INTERFACE TECNOLÓGICA

ABORDAGENS E DESAFIOS DA SEGURANÇA NA COMPUTAÇÃO EM NUVEM: criptografia, privacidade e controle de acesso

SECURITY APPROACHES AND CHALLENGES IN CLOUD COMPUTING: encryption, privacy, and access control

Valdenilson dos Santos Lima – valdenilsonlima@hotmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Elielson Antonio Sgarbi – elielson.sgarbi@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v21i2.2142
Data de submissão: 27/09/2024
Data do aceite: 23/11/2024
Data da publicação: 20/12/2024

RESUMO

Este trabalho tem por objetivo investigar as abordagens e desafios de segurança na computação em nuvem, com ênfase em criptografia, privacidade e controle de acesso. Primeiramente, explora-se a importância da segurança na nuvem e os principais riscos enfrentados pelos usuários e provedores de serviços. Em seguida, são discutidas as técnicas de criptografia utilizadas para proteger dados em trânsito e em repouso, bem como os desafios associados à sua implementação. Além disso, são abordadas questões de privacidade relacionadas à coleta, armazenamento e processamento de dados na nuvem, incluindo regulamentações e padrões de dados sensíveis contra acessos não autorizados. Conclui-se destacando a importância de abordagens integradas de segurança e seguindo áreas para futuras pesquisas visando aprimorar a segurança da computação em nuvem. Dentre as obras que norteiam a análise deste trabalho estão "O Escudo da Privacidade na Era da Conectividade" (2023), de Juliane Ferreira, "What is identity and access management?" by Matthew Kosinski e Amber Forrest (2024) and "A survey on security issues in service delivery models of cloud computing" (2010), by S. Subashini e V. Kavitha.

Palavras-chave: Segurança. Criptografia. Privacidade. Dados. Gerenciamento.

ABSTRACT

This work investigates the approaches and challenges of security in cloud computing, with emphasis on cryptography, privacy, and access control. Firstly, the importance of cloud security and the main risks faced by users and service providers are explored. Next, cryptographic techniques used to protect data in transit and at rest are discussed, as well as the challenges associated with their implementation. Additionally, privacy issues related to data collection, storage, and processing in the cloud, including regulations and standards for sensitive data against unauthorized access, are addressed. It is concluded by highlighting the importance of integrated security approaches and suggesting areas for future research to enhance cloud computing security. Among the works that guide the analysis are "O Escudo da

Privacidade na Era da Conectividade" (2023), by Juliane Ferreira, "What is identity and access management?" by Matthew Kosinski e Amber Forrest (2024) e "A survey on security issues in service delivery models of cloud computing" (2010), de S. Subashini and V. Kavitha.

Keywords: Security. Cryptography. Privacy. Data. Management.

1 INTRODUÇÃO

Nos últimos anos, a computação em nuvem ou *cloud computing* surgiu como uma solução revolucionária para armazenamento, processamento e acesso de dados, oferecendo às organizações uma flexibilidade única, além da capacidade de escalar recursos conforme necessário.

Embora o termo *cloud computing* tenha sido adotado recentemente por usuários de Tecnologia da Informação (TI), o conceito surge em 1997, em uma palestra proferida pelo professor Ramnath Chellappa, intitulada *Intermediaries Cloud computing*, apresentada em um encontro da INFORMS em Dallas, no Texas. A partir de então, o termo ganhou popularidade, trazendo inúmeros benefícios para seus usuários, tais como redução de custo com infraestrutura, economia de espaço físico, centralização da informação e adoção do trabalho remoto, segundo artigo publicado pela Empresa Júnior da Fundação Getúlio Vargas.

