CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO: GERENCIAMENTO DE RISCOS EM TECNOLOGIAS APIS E COMPUTAÇÃO EM NUVEM

Autores: Felipe Henrique Martini, Maiara Soarde Fazan

Orientador: prof. Me Wdson de Oliveira

wdson.oliveira01@fatec.sp.gov.br

Resumo

A digitalização crescente e a interconectividade ampliada dos sistemas de informação têm desafiado significativamente a segurança da informação. A implementação de tecnologias como APIs e computação em nuvem, embora revolucionária na geração, transmissão e armazenamento de dados, traz consigo novas vulnerabilidades que devem ser gerenciadas de forma eficaz. As APIs, se não forem devidamente protegidas, podem criar pontos vulneráveis para acessos não autorizados. Além disso, a utilização de computação em nuvem para armazenamento e processamento de dados exige estratégias de segurança robustas para assegurar a confidencialidade, integridade e disponibilidade dos dados. Essas tecnologias, embora otimizem a gestão de dados, introduzem novas vulnerabilidades. A principal questão abordada é como gerenciar tecnologias de APIs e computação em nuvem para mitigar riscos e proteger as informações. O objetivo é buscar avaliar a segurança na implementação de APIs e computação em nuvem, identificando padrões e boas práticas a serem aplicadas, através do estudo de exemplos reais.

Palavras-chave: Segurança da informação, Computação em nuvem, APIs.

Abstract

The increasing digitalization and expanded interconnectivity of information systems have significantly challenged information security. The implementation of technologies such as APIs and cloud computing, while revolutionary in data generation, transmission, and storage, introduces new vulnerabilities that must be effectively managed. APIs, if not properly secured, can create entry points for unauthorized access. Additionally, the use of cloud storage and data processing requires robust security strategies to ensure data confidentiality, integrity, and availability. While these technologies optimize data management, they also introduce new risks. The main issue addressed is how to manage API and cloud computing technologies to mitigate risks and protect information. This study aims to assess security in API and cloud implementation, identifying applicable standards and best practices through the analysis of real-world examples.

Keywords: Information security, Cloud computing, APIs

Julho/2025

1. INTRODUÇÃO

O crescimento da Internet e da tecnologia criou uma interconexão contínua entre pessoas, máquinas e empresas, permitindo o desenvolvimento de produtos personalizados e competitivos para os consumidores. Essa evolução exige a utilização de ferramentas de previsão para processar dados de maneira sistemática, convertendo-os em informações que elucidam incertezas e facilitam decisões mais embasadas (Chiarini, 2014).

Com a ampliação da conectividade, surgem novos desafios relacionados à segurança da informação. A proteção dos dados transmitidos entre dispositivos e sistemas é fundamental para prevenir violações que possam comprometer a integridade e a confidencialidade das informações. A cibersegurança deve ser integrada desde o início do desenvolvimento, adotando técnicas como criptografia, autenticação robusta e monitoramento contínuo para identificar e neutralizar possíveis ameaças.

A segurança da informação de *Application Programming Interface* (API) é essencial para garantir a confiança e a credibilidade das aplicações e serviços que dependem dessas interfaces para funcionar corretamente. Ao implementar práticas de segurança robustas, como autenticação, autorização, criptografia e monitoramento de tráfego, as organizações podem proteger suas APIs contra ameaças e vulnerabilidades, assegurando a proteção dos dados e a continuidade das operações (Grégio et al., 2009).

A utilização de serviços de computação em nuvem para armazenamento de dados permite o acesso global e contínuo, eliminando a necessidade de instalar software ou manter dados localmente. O acesso a programas, serviços e arquivos é realizado remotamente pela Internet, o que justifica a expressão "nuvem". Esse modelo é considerado mais eficiente do que o uso de unidades físicas, proporcionando maior flexibilidade e conveniência.

A crescente digitalização e interconectividade dos sistemas de informação têm ampliado a complexidade da segurança da informação, especialmente com a aplicação de APIs e computação em nuvem. Essas tecnologias transformam a geração, transmissão e armazenamento de dados, mas introduzem novos desafios e vulnerabilidades. APIs podem expor pontos frágeis se não protegidas

adequadamente, e o armazenamento em computação em nuvem requer estratégias robustas para manter a confidencialidade, integridade e disponibilidade dos dados. A problemática central é como as organizações podem implementar e gerenciar essas tecnologias para mitigar riscos e garantir a segurança da informação em um ambiente digital cada vez mais complexo. Quais são os impactos e resultados na segurança da informação ao desenvolver APIs e adotar soluções em computação em nuvem?

O objetivo geral é avaliar a segurança da informação, com ênfase em APIs e computação em nuvem, e analisar os resultados decorrentes da implementação dessas tecnologias. Os objetivos específicos são analisar as práticas de cibersegurança e suas aplicações para proteger sistemas, redes e programas no ambiente digital; avaliar a implementação de criptografia e outras medidas de segurança para proteger dados transmitidos por APIs; analisar os desafios e estratégias de segurança na utilização de computação em nuvem para armazenamento e processamento de dados.

A relevância desse trabalho se dá pela crescente digitalização e interconectividade dos sistemas de informação, que introduzem novos desafios e vulnerabilidades. A análise da segurança da informação, especialmente no contexto da aplicação de APIs e computação em nuvem, é essencial para identificar e mitigar riscos. A compreensão dessas tecnologias e a implementação de estratégias de segurança são essenciais para proteger dados sensíveis, prevenir incidentes que possam comprometer a reputação das organizações e garantir a integridade, confidencialidade e disponibilidade das informações em ambientes digitais complexos.

Para complementar a revisão teórica e os estudos de caso analisados, este trabalho também incorporou uma pesquisa de campo com profissionais da área, com o intuito de compreender a realidade prática das organizações quanto à adoção segura de APIs e computação em nuvem.

2 REFERENCIAL TEÓRICO

2.1. Segurança da Informação e Cybersegurança

Carvalho (2023) cita que a Cibersegurança é essencialmente a prática de salvaguardar sistemas, redes e programas no ambiente digital de ataques mal-

intencionados. Ela incorpora a aplicação de técnicas como criptografia e a observância de diretrizes e regulamentos para prevenir danos tanto em hardware quanto em software. Esta área abrange uma variedade de instrumentos, políticas, estratégias de segurança, diretrizes, métodos de gestão de riscos, práticas recomendadas e tecnologias destinadas a proteger os ambientes digitais, as organizações e seus usuários. A proteção se estende a computadores, infraestruturas e sistemas de telecomunicações que armazenam informações valiosas no ambiente digital.

A finalidade da Cibersegurança é assegurar propriedades críticas como integridade, disponibilidade e confidencialidade das informações, mitigando riscos potenciais no ambiente digital. Além de focar na proteção do próprio ambiente digital, ela também visa proteger as operações que ocorrem dentro desse espaço e quaisquer ativos associados, diretamente ou indiretamente, com o ambiente digital (Moreira, 2023).

A segurança nos sistemas digitais representa um desafio tanto técnico quanto social. Do ponto de vista técnico, a crescente complexidade das arquiteturas de hardware, sistemas operacionais e protocolos exige políticas de segurança mais sofisticadas. Socialmente, a falta de conhecimento técnico entre os usuários dos sistemas de informação pode aumentar a vulnerabilidade a problemas de segurança (Gil, 2022).

Atualmente, as organizações enfrentam a necessidade urgente de garantir que seus sistemas sejam robustos o suficiente para resistir a ataques cibernéticos. Um ataque bem-sucedido pode acarretar custos elevados, prejudicando a reputação, o negócio e a estabilidade financeira da entidade afetada. Isso se deve à dificuldade de detectar ataques em tempo real e à crescente sofisticação das técnicas de ataque (Rabadão, 2021).

Nos últimos anos, o panorama dos ataques cibernéticos tem se tornado uma preocupação crescente para organizações e indivíduos globalmente. A prevalência destes ataques tem aumentado exponencialmente, impulsionada pela digitalização acelerada de serviços em diversas esferas da vida cotidiana. Ataques de *phishing*, *ransomware*, violações de dados e outras formas de ciberataques têm demonstrado não apenas sua frequência, mas também a

sofisticação crescente, causando impactos significativos que vão desde prejuízos financeiros substanciais até a perda de confiança e danos irreparáveis à reputação de entidades afetadas. O cenário atual exige soluções de cibersegurança mais robustas e inovadoras, capazes de combater essas ameaças digitais cada vez mais complexas e adaptativas (Val, 2024).

2.2. APIs (Interfaces de Programação de Aplicativos)

Grégio et al. (2009), as APIs desempenham um papel crucial na comunicação e interação entre diferentes softwares e sistemas. Elas definem as formas pelas quais os componentes de software podem se comunicar, permitindo a integração de funcionalidades e a troca de dados de forma estruturada. No contexto da segurança da informação, as APIs podem ser utilizadas para acessar e analisar registros de eventos gerados por sistemas, aplicativos e dispositivos, fornecendo insights valiosos sobre a atividade do sistema e possíveis ameaças à segurança.

De acordo com Castro (2023), no contexto da segurança do trabalho, as APIs desempenham um papel de permitir a comunicação entre diferentes sistemas e facilitar a integração de funcionalidades. As APIs são essenciais para garantir a proteção dos dados e informações sensíveis relacionadas à saúde e segurança dos trabalhadores. Dessa forma, as APIs são utilizadas para conectar sistemas de gestão de segurança do trabalho, permitindo a troca de informações relevantes, o monitoramento de dados de segurança, a geração de relatórios e a implementação de medidas preventivas. Essa integração entre diferentes plataformas e sistemas contribui significativamente para a eficiência na gestão da segurança do trabalho e para a garantia do cumprimento das normas e regulamentações vigentes (Castro, 2023).

Para Gonçalves e De Tárcis (2020), as APIs são fundamentais para executar operações de criptografia exigidas pelos aplicativos. Essas APIs, baseadas em sessões, oferecem serviços de descarregamento de algoritmos de criptografia e de transferência de protocolos para IPSec usando um conjunto variado de APIs. No contexto da segurança do trabalho, as APIs desempenham um papel crucial na implementação de mecanismos de criptografia, assegurando a integridade,

confidencialidade e autenticidade dos dados trafegados no plano de dados de redes definidas por software.

Além disso, ao analisar os logs gerados por APIs, os profissionais de segurança da informação podem identificar padrões de comportamento suspeitos, detectar atividades maliciosas, monitorar o tráfego de rede e responder rapidamente a incidentes de segurança (Grégio; Abed; et al., 2009). A visualização de dados provenientes desses logs, por meio de técnicas e ferramentas especializadas, pode facilitar a identificação de anomalias, a compreensão de tendências e a tomada de decisões informadas para fortalecer a segurança dos sistemas de informação.

De acordo com Castro (2023), a segurança da informação em APIs é essencial para garantir a integridade, confidencialidade e disponibilidade dos dados transmitidos e processados por meio dessas interfaces. Alguns dos principais aspectos sobre como ocorre a segurança da informação em APIs incluem:

1. **Conscientização dos riscos:** O ensino-aprendizagem em segurança da informação em APIs ajuda os alunos a compreender os riscos associados ao uso inadequado ou não seguro das APIs, incluindo a identificação de vulnerabilidades comuns e a aplicação das melhores práticas para mitigar esses riscos (Castro, 2023).
2. **Conhecimento de técnicas de proteção:** Os alunos aprendem técnicas e estratégias eficazes para proteger suas APIs contra-ataques, como métodos de autenticação segura, criptografia, validação de entrada, controle de acesso e monitoramento de atividades suspeitas (Castro, 2023).
3. **Habilidades de detecção e resposta a incidentes:** O ensino-aprendizagem em segurança da informação em APIs capacita os alunos a identificar e responder rapidamente a incidentes de segurança, detectando atividades suspeitas, investigando possíveis violações e tomando medidas corretivas adequadas (Castro, 2023).
4. **Preparação para carreiras em segurança**: O ensino-aprendizagem em segurança da informação em APIs prepara os alunos para carreiras em segurança cibernética, fornecendo as habilidades necessárias para enfrentar os desafios do mundo real e proteger efetivamente as APIs

desenvolvidas, garantindo a integridade e confidencialidade dos dados (Castro, 2023).

Esses são alguns dos aspectos abordados no trabalho que destacam a importância e as práticas relacionadas à segurança da informação em APIs.

De acordo com Grégio et al. (2009), a segurança da informação de API envolve a proteção dos dados e eventos gerados por interfaces de programação de aplicativos, garantindo a integridade, confidencialidade e disponibilidade das informações trocadas entre sistemas e aplicativos por meio dessas interfaces.

De acordo com Gonçalves e De Társis Cezare (2020), as APIs são essenciais para a Segurança da Informação, pois permitem a execução de operações de criptografia necessárias para garantir a integridade, confidencialidade e autenticidade dos dados trafegados no plano de dados de redes definidas por software. Além disso, as APIs são utilizadas para realizar testes de desempenho nas funções criptográficas da API OpenDataPlane (ODP) e avaliar diversos modelos de criptografia implementados na API em um Raspberry PI.

Essas operações são cruciais para proteger os dados transmitidos em ambientes de rede, assegurando que informações sensíveis sejam mantidas seguras contra acessos não autorizados e ataques cibernéticos. A capacidade de realizar criptografia eficiente e robusta através de APIs também permite que as organizações implementem rapidamente mecanismos de segurança avançados, adaptando-se às crescentes ameaças no cenário digital. Portanto, as APIs desempenham um papel vital na implementação de mecanismos de segurança e na garantia da proteção dos dados transmitidos em ambientes de rede (GONÇALVES; DE TÁRSIS CEZARE, 2020).

A importância da segurança da informação de API reside no fato de que as APIs são utilizadas para facilitar a comunicação e integração entre diferentes sistemas e serviços. Ao proteger as APIs e os dados que transitam por elas, as organizações podem evitar vazamentos de informações sensíveis, ataques cibernéticos e violações de segurança que possam comprometer a confidencialidade e a integridade dos dados (Grégio et al., 2009).

Assim, as APIs são essenciais para a Segurança da Informação, pois permitem a execução de operações de criptografia necessárias para garantir a integridade,

confidencialidade e autenticidade dos dados trafegados no plano de dados de redes definidas por software (Gonçalves; De Tárcis, 2020). Além disso, as APIs são utilizadas para realizar testes de desempenho nas funções criptográficas da API ODP e avaliar diversos modelos de criptografia implementados na API em um Raspberry PI 4.

2.3. Computação em nuvem

Cloud Computing é um modelo de serviço de Tecnologia da Informação (TI) em que recursos de computação, tanto hardware quanto software, são fornecidos sob demanda aos clientes por meio de uma rede de dados. Este modelo permite que os serviços sejam acessados de forma autosserviço, independentemente do dispositivo e da localização do usuário. Além disso, os recursos necessários para fornecer os níveis de qualidade de serviço exigidos são compartilhados, escaláveis de maneira dinâmica, provisionados rapidamente, virtualizados e liberados com o mínimo de interação com o provedor do serviço (MARCHISOTTI; JOIA; CARVALHO, 2019).

De acordo com Celegato (2011), o termo "*Cloud Computing*" refere-se a um modelo de computação em que os recursos de TI são disponibilizados como serviços pela internet. Este modelo permite o acesso a recursos computacionais compartilhados e configuráveis, como redes, servidores, armazenamento, aplicativos e serviços, que podem ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços.

Segundo a análise de Soldan, De Ávila e Neto (2017), a computação em nuvem tem se consolidado como uma solução eficiente para atender às crescentes necessidades dos usuários de tecnologia da informação. Esse modelo facilita o acesso a serviços de diversos locais através da Internet, utilizando diferentes dispositivos, incluindo computadores e dispositivos móveis. Com essas vantagens, muitas empresas estão optando por adotar a computação em nuvem.

De acordo com a definição do NIST (National Institute of Standards and Technology), a computação em nuvem é descrita como um modelo que oferece acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, como redes, servidores, armazenamento, aplicações e serviços. Esses

recursos podem ser obtidos e liberados com um mínimo de esforço gerencial ou interação com o provedor de serviços (SOLDAN; DE ÁVILA; NETO, 2017).

Segundo Marchisotti, Joia e Carvalho (2019), a segurança da informação no contexto da computação em nuvem envolve a proteção dos dados, informações, softwares e aplicativos que são armazenados remotamente no ambiente de computação em nuvem. Este conceito abrange a garantia de privacidade, sigilo e confidencialidade das informações dos usuários.

No contexto da Segurança da Informação, a utilização de serviços em nuvem apresenta desafios e preocupações específicas relacionadas à proteção dos dados e sistemas. A segurança em computação em nuvem envolve questões como integridade, confidencialidade, disponibilidade, autenticidade e não repúdio dos dados armazenados e processados na nuvem (CELEGATO, 2011).

Ademais, é importante que as organizações usuárias da tecnologia computação em nuvem tenham visibilidade da segurança aplicada na nuvem, incluindo transparência nos processos de mudança, gerenciamento de incidentes e emissão de relatórios de auditoria aos clientes da nuvem. A visibilidade do cliente é fundamental para garantir a eficácia da segurança na nuvem (CELEGATO, 2011).

Assim, os usuários pagam pelo serviço como uma despesa operacional, evitando a necessidade de grandes investimentos iniciais. Os serviços em nuvem utilizam um sistema de medição que divide o recurso de computação em blocos apropriados, facilitando a cobrança baseada no uso real dos recursos (MARCHISOTTI; JOIA; CARVALHO, 2019).

De acordo com Soldan, De Ávila e Neto (2017), o uso da computação em nuvem para a segurança da informação resulta em uma estrutura de Disaster Recovery Plan (DRP) que garante a criptografia dos dados sem maiores interferências, proporcionando segurança para as empresas que utilizam essa tecnologia. Isso significa que, quando implementada corretamente com um plano de recuperação de desastres eficaz, a computação em nuvem pode contribuir significativamente para a proteção dos dados e a privacidade das informações das organizações.

A estrutura de DRP em computação em nuvem é projetada para assegurar a continuidade das operações em caso de falhas ou desastres, oferecendo medidas de

proteção robustas, como a criptografia dos dados em trânsito e em repouso. Essas medidas são essenciais para proteger os dados contra acessos não autorizados e outras ameaças à segurança. Portanto, a computação em nuvem, quando associada a um plano de recuperação de desastres bem estruturado, pode proporcionar um ambiente seguro e resiliente para as organizações, garantindo a integridade, confidencialidade e disponibilidade das informações críticas (SOLDAN; DE ÁVILA; NETO, 2017).

A falta de controle total sobre os dados e processos na nuvem, comparada aos ambientes tradicionais *in-house*, é uma preocupação significativa. A necessidade de criar planos de contingência e Acordos de Níveis de Serviço (SLA) para garantir a confiabilidade e minimizar os impactos de desastres também é destacada como uma questão crucial na segurança em computação em nuvem (CELEGATO, 2011).

Celegato (2011), a utilização de computação em nuvem traz tanto benefícios quanto desafios para a segurança da informação. Entre os benefícios, destacam-se a redução de custos, menor capital de investimento e menor risco de perda de dados, uma vez que os dados estão armazenados na "web". No entanto, persiste a desconfiança em relação à eficácia da computação em nuvem, especialmente quanto à integridade, confidencialidade, disponibilidade, autenticidade e não repúdio dos dados na nuvem.

3. METODOLOGIA

Este estudo enquadra-se nas categorias de pesquisa exploratória e descritiva em termos de seus objetivos, aplicando-se ao tema de segurança da informação com ênfase em APIs e computação em nuvem. Para a sua elaboração, teve como base a revisão bibliográfica, com análise de materiais já publicados, como livros, sites e artigos científicos, e a análise de casos reais.

A metodologia adotada consiste no levantamento de literatura sobre segurança da informação, APIs e computação em nuvem, com base em artigos científicos, normativas internacionais (NIST e ISO/IEC 27001) e relatórios de cibersegurança. Complementarmente, foram analisados estudos de caso sobre incidentes de segurança, selecionados com base em sua relevância e considerando apenas casos

amplamente reportados, para a aplicação de conceitos teóricos e avaliação da eficiência das soluções identificadas.

Além da revisão bibliográfica e análise documental, foi aplicada uma pesquisa quantitativa por meio de um questionário estruturado com nove perguntas, direcionado a profissionais da área de tecnologia da informação. A coleta de dados ocorreu no mês de maio de 2025, utilizando formulário online. O questionário obteve 10 respostas válidas, com perguntas relacionadas ao uso de APIs e computação em nuvem, práticas de segurança, incidentes enfrentados, eficácia das medidas adotadas e percepção sobre custo-benefício dos investimentos.

Através desses recursos, os pesquisadores contribuem para o conhecimento na área de segurança da informação, especialmente no contexto das APIs e computação em nuvem, fornecendo insights valiosos e fundamentos teóricos para a análise e discussão dos dados.

4. **ANÁLISE E DISCUSSÃO DOS RESULTADOS**

A análise dos dados coletados na pesquisa de campo e nos estudos de caso demonstrou que a segurança em APIs e ambientes de computação em nuvem continua sendo um desafio crítico. As organizações enfrentam dificuldades tanto na aplicação de políticas preventivas quanto na resposta a incidentes, especialmente diante da complexidade crescente das arquiteturas e da limitação técnica dos usuários.

Os casos analisados, como o do Facebook e o da Capital One, revelam falhas comuns, como ausência de autenticação robusta e configuração inadequada de permissões na nuvem. Esses incidentes reforçam a necessidade de práticas como controle de acesso rigoroso, revisão contínua de configurações e monitoramento de anomalias para prevenir vazamentos de dados.

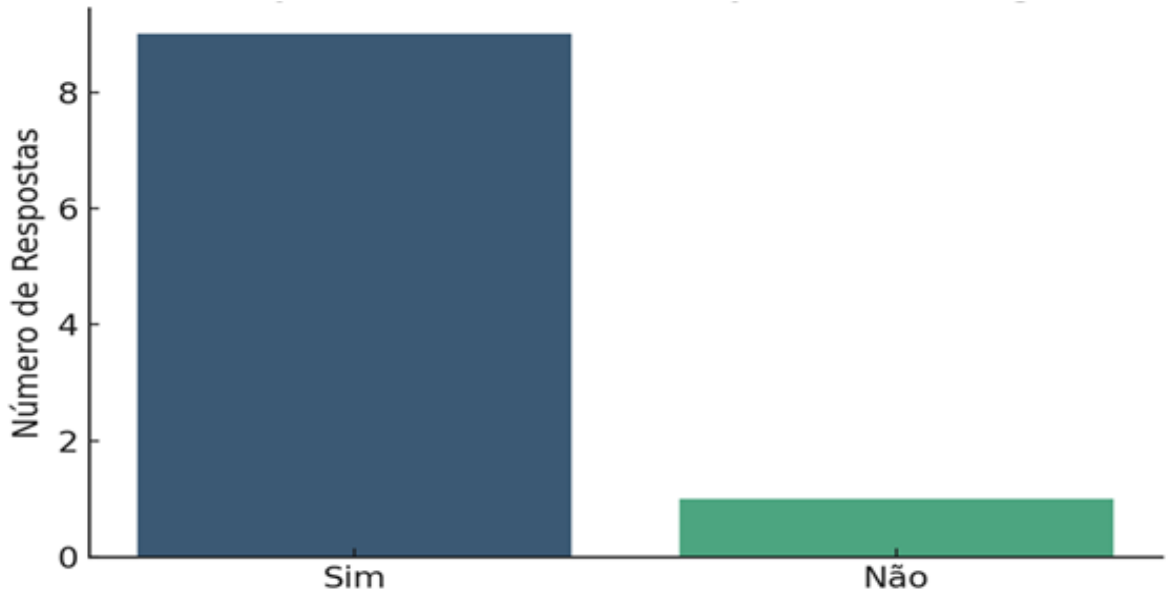
A pesquisa de campo indicou que muitas empresas ainda não adotam integralmente soluções como autenticação multifator, segmentação de rede baseada em risco ou criptografia de ponta a ponta. Essa lacuna evidencia a importância de alinhar estratégias de segurança com os riscos reais observados, priorizando ações proativas em vez de reativas.

Com o objetivo de aprofundar a compreensão sobre os desafios enfrentados pelas empresas no uso seguro de APIs e computação em nuvem, foi aplicada uma pesquisa com profissionais da área de tecnologia da informação. O questionário contou com a participação de 10 respondentes e foi estruturado com perguntas sobre a adoção dessas tecnologias, os incidentes enfrentados, as medidas de segurança implementadas e a percepção sobre sua eficácia e custo-benefício.

A pesquisa revelou que a maioria dos participantes atuam em funções diretamente relacionadas ao desenvolvimento ou gestão de sistemas, o que lhes confere uma perspectiva relevante sobre o tema. Em seguida, buscou-se entender a adoção de tecnologias-chave nas empresas dos participantes.

Os resultados, conforme Figura 1, indicam que um número significativo das empresas representadas pelos respondentes já incorpora APIs em suas soluções, ressaltando a relevância da segurança nesse ecossistema.

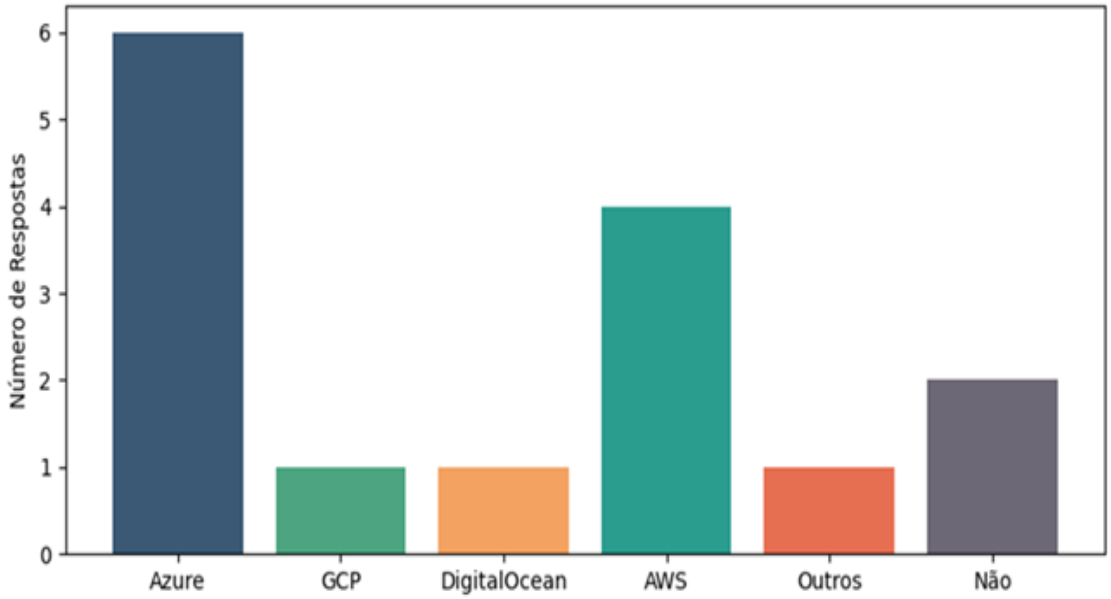
Figura 1 – Utilização de APIs em soluções tecnológicas.



Fonte: Os autores (2025).

Complementarmente, a pesquisa investigou o uso de serviços de computação em nuvem e os provedores preferenciais, conforme a Figura 2.

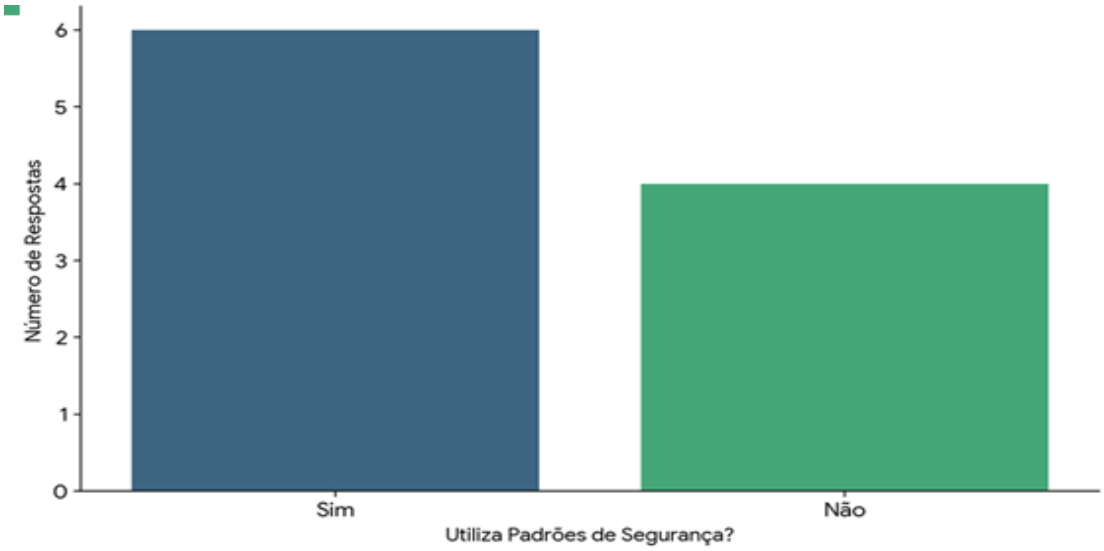
Figura 2 – Utilização de serviços de computação em nuvem.



Fonte: Os autores (2025).

A ampla adoção de serviços de nuvem, com destaque para provedores como AWS e Azure, demonstra a centralidade dessas plataformas no cenário tecnológico atual, justificando a preocupação com a segurança de seus ambientes. Para avaliar a aderência a boas práticas, questionou-se sobre a utilização de padrões de segurança formais, conforme apresentado na Figura 3.

Figura 3 – Utilização de Padrões de segurança (ISO 27001, NIST).

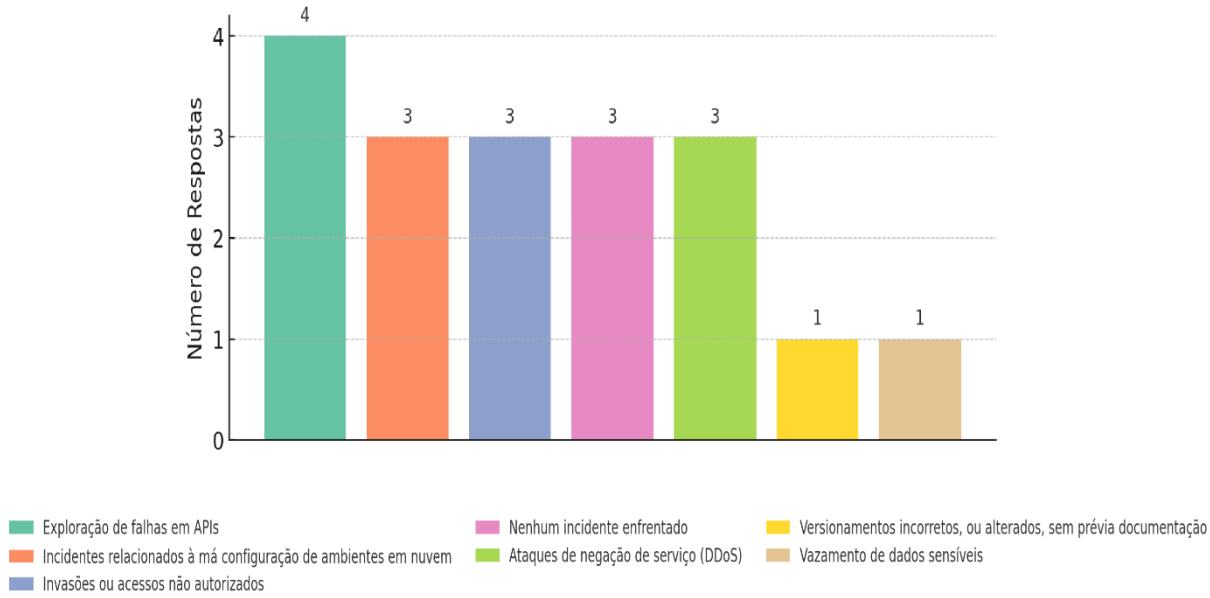


Fonte: Os autores (2025).

Ainda que a maioria das empresas utilize padrões de segurança, há espaço para maior conscientização e implementação desses referenciais. Entre os resultados obtidos sobre incidentes, destaca-se que 6 dos 10 profissionais (60%) relataram que suas empresas já enfrentaram algum tipo de incidente relacionado a APIs ou computação em nuvem.

Conforme mostra a Figura 4, os incidentes mais comuns incluem exploração de falhas em APIs, acessos não autorizados e ataques de negação de serviço (DDoS). Também foram relatados casos de vazamentos de dados sensíveis e versionamentos incorretos, ainda que em menor proporção. Esses dados reforçam a importância de uma abordagem preventiva e alinhada às boas práticas de segurança.

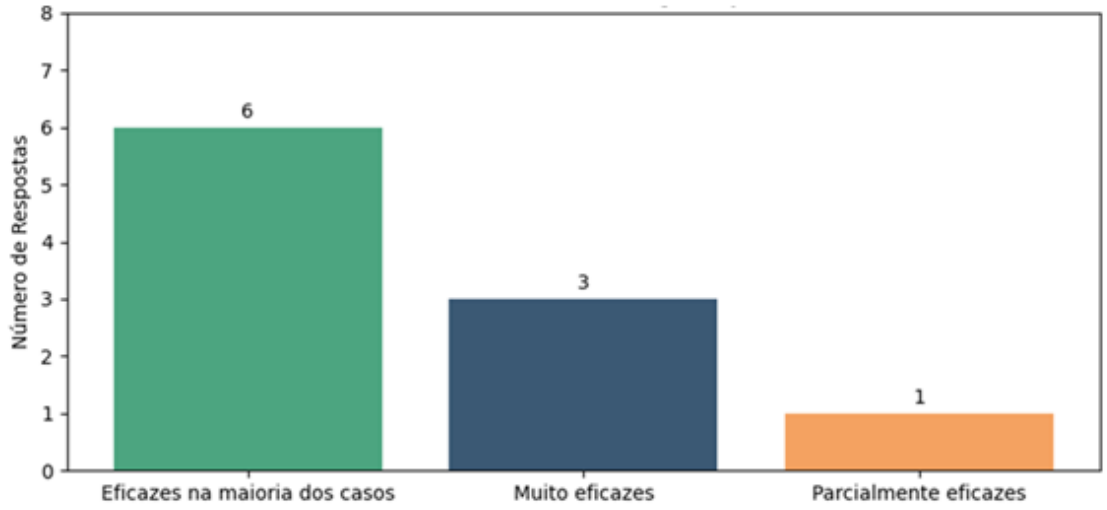
Figura 4 – Eficácia das medidas de segurança adotadas.



Fonte: Os autores (2025).

A respeito da eficácia das medidas de segurança adotadas, os resultados são apresentados na Figura 5.

Figura 5 – Eficácia das medidas de segurança adotadas.

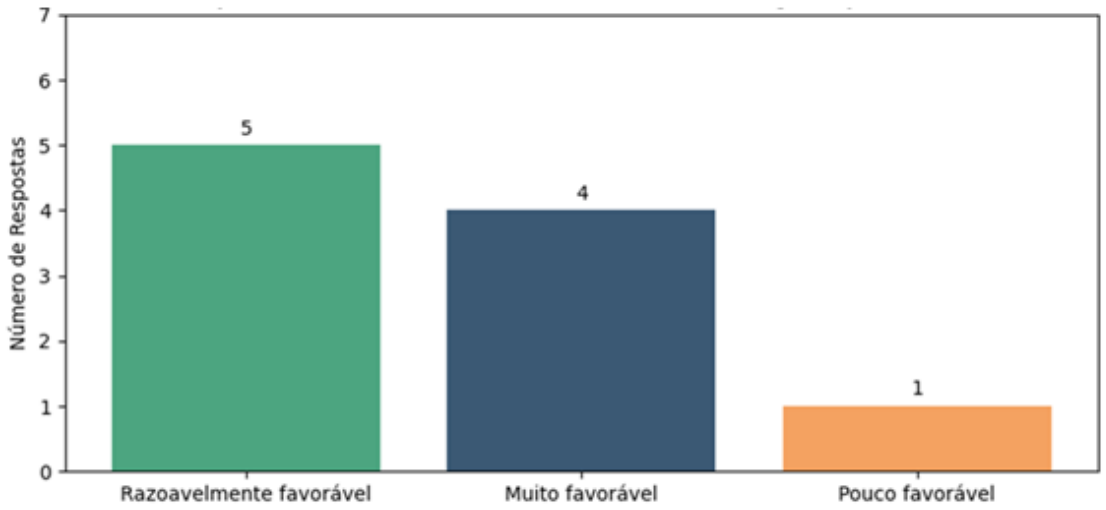


Fonte: Os autores (2025).

Conforme a Figura 5, apenas 3 dos 10 respondentes (30%) consideraram as medidas de segurança como "Muito eficazes", enquanto 6 dos 10 (60%) afirmaram que são "eficazes na maioria dos casos, mas com pontos a melhorar". Apenas 1 dos 10 (10%) considerou as medidas "parcialmente eficazes", sugerindo que há um espaço significativo para revisão e fortalecimento das políticas de segurança em muitas organizações.

Finalmente, a pesquisa avaliou a percepção sobre a relação custo-benefício dos investimentos em segurança da informação, conforme a Figura 6.

Figura 6 – Avaliação do Custo-Benefício de investimentos em segurança (APIs/Cloud).



Fonte: Os autores (2025).

A Figura 6 mostra que 5 dos 10 profissionais (50%) indicaram que os custos são justificados pelos benefícios obtidos ("Razoavelmente favorável"), enquanto 4 dos 10 (40%) avaliaram que o retorno é "Neutro". Apenas 1 dos 10 (10%) acredita que os custos superam os benefícios ("Pouco favorável"), o que sinaliza uma percepção positiva, ainda que moderada, sobre o valor estratégico da segurança.

Esses resultados contribuem para reforçar os argumentos discutidos ao longo do trabalho, especialmente sobre a necessidade de medidas como autenticação forte, criptografia de dados e auditorias regulares. Eles também

destacam a importância de uma gestão estratégica de riscos, com foco não apenas em conformidade, mas em eficácia operacional e sustentabilidade da segurança digital.

A segurança de APIs e computação em nuvem em ambientes corporativos representa um grande desafio atualmente. Principalmente com o crescente número de ataques cibernéticos. Um caso real que evidência isso é o do Facebook, que em 2018, por uma falha em APIs permitiu que hackers acessassem tokens de acesso de cerca de 50 milhões de usuários, comprometendo informações e dados pessoais sensíveis. Esse incidente destacou a importância da implementação de autenticação e controle e monitoramento contínuo de acessos. Já no caso da Capital One, em 2019, um vazamento de dados afetou mais de 100 milhões de clientes devido a uma configuração incorreta de permissões na nuvem da AWS, uma vulnerabilidade que poderia ser evitada com políticas rigorosas de controle de acesso e revisão de configurações.

Empresas como a Google e a Microsoft têm implementado autenticação multifator (MFA), segmentação de rede baseada em risco e monitoramento proativo de anomalias. Essas práticas demonstram como uma abordagem preventiva pode mitigar ameaças.

Diante dos casos expostos, podemos adotar como solução, algumas boas práticas para garantir a segurança dessas tecnologias, como a implementação de protocolos seguros de autenticação e autorização, como O Auth 2.0 e OpenID Connect, para evitar acessos não autorizados. O uso de criptografia AES-256 para armazenamento e TLS 1.2 ou superior para transmissão garante a proteção dos dados em trânsito. O monitoramento contínuo de acessos e a análise de logs com ferramentas como AWS CloudTrail e Google Cloud Security Command Center são bastante úteis para detectar atividades suspeitas. O princípio do menor privilégio pode ser adotado, garantindo que os acessos sejam concedidos apenas na medida estritamente necessária para o desempenho dos cargos e com base nas funções exercidas. Ademais, auditorias regulares e testes de penetração devem ser conduzidos periodicamente para verificar a eficácia das medidas de segurança já implementadas. O gerenciamento de vulnerabilidades

por meio da adoção de sistemas de detecção e resposta a ameaças, como SIEM e firewalls de próxima geração, também é uma medida recomendada.

5. CONSIDERAÇÕES FINAIS

A integração de tecnologias como APIs e computação em nuvem oferece inúmeros benefícios, incluindo maior eficiência operacional, melhorias na produtividade e personalização de produtos e serviços. No entanto, essas tecnologias também aumentam a superfície de ataque, exigindo medidas de segurança mais avançadas e integradas. A análise realizada deixa claro que a segurança da informação em APIs e computação em nuvem depende de estratégias robustas de proteção, envolvendo criptografia, controle de acesso, monitoramento contínuo e conformidade com padrões reconhecidos. O estudo de casos, como o do Facebook e o da Capital One, reforça a necessidade de revisões periódicas nas configurações e da implementação de soluções automatizadas para identificação de vulnerabilidades, como o monitoramento de logs.

No âmbito da cibersegurança, a aplicação de APIs e computação em nuvem demanda uma abordagem multidisciplinar. Desenvolver e implementar estratégias de segurança que contemplem tanto aspectos técnicos quanto sociais é imperativo. A complexidade crescente das arquiteturas de hardware e software, combinada com a falta de conhecimento técnico entre usuários, aumenta a necessidade de soluções inovadoras e robustas para proteger sistemas de informação. A mitigação de riscos e a proteção de informações exigem uma abordagem proativa e contínua, adaptando-se às novas ameaças e evoluções tecnológicas.

Portanto, os impactos e resultados da aplicação de APIs e computação em nuvem na segurança da informação são profundos e diversos. Eles requerem uma gestão cuidadosa e estratégias de segurança bem definidas para minimizar vulnerabilidades e proteger os dados. O sucesso na implementação dessas tecnologias depende da adoção de práticas de segurança avançadas, que assegurem a integridade, confidencialidade e disponibilidade das informações em um cenário digital cada vez mais complexo e interconectado. A colaboração entre profissionais de TI, desenvolvedores e gestores é vital para criar um ambiente digital seguro e

resiliente, capaz de enfrentar ameaças cibernéticas emergentes e proteger os ativos digitais das organizações.

Diante do exposto, a transformação tecnológica trazida pelas APIs e computação em nuvem representa tanto oportunidades quanto desafios significativos para a segurança da informação. Com a digitalização continuando a avançar, é essencial que as organizações permaneçam vigilantes e proativas na proteção de seus sistemas de informação, garantindo a segurança, integridade e confiabilidade dos dados em um ambiente digital dinâmico.

Este estudo destacou a adoção de boas práticas a fim de contribuir para a segurança de APIs e computação em nuvem. Entretanto, a crescente evolução das ameaças e ataques digitais exige atualizações constantes nas estratégias de proteção. Os dados obtidos na pesquisa aplicada reforçam as evidências teóricas ao demonstrar que, embora muitas empresas adotem boas práticas, ainda enfrentam vulnerabilidades críticas. A percepção dos profissionais sobre a eficácia e o custo-benefício das medidas de segurança adotadas também oferece subsídios práticos para a formulação de políticas mais eficazes nas organizações. Como limitação, este trabalho baseou-se apenas em estudos documentados e na pesquisa de campo realizada, sem experimentação prática, e sugere-se ser explorado em pesquisas futuras, incluindo o estudo sobre o impacto de tecnologias como a inteligência artificial e o machine learning aplicadas na segurança de APIs e computação em nuvem.

REFERÊNCIAS

AMAZON WEB SERVICES (AWS). AWS Security Best Practices. Disponível em: https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/aws-security-best-practices.html. Acesso em: 19 mar. 2025.

ARATA, Estefânia A. Pianoski; NASCIMENTO, Maikol; DE NOVAIS, Caroline Batista Fantini. SEGURANÇA DA INFORMAÇÃO PARA APLICAÇÕES IOT–INTERNET OF THINGS. **South American Development Society Journal**, v. 6, n. 18, p. 301, 2020.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 19 mar. 2025.

CAPITAL ONE. Capital One Cyber Incident, 2019. Disponível em: https://www.capitalone.com/digital/cyber-incident/. Acesso em: 19 mar. 2025.

CARVALHO, André Ferreira Almeida de; SANTOS, Christyan Matteus Lima; GONÇALVES, Lucas Vaz. Segurança em IoT. 2022.

CASTRO, Ricardo Henrique Rodrigues de. Desenvolvimento de uma artefato para aprendizado sobre segurança da informação em APIs. 2023. Trabalho de Conclusão de Curso. Brasil.

CELEGATO, Angélica Cristina. Segurança em cloud computing. 2011.

CLOUD SECURITY ALLIANCE (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 2017. Disponível em: https://cloudsecurityalliance.org/. Acesso em: 19 mar. 2025.

GONÇALVES, João Gabriel Rangel; DE TÁRSIS CEZARE, Thales. A análise de desempenho das funções criptográficas implementadas na API OpenDataPlane (ODP). **Prospectus (ISSN: 2674-8576)**, v. 2, n. 1, 2020.

GRÉGIO, André Ricardo Abed et al. Técnicas de Visualização de Dados aplicadas à Segurança da Informação. Sