nacional [18], e o sistema Pix — cujo protocolo de assinatura digital emprega atualmente RSA com XMLDSig sobre TLS 1.2 na Rede do

Sistema Financeiro Nacional — é objeto de estudos de migração para algoritmos resistentes a ataques quânticos [35, 19]. Ferreira et al. [19] avaliaram a viabilidade de substituir o RSA-SHA256 pelo algoritmo Picnic no processo de assinatura de mensagens ISO 20.022 do Sistema de Pagamentos Instantâneos (SPI), adotando como critérios segurança, performance e cripto-agilidade — esta última entendida como a facilidade de transição de um sistema criptográfico clássico para um pós-quântico sem redesenho completo da arquitetura. Os resultados indicaram que, embora o Picnic ofereça resistência quântica superior, seu tempo de processamento é de quatro a cinco vezes maior do que o exigido pelos padrões operacionais do Pix (até 50 ms por mensagem a 2000 transações por segundo), evidenciando que a cripto-agilidade e o custo computacional são os principais gargalos da transição pós-quântica em sistemas de pagamento de alta demanda [19].

Paralelamente, o sistema eleitoral brasileiro incorporou protocolos híbridos pós-quânticos na biblioteca criptográfica libharpia, desenvolvida pelo CEPESC em parceria com o TSE [17]. Nessa biblioteca, algoritmos da família CRYSTALS — Kyber para encapsulamento de chaves e Dilithium para assinaturas digitais, ambos selecionados pelo NIST como padrões pós-quânticos em 2022 — são combinados com curvas elípticas clássicas em protocolos híbridos, de modo que a segurança do sistema só pode ser comprometida se ambos os primitivos forem quebrados simultaneamente. Essa arquitetura conservadora posiciona as eleições brasileiras como as primeiras no mundo a operar com criptografia pós-quântica em ambiente de produção, sinalizando que infraestruturas críticas brasileiras já estão na vanguarda dessa transição.

Em ambientes corporativos colaborativos, o problema central é diferente: como compartilhar arquivos entre múltiplos usuários sem entregar ao servidor a chave que os protege. A camada de PRE customizada do QuCloud resolve isso de forma prática, permitindo que a nuvem re-criptografe os arquivos para diferentes destinatários sem nunca enxergar o conteúdo original.

O que esses três segmentos ilustram é que não existe uma configuração ideal única. A PQC tem alta prontidão de mercado e pode ser adotada imediatamente por qualquer organização, já que não exige hardware novo. O QKD, por outro lado, ainda enfrenta barreiras reais de custo e infraestrutura, o que restringe sua adoção a cenários onde o custo de uma brecha futura supera com clareza o investimento atual. A escolha, portanto, é menos uma questão técnica e mais uma questão de gestão de risco.

8. Conclusão

Com base nos dados e estudos apresentados, vemos que a utilização da nuvem para sistemas em geral, junto com os benefícios, utilização sob demanda, acesso ao sistema de qualquer localização e a não necessidade de infraestrutura física, traz também dificuldades, como o aumento da superfície de ataque, dado que os servidores não estarão no domínio do proprietário dos dados, o risco de "servidores honestos, mas curiosos", que podem ler os dados do proprietário, há também o risco de provedores de nuvem deletarem dados com o fito de reduzirem o consumo utilizado, entre vários outros problemas que podem surgir. Com o avanço da disponibilidade desses sistemas de nuvem, veio também o avanço da segurança da informação nesses ambientes. Algoritmos como o KP-ABE auxiliam na criptografia dos dados, impedindo que servidores curiosos possam analisá-los; já técnicas de auditoria, como PORs, auxiliam o Data Owner a verificar se houve deleção

de dados, devendo isso ao sistema de sentinelas discutido nesse trabalho.

No entanto, como mencionado neste trabalho, a tecnologia avançou e os computadores quânticos representam uma ameaça às técnicas tradicionais de criptografia, como RSA e ECC, que podem ser quebradas pelo algoritmo de Shor. Com isso em mente, o NIST conduziu um processo global de padronização para algoritmos de Criptografia Pós-Quântica (PQC) resistentes a ataques quânticos. Dessa disputa de algoritmos PQC, surgem os finalistas CRYSTALS-Kyber (ML-KEM) para troca de chaves, CRYSTALS-Dilithium (ML-DSA) e Falcon (FN-DSA) para assinaturas digitais, algoritmos que podem ser implementados de forma quase imediata; entretanto, sua implementação deve ser feita de forma cuidadosa para prevenir possíveis vazamentos através de canais laterais ou tempo de execução.

No topo da hierarquia, o *framework* QuCloud exemplifica a vanguarda da proteção na camada de aplicação, integrando PQC a protocolos da física quântica, como o E91. Essa hibridização é crucial para neutralizar a ameaça de "colher agora, decifrar depois"(HNDL), utilizando chaves efêmeras baseadas em emaranhamento quântico que tornam dados interceptados hoje inúteis no futuro. Embora a exigência de *hardware* especializado para protocolos como o BB84 e o E91 ainda limite sua disponibilidade no mercado como um todo, sua aplicação em setores de alta regulação e segurança nacional é uma realidade crescente. No cenário brasileiro, a ABIN e órgãos governamentais já lideram a adoção dessas técnicas em infraestruturas vitais, como as urnas eletrônicas e o sistema Pix, para garantir a soberania digital contra futuras capacidades computacionais. Em última análise, a proteção na nuvem não é uma garantia estática, mas uma corrida contínua onde a defesa em profundidade é o único caminho para a resiliência a longo prazo.

Nesse sentido, este trabalho abre caminho para investigações futuras, como uma análise mais aprofundada do comportamento dos algoritmos PQC frente a um mercado cada vez mais aquecido e em constante transformação. Destaca-se a exploração de vulnerabilidades em criptografias baseadas em reticulados por meio de ataques de canal lateral, como percebido no CRYSTALS-Kyber [14], bem como a avaliação contínua desses algoritmos frente a técnicas de criptoanálise clássica, cujo potencial de ameaça não deve ser subestimado mesmo diante da transição pós-quântica.

Referências

[1] CNN Brasil. Oracle dispara com aumento da demanda por serviços de nuvem no setor de ia, 2024. URL `https://www.cnnbrasil.com.br/economia/negocios/oracle-dispara-com-aumento-da-demanda-por-servicos-de-nuvem-no-setor-de-ia/`. Acessado em: 22 mai. 2024.

[2] Sandeep Bhowmik. *Cloud Computing*. Cambridge University Press, Cambridge, 2017. ISBN 978-1-316-63810-1.

[3] NIST, Peter Mell, and Timothy Grance. The NIST definition of cloud computing. Special Publication (NIST SP) 800-145, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2011. URL `https://csrc.nist.gov/publications/detail/sp/800-145/final`.

[4] John R. Vacca, editor. *Cloud Computing Security: Foundations and Challenges*. CRC Press, Boca Raton, 2017. ISBN 978-1-4822-6094-6.

[5] Netconn Group. Top 10 ferramentas de segurança na nuvem: Guia completo 2025, 2025. URL https://www.netconn.com.br/post/top-10-ferramentas-de-seguranca-na-nuvem-guia-completo-2025. Acessado em: 26 jun. 2026.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM*, pages 1–9. IEEE, 2010. doi: 10.1109/INFCOM.2010.5462174.

[7] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for data storage security in cloud computing. In *Proceedings of the 29th Conference on Information Communications (INFOCOM'10)*, pages 525–533, San Diego, CA, USA, 2010. IEEE. doi: 10.1109/INFCOM.2010.5462124.

[8] Ari Juels and Burton S. Kaliski, Jr. Pors: Proofs of retrievability for large files. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pages 584–597, New York, NY, USA, 2007. ACM. doi: 10.1145/1315242.1315313.

[9] Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 1–9, New York, NY, USA, 1996. ACM. doi: 10.1145/237814.237838.

[10] Oded Regev. On lattices, learning with errors, cryptographic applications, and learning groups. *Journal of the ACM (JACM)*, 56(6):1–40, 2009. doi: 10.1145/1568318.1568324.

[11] Farshad Rahimi Ghashghaei, Yussuf Ahmed, Nebrase Elmrabit, and Mehdi Yousefi. Enhancing the security of classical communication with post-quantum authenticated-encryption schemes for the quantum key distribution. *Computers*, 13(7):163, 2024. ISSN 2073-431X. doi: 10.3390/computers13070163. URL https://doi.org/10.3390/computers13070163.

[12] NIST, Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, and Dawn Leaf. NIST cloud computing reference architecture. Special Publication (NIST SP) 500-292, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2011. URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf.

[13] National Institute of Standards and Technology (NIST). Call for proposals - post-quantum cryptography standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals, December 2016. Acedido em: 8 de junho de 2026.

[14] National Institute of Standards and Technology (NIST). Nist to standardize encryption algorithms that can resist attack by quantum computers. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers, August 2023. Acedido em: 8 de junho de 2026.

[15] Anika Taffannum Zarin, Omar Radee, Md Shawmoon Azad, and M. R. C. Mahdy. Qucloud: Enhancing cloud storage security by combining quantum key distribution, post-quantum cryptography, and custom proxy re-encryption. *Journal of Information Security and Applications*, 99:104449, 2026. ISSN 2214-2126. doi: 10.1016/j.jisa.2026.104449.

[16] Chris Peikert. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(1–4):1–355, 2016. doi: 10.1561/0400000074.

[17] Rodrigo Pacheco, Douglas Braga, Iago Passos, Thiago Araújo, Vinícius Lagrota, and Murilo Coutinho. libharpia: a new Cryptographic Library for Brazilian Elections. In *Anais do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 250–263, Porto Alegre, RS, Brasil, 2022. SBC. doi: 10.5753/sbseg.2022.224098. URL https://sol.sbc.org.br/index.php/sbseg/article/view/21672.

[18] Agência Brasileira de Inteligência. ABINcast - criptografia pós-quântica para urnas eletrônicas, 2022. URL https://www.gov.br/abin. Podcast oficial da Agência Brasileira de Inteligência.

[19] Rodrigo Ferreira, Pedro Ripper, Rafael Veríssimo, and Aristides Andrade Cavalcante Neto. Análise da viabilidade de aplicação de métodos de criptografia pós-quântica aplicados ao sistema de pagamentos instantâneos brasileiro (Pix). *Revista do Laboratório de Inovações Financeiras e Tecnológicas*, 4, abril 2022. Brazil Quantum, São Paulo, SP, Brasil.

[20] Brasil. Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd), 2018. URL https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[21] União Europeia. Regulamento (ue) 2016/679 do parlamento europeu e do conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados - gdpr), 2016. URL https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679.

[22] Amazon Web Services. AWS Elastic Beanstalk developer guide, 2026. URL https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html.

[23] Google Cloud. App Engine documentation, 2026. URL https://cloud.google.com/appengine/docs.

[24] Heroku. How Heroku works - Heroku Dev Center, 2026. URL https://devcenter.heroku.com/articles/how-heroku-works.

[25] Google Cloud. Cloud SQL overview, 2026. URL https://cloud.google.com/sql.

[26] Huawei Cloud. ServiceStage - application management and hosting platform, 2026. URL https://www.huaweicloud.com/intl/en-us/product/servicestage.html.

[27] Huawei Cloud. GaussDB nosql - cloud-native distributed database, 2026. URL https://www.huaweicloud.com/intl/en-us/product/gaussdbnosql.html.

[28] Microsoft. What is Microsoft 365 for business?, 2026. URL https://support.microsoft.com/en-us/office/what-is-microsoft-365-for-business-d94892fb-912c-47bc-9407-77fa8f6e6ec1.

[29] Google Cloud. Google Workspace overview, 2026. URL https://workspace.google.com/intl/en/features/.

[30] GitHub. About GitHub - the developer platform, 2026. URL https://github.com/about.

[31] Cisco Community. Principais provedores de IaaS, 2024. URL https://community.cisco.com/t5/blogues-de-data-center-e-cloud/principais-provedores-de-iaas/ba-p/5132199.

[32] Huawei Cloud. Huawei cloud thailand market share: No. 3 in IaaS market by revenue in 2023, 2024. URL https://www.huaweicloud.com/intl/en-us/news/20240607151847120.html. Baseado em dados de participação de mercado da Gartner.

[33] System Design One. AWS S3 System Design: Understanding object storage architecture, 2024. URL https://newsletter.systemdesign.one/p/aws-s3-system-design.

[34] Google LLC. Notebooklm: Inteligência artificial para análise e contextualização de documentos, 2026. URL https://notebooklm.google/. Imagem gerada via plataforma para fins de analogia conceitual.

[35] Microsoft News Center Brasil. Com apoio da Fenasbac, Banco Central, Brazil Quantum e Microsoft exploram o uso de criptografia pós-quântica para melhorar segurança do Sistema Pix, maio 2022. URL https://news.microsoft.com/pt-br/com-apoio-da-fenasbac-banco-central-brazil-quantum-e-microsoft-exploram-o-uso-de-criptografia-pos-quantica-para-melhorar-seguranca-do-sistema-pix/.

[36] ISO/IEC. ISO/IEC 17788:2014: Information technology – cloud computing – overview and vocabulary, 2014. URL https://www.iso.org/standard/60544.html.

[37] ETSI. Cloud computing; Cloud Standards Coordination; final report. Technical Report ETSI TR 103 125 V1.1.1, European Telecommunications Standards Institute (ETSI), Sophia Antipolis, FR, 2013. URL https://www.etsi.org/deliver/etsi_tr/103100_103199/103125/01.01.01_60/tr_103125v010101p.pdf.

[38] Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Cloud Security Alliance (CSA), Seattle, WA, 2017. URL https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.