A computação em nuvem, portanto, se configura como um importante recurso capaz de garantir aos seus usuários o acesso remoto a softwares e arquivos por meio de qualquer dispositivo com o auxílio da Internet, proporcionando aos seus usuários um novo modelo de armazenamento de dados, compatível com o contexto de cada usuário. Mell e Grance (2011) elucidam que *cloud computing* é um modelo que possibilita acesso universal, sob demanda de rede, a partir de um conjunto compartilhado de recursos computacionais configuráveis, que abrange desde redes e servidores até armazenamento e aplicativos de serviços. Tais recursos podem "ser rapidamente provisionados e liberados com um esforço de gerenciamento mínimo ou interação com o provedor de serviços." (Mell; Grance, 2011, p. 2, tradução nossa).

Segundo Kamila (2013), a computação em nuvem é um novo conceito da área de computação, especialmente na indústria de serviços de TI, que pode ser considerada como "A Terceira Revolução Industrial", após o surgimento do computador pessoal e da Internet. Tal ferramenta, de acordo com Kamila, oferece aplicativos com o auxílio da internet, acesso a partir de um navegador web, enquanto o software e dados empresariais são armazenados em servidores em um local remoto. *Cloud computing* corresponde, portanto, à entrega da

computação como um serviço em vez de um produto, por recurso compartilhado; software e informações são fornecidos a seus usuários por dispositivos como utilidade via rede e uma nova forma de armazenar as informações.

2 FUNDAMENTAÇÃO TEÓRICA

Este artigo elenca o conceito de *cloud computing*, suas aplicações no ambiente virtual e os principais benefícios que tal ferramenta proporciona a seus usuários, bem como as possíveis falhas as quais essa ferramenta está suscetível. Nesse sentido, o artigo fundamenta-se nas percepções de Nobles (2022), cujo conteúdo descreve os erros humanos como principais causadores de falhas nos sistemas de nuvens. O trabalho de Ambrust *et al.* faz uma reflexão acerca da computação em nuvem como utilidade, abrindo novos horizontes para as indústrias de TI, que tornarão qualquer software ainda mais atrativo como um serviço, além de moldar a maneira como um hardware de TI é criado e adquirido por seus usuários.

2.1 Desafios de Segurança na Computação em Nuvem

Embora o uso da computação em nuvem tenha modificado o *modus operandi* de seus provedores e usuários, permitindo que estes acessem seus dados de qualquer aparelho, essa transição para a nuvem também trouxe consigo uma série de preocupações relacionadas à segurança dos dados. De acordo com pesquisas recentes, a maioria das violações de segurança na nuvem até 2025 será causada por erros de seus usuários, comprometendo a realização de trabalhos no ambiente virtual e colocando em risco a segurança de seus dados. Harrison (2022) aponta que 88% das violações em nuvem são causadas por erro humano, comprometendo, portanto, a segurança do ambiente corporativo e de seus usuários. Nesse sentido, a proteção dos dados contra ameaças cibernéticas tornou-se prioridade para empresas e usuários individuais, que estão suscetíveis a esses ataques. Paganini (2021) reconhece que erros humanos potencializam a chamada desconfiguração da nuvem devido à falta de entendimento de políticas e segurança da nuvem, falha na supervisão de dados e sobrecarga com interfaces de programas de aplicativos. A desconfiguração em nuvem, causada por seus usuários, intensifica tais erros colocando em xeque os dados do ambiente virtual, impedindo o cumprimento das normas de segurança e reduzindo as iniciativas de transformação digital.

Essas desconfigurações, segundo Nobles (2022) se intensificaram durante a pandemia de Covid 19 (Paganini, 2021 *apud* Nobles, 2022, p. 60) obrigando as organizações a migrarem de um sistema operacional centralizado para um constructo operacional

descentralizado, evitando uma desestruturação no sistema operacional dessas empresas. Segundo Paganini, as organizações corporativas foram absorvendo esses modelos de nuvem, disponibilidade e compartilhamento de recursos para apoiar o trabalho remoto, já que tal modelo se tornou dominante durante pandemia, consolidando-se no meio corporativo no período pós-pandemia.

Embora nenhum ambiente virtual esteja imune a erros humanos ou ataques cibernéticos, a computação em nuvem, segundo Armbrust *et al.* (2010) está transformando profundamente a forma como as organizações realizam seus negócios. Para este autor, *cloud computing*, o antigo sonho da computação como utilidade, promete abrir novos caminhos para grande parte da indústria de TI, tornando qualquer software ainda mais atrativo como um serviço e moldando a maneira como um hardware de TI é criado e adquirido por seus usuários (Armbrust *et al.*, 2010, p. 50).

2.1.1 Confidencialidade dos dados

A confidencialidade dos dados é a garantia de que apenas usuários autorizados tenham acesso às informações. Mell e Grance (2011) afirmam que a confidencialidade é essencial para proteger informações sensíveis contra acesso não autorizado, garantindo a privacidade dos usuários e a integridade dos dados armazenados. Nesse sentido, a criptografia desempenha um papel central, garantindo que os dados sejam ilegíveis para usuários não autorizados, mesmo que eles acessem os recursos de armazenamento em nuvem.

2.1.2 Integridade dos dados

A integridade dos dados refere-se à garantia de que os dados permaneçam precisos e não sejam alterados de forma não autorizada. De acordo com Subashini e Kavitha (2011), a integridade dos dados é crucial para garantir a confiabilidade das informações armazenadas na nuvem. Eles também destacam que medidas de segurança adequadas são necessárias para prevenir alterações não autorizadas nos dados, assegurando sua integridade ao longo do tempo.

2.1.3 Disponibilidade dos serviços

Segundo Oliveira e Oliveira (2023) a disponibilidade é considerada um dos pilares deste modelo de computação, pois visa garantir que dados e serviços armazenados possam ser consultados a todo momento e em qualquer lugar no mundo. Segundo Lopes (2023), podemos

definir a disponibilidade como a capacidade de eliminar todas as falhas que podem ser encontradas na entrega de serviços. Em termos práticos, isso significa que, em caso de falha de um servidor, há um outro para substituição imediata.

2.1.4 Privacidade dos dados

A privacidade dos dados em *cloud computing* é uma questão complexa que envolve uma série de considerações importantes. Primeiramente, é crucial entender que essa responsabilidade é compartilhada entre o provedor de serviços em nuvem e o cliente. Segundo Marduque (2023), enquanto os provedores devem implementar medidas adequadas para proteger os dados dos clientes, estes últimos também devem adotar práticas de segurança e privacidade em seus próprios processos e sistemas.

Além disso, a conformidade regulatória desempenha um papel fundamental na proteção da privacidade dos dados. Regulamentações como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil estabelecem requisitos rigorosos para o tratamento de dados pessoais, exigindo que tanto os provedores quanto os clientes estejam em conformidade para garantir a proteção adequada dos dados. Conforme afirma Ferreira (2023), garantir a conformidade com a LGPD não apenas protege a privacidade das pessoas, mas também pode gerar confiança entre os clientes, melhorar a imagem da empresa e diminuir a probabilidade de ocorrência de violações de dados.

2.1.5 Gerenciamento de identidade e acesso

O gerenciamento de identidade e acesso refere-se ao controle de quem pode acessar os recursos na nuvem e quais ações eles podem realizar. Rittinghouse & Ransome (2009) destacam que o gerenciamento eficaz de identidade e acesso é fundamental para proteger os dados na nuvem contra acessos não autorizados. Eles também observam que políticas de controle de acesso robustas e mecanismos de autenticação multifatorial são essenciais para garantir a segurança dos recursos na nuvem e proteger contra acessos não autorizados.

2.2 Estratégias de Segurança na Computação em Nuvem

Embora a computação em nuvem traga inúmeros benefícios aos seus usuários, é crucial adotar estratégias utilizadas para mitigar os riscos presentes nesse domínio. Nesse

sentido, há uma série de medidas cautelares a serem adotadas para garantir a segurança dos dados, preservando, portanto, os seus usuários e os conteúdos disponibilizados na nuvem.

2.2.1 Criptografia

Implementar criptografia de dados é uma medida fundamental para proteger as informações confidenciais da sua empresa. Em essência, a criptografia atua como uma camada de proteção que dificulta a leitura dos dados por indivíduos não autorizados, tornando-os ilegíveis. Dessa forma, a criptografia serve como uma barreira contra possíveis violações de dados, já que, mesmo se os dados forem comprometidos, sua forma criptografada os torna praticamente inúteis para qualquer pessoa não autorizada.

Assim sendo, ao armazenar dados criptografados na nuvem, sua empresa pode garantir uma camada adicional de segurança e confidencialidade, alinhada com as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD).

Conforme artigo publicado pela *Google Cloud* (2022), a criptografia desempenha um papel fundamental na proteção dos dados em três estágios distintos:

- **Criptografia em repouso:** Esta técnica visa proteger os dados enquanto estão armazenados, evitando que sejam acessados ou comprometidos indevidamente. Geralmente, utiliza-se o algoritmo de criptografia avançada (AES) para cifrar os dados armazenados, garantindo sua segurança contra ameaças externas.
- **Criptografia em trânsito:** Aqui, os dados são protegidos durante sua transmissão entre diferentes pontos, como entre um dispositivo e um serviço na nuvem, ou entre dois serviços distintos. Esse processo envolve criptografar os dados antes de sua transmissão, utilizando protocolos como o *Transport Layer Security* (TLS) para garantir a segurança das comunicações. Além disso, a autenticação dos *endpoints* é realizada para garantir a integridade dos dados, descriptografando-os apenas no destino e verificando se não foram modificados durante o trânsito. Por exemplo, as *Secure/Multipurpose Internet Mail Extensions* (S/MIME) são comumente empregadas para proteger mensagens de e-mail durante sua transmissão.
- **Criptografia em uso:** Esta medida visa proteger os dados enquanto estão em uso na memória do sistema, evitando seu comprometimento ou exfiltração durante o processamento. Isso é alcançado através da aplicação de técnicas de criptografia que

cifram os dados enquanto estão sendo manipulados, garantindo sua segurança mesmo durante operações de processamento sensíveis.

2.2.2 Controles de acesso e autenticação

Os controles de acesso e autenticação são essenciais para garantir a segurança dos dados na nuvem. De acordo com Subashini e Kavitha (2011), políticas robustas de controle de acesso e autenticação multifatorial são cruciais para essa proteção. Além disso, soluções como *Single Sign-On* (SSO) e *Identity and Access Management* (IAM) são empregadas para simplificar o gerenciamento de identidade e acesso.

O *Single Sign-On* (SSO) é uma técnica que permite aos usuários acessarem várias aplicações com apenas um login, proporcionando maior conveniência e eficiência, como observado em um artigo da TOTVS (2022). Na prática, quando um usuário realiza o login em um serviço utilizando o SSO, é gerado um token de autenticação que é armazenado no navegador ou nos servidores do provedor de SSO. Esse token é então utilizado automaticamente sempre que o usuário acessa outros aplicativos ou sites conectados, agilizando o processo de login em todas as plataformas conectadas ao SSO.

Já o *Identity and Access Management* (IAM) é uma área da segurança cibernética responsável pelo controle de acesso dos usuários aos recursos digitais, conforme explicado no artigo de Kosinski e Forrest (2024). Os sistemas de IAM atuam como barreiras contra invasões, garantindo que cada usuário possua apenas as permissões necessárias para suas atividades, sem acesso indevido a outras áreas.

2.2.3 Monitoração e detecção de ameaças

O monitoramento contínuo e a detecção de ameaças são essenciais para identificar atividades suspeitas na nuvem. Praticamente todos os provedores de nuvem zelam para que este tópico seja atendido, visando a confiabilidade do cliente. Segundo Rea e Leavitt (2024), o monitoramento de segurança envolve a coleta de dados em vários níveis da infraestrutura, aplicativos e operações para identificar atividades suspeitas. Isso ajuda a antecipar incidentes e a aprender com eventos passados. Os dados coletados são essenciais para analisar o que aconteceu após um incidente, auxiliando na resposta e em investigações posteriores.

2.2.4 Conformidade e segurança

A conformidade e governança são aspectos críticos da segurança na computação em nuvem, garantindo que as práticas adotadas estejam alinhadas com regulamentações e padrões de segurança estabelecidos. Segundo Rittinghouse e Ransome (2009), estabelecer políticas de segurança em conformidade com regulamentações é vital para proteger os dados na nuvem. Além disso, eles ressaltam a importância de realizar auditorias regulares para garantir a conformidade contínua e mitigar os riscos. Em outras palavras, a conformidade refere-se à adesão a leis, regulamentos e padrões relevantes, enquanto a governança se concentra em estabelecer processos e políticas para garantir a conformidade e gerenciar os riscos de forma eficaz. Essas práticas garantem que a organização esteja operando dentro dos limites legais e éticos, protegendo os dados e mantendo a confiança dos clientes e partes interessadas.

2.2.5 Educação e conscientização

A educação e conscientização do usuário são aspectos essenciais para fortalecer a segurança na computação em nuvem. De acordo com artigo publicado pela Karspersky (2024), os programas de treinamento em segurança da informação devem fazer parte do processo de integração, com o objetivo de instruir os novos funcionários quanto as políticas da empresa. Esses programas são projetados para ajudar os usuários a reconhecerem e responder adequadamente a ameaças potenciais, como *phishing* e outras tentativas de ataques cibernéticos.

Os programas de treinamento também abordam práticas seguras de computação em nuvem, orientando os usuários sobre a importância de proteger suas credenciais de login, como o uso de senhas fortes e atualizadas, e o uso de recursos de segurança oferecidos pela plataforma de nuvem.

3 PROCEDIMENTOS METODOLÓGICOS

A principal abordagem adotada neste estudo foi a revisão bibliográfica, que envolveu a pesquisa e análise de artigos, livros e dissertações, com foco na organização e estruturação de dados.

Para complementar a revisão bibliográfica e obter *insights* diretamente dos usuários, foi conduzida uma pesquisa por meio do *Google Forms*, que teve como objetivo coletar dados quantitativos e qualitativos sobre as percepções, experiências e necessidades dos usuários relacionadas ao tema em estudo. A pesquisa pelo *Google Forms* seguiu as seguintes etapas:

- **Elaboração do Questionário:** Foi elaborado um questionário estruturado contendo perguntas específicas relacionadas aos objetivos da pesquisa.
- **Divulgação e Coleta de Dados:** O link para o questionário foi divulgado por meio de redes sociais e e-mails.
- **Análise de Dados:** As respostas coletadas foram analisadas quantitativamente e qualitativamente para identificar padrões, tendências e *insights* relevantes. Foram utilizadas técnicas estatísticas e análise de conteúdo para interpretar os dados e extrair conclusões significativas.

Os resultados da revisão bibliográfica e da pesquisa pelo *Google Forms* foram integrados para fornecer uma visão abrangente e aprofundada do tema em estudo. As descobertas foram interpretadas à luz da teoria existente e das percepções dos usuários, permitindo uma análise abrangente e fundamentada.

4 RESULTADOS E DISCUSSÃO

O questionário aplicado contou com 8 perguntas e 18 entrevistados. O objetivo da pesquisa foi investigar o nível de conhecimento e as preocupações dos usuários em relação à segurança na computação em nuvem, além de identificar as medidas de segurança consideradas mais importantes e as áreas que precisam ser aperfeiçoadas na perspectiva dos participantes.

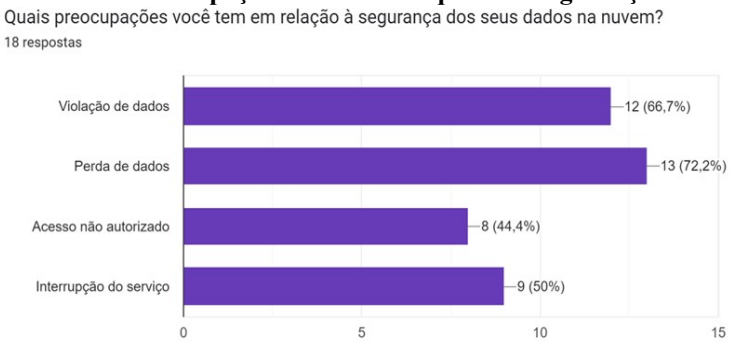
Dados os resultados, realizamos as seguintes considerações:

- **Familiaridade com os conceitos de segurança na computação em nuvem:** A maioria dos participantes mostrou um nível moderado de familiaridade com os conceitos de segurança na computação em nuvem, com 55,6% se considerando moderadamente familiarizados. Cerca de 27,8% se sentiram pouco familiarizados, enquanto 16,7% se consideraram muito familiarizados. Isso sugere que, embora muitos tenham algum conhecimento sobre segurança na computação em nuvem, ainda há uma parcela considerável que se sente pouco à vontade com o tema. Esses resultados destacam a importância de programas de educação e conscientização em segurança cibernética, especialmente no contexto da computação em nuvem, para

garantir que os usuários estejam bem-informados e preparados para enfrentar os desafios de segurança associados a essa tecnologia.

- **Utilização de serviços de computação em nuvem:** A grande maioria dos participantes (83,3%) afirmou utilizar serviços de computação em nuvem em suas organizações ou atividades pessoais. Essa alta taxa de utilização sugere que os serviços de computação em nuvem são considerados uma solução viável e conveniente para armazenamento, processamento e acesso a dados. Essa ampla adoção também reflete a crescente confiança na segurança e na eficácia dos serviços de nuvem por parte dos usuários.
- **Tipos de dados armazenados ou processados na nuvem:** Os tipos de dados armazenados ou processados na nuvem variam, mas a prevalência de dados pessoais (83,3%) destaca a importância da proteção da privacidade dos usuários. Além disso, o armazenamento de dados financeiros (38,9%) e dados confidenciais da empresa (44,4%) ressalta a necessidade de medidas de segurança robustas para proteger informações sensíveis.
- **Preocupações em relação à segurança dos dados na nuvem:** As principais preocupações dos participantes, incluindo violação de dados (66,7%), perda de dados (72,2%) e interrupção do serviço (50%), refletem as ameaças percebidas à segurança da computação em nuvem. Essas preocupações destacam a importância de abordagens proativas para mitigar riscos e garantir a continuidade dos serviços.

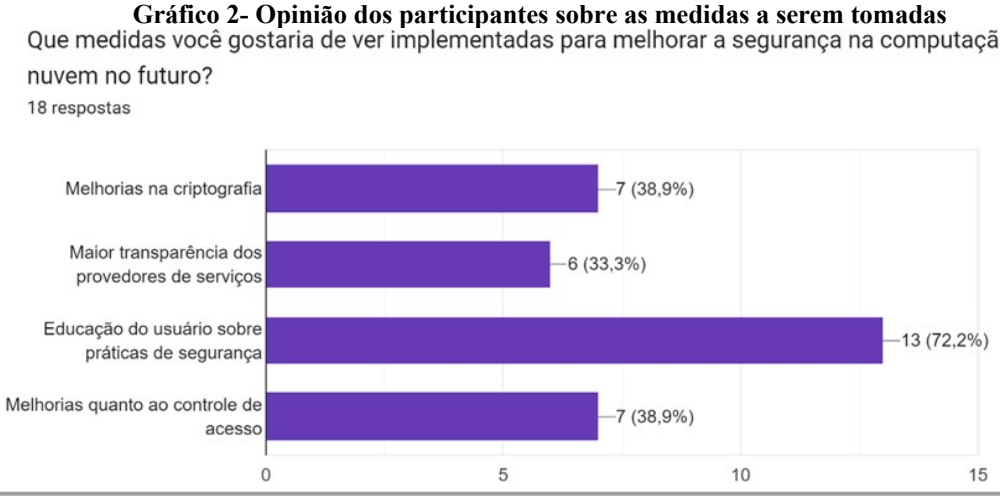
Gráfico 1- Preocupação dos usuários quanto a segurança dos dados



Fonte: Gráfico gerado a partir de entrevista realizada pelos autores (2024) por meio do Google Forms, com 18 participantes, abordando o uso e segurança de computação em nuvem.

- **Medidas de segurança consideradas importantes:** As medidas de segurança consideradas importantes pelos participantes, como criptografia de dados (77,8%) e controle de acesso rigorosos (66,7%), sugerem uma ênfase na proteção dos dados e na prevenção de acessos não autorizados. Além disso, a importância atribuída ao *backup* regular dos dados (72,2%) e ao monitoramento de segurança contínuo (55,6%) destaca a necessidade de estratégias abrangentes de proteção.
- **Confiança na segurança dos serviços de computação em nuvem:** A alta confiança na segurança dos serviços de computação em nuvem (88,9%) indica uma percepção geral positiva em relação aos provedores de serviços de nuvem líderes, embora seja importante manter a vigilância e implementar medidas adicionais de segurança para garantir a proteção dos dados.
- **Incidentes de segurança relatados:** Os incidentes de segurança relatados por uma minoria dos participantes (22,2%) destacam a realidade das ameaças à segurança na computação em nuvem e a importância de uma abordagem proativa para mitigar riscos e responder efetivamente a incidentes.
- **Medidas desejadas para melhorar a segurança na computação em nuvem no futuro:** Os participantes expressaram o desejo de ver implementadas melhorias na criptografia (38,9%), maior transparência dos provedores de serviço (33,3%), educação do usuário sobre práticas de segurança (72,2%) e melhorias no controle de acesso (38,9%). Essas respostas fornecem orientações valiosas para o desenvolvimento de estratégias de segurança mais eficazes e abrangentes.

Gráfico 2- Opinião dos participantes sobre as medidas a serem tomadas



Fonte: Gráfico gerado a partir de entrevista realizada pelos autores (2024) por meio do Google Forms, com 18 participantes, abordando o uso e segurança de computação em nuvem.

5 CONCLUSÃO

Após analisar os resultados da pesquisa e considerar a revisão bibliográfica realizada, torna-se evidente que a segurança na computação em nuvem é uma preocupação crescente para indivíduos e organizações que utilizam esse modelo de serviço. A maioria dos participantes demonstrou um nível moderado de familiaridade com os conceitos de segurança na nuvem, refletindo a necessidade de educação contínua nessa área. Apesar disso, a confiança na segurança dos serviços de nuvem foi alta, indicando uma percepção positiva em relação aos provedores de serviços. As principais preocupações dos participantes incluíram violação de dados, perda de dados e interrupção do serviço, destacando a importância de medidas de segurança robustas para proteger os dados na nuvem. Medidas como criptografia de dados e controle de acesso rigoroso foram consideradas essenciais para garantir a segurança dos dados na nuvem. Assim, com uma abordagem proativa, é possível mitigar os riscos associados à computação em nuvem e garantir a proteção dos dados confidenciais.

REFERÊNCIAS

ARMBRUST, M. *et al*. A view of cloud computing. **Communications of the ACM**, [s.l], abril, 2010, v. 53, n. 4. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/1721654.1721672>.

CLOUD COMPUTING: quais as revoluções trazidas pela computação em nuvem? **Empresa Júnior – Fundação Getúlio Vargas**. [s.d]. Disponível em: <https://ejfgv.com/cloud-computing/>. Acesso em: 15 set. 2024.

FERREIRA, J. **LGPD: O Escudo da Privacidade na Era da Conectividade**, 11 set. 2023. Disponível em: <https://www.dio.me/articles/lgpd-o-escudo-da-privacidade-na-era-da-conectividade>. Acesso em: 10 jan. 2024.

GOOGLE CLOUD. **Criptografia em trânsito,** set. 2022. Disponível em: <https://cloud.google.com/docs/security/encryption-in-transit?hl=pt-br>. Acesso em: 25 mar. 2024.

HARRISON, P. J. 88% of Cloud Breaches Are Due to Human Error: Here's How to Avoid Data Breaches. **The Fintech Times**, 9 mai. 2022. Disponível em:<https://thefintechtimes.com/88-of-cloud-breaches-are-due-to-human-error-heres-how-to-avoid-data-breaches/>. Acesso em: 10 set. 2024.

KASPERSKY.**O que é criptografia de dados?** Definição e explicação, [s.d.]. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/encryption>. Acesso em: 03 abr. 2024.

KOSINSKI, M.; FORREST, A**. What is identity and access management?** IAM, SSO, MFA and IDaaS definitions | IBM, 22 jan. 2024. Disponível em: <https://www.ibm.com/topics/identity-access-management>. Acesso em: 05 abr. 2024.

LOPES, P. **Computação em Nuvem:** Disponibilidade e Resiliência na Tecnologia. LinkedIn, 26 jan. 2023. Disponível em: <https://www.linkedin.com/pulse/computa%C3%A7%C3%A3o-em-nuvem-disponibilidade-e-resili%C3%AAncia-na-tecnologia>. Acesso em: 03 abr. 2024.

MARDUQUE, M. **Privacidade dos Dados em Cloud.** Linkedin, 7 jul. 2023. Disponível em: <https://pt.linkedin.com/pulse/privacidade-dos-dados-em-cloud-max-marduque-santana-da-costa>. Acesso em: 26 mar. 2024.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing.** National Institute of Standards and Technology, Special Publication 800-145, Gaithersburg, 2011. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-145/final>. Acesso em: 03 abr. 2024.

NOBLES, C. Investigating cloud computing misconfiguration errors using the human factors analysis and classification system. **Sciendo – Scientific Bulletin**. Vol. XXVII, No. 1(53), 2022. Disponível em: <https://intapi.sciendo.com/pdf/10.2478/bsaft-2022-0007>. Acesso em: 10 ago. 2024.

OLIVEIRA, J. H.; OLIVEIRA, W. A segurança de um banco de dados na AWS. **Ciências Exatas e da Terra**, v. 27, 2023. Disponível em: <https://revistaft.com.br/a-seguranca-de-um-banco-de-dados-na-aws/>. Acesso em: 21 jul. 2024.

RITTINGHOUSE, J. W.; RANSOME, J. F. **Cloud Computing:** Implementation, Management, and Security, 2009.

SUBASHINI, S.; KAVITHA, V. **A survey on security issues in service delivery models of cloud computing**. Journal of Network and Computer Applications, v. 34, n. 1, p. 1–11, jan. 2011.

TOTVS, E. **Criptografia: tipos, exemplos e importância nas empresas,** 2024. Disponível em: <https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/criptografia>. Acesso em: 02 abr. 2024.

KAMILA, K. **Role of cloud computing in modern libraries: A critical appraisal**. *International Journal of Information Library and Society*, v. 2, n. 1, p. 1-2, 2013.

PAGANINI, P. **Cloud misconfigurations are the most common cloud security risks**. Security Affairs, 28 abr. 2021. Disponível em: <https://securityaffairs.com/117305/security/cloud-misconfiguration-risks.html>. Acesso em: 15 abr. 2024.

LEAVITT, S.; REA, D. **Recomendações para monitoramento e detecção de ameaças.** *Microsoft Learn*, 13 fev. 2024. Disponível em: <https://learn.microsoft.com/pt-br/azure/well-architected/security/monitor-threats>. Acesso em: 16 abr. 2024.

LIMA, V.; SGARBI, E. **Pesquisa sobre o uso de computação em nuvem**. 2024. Pesquisa realizada via plataforma *Google Forms*. Local de pesquisa: Faculdade de Tecnologia de Taquaritinga (FATEC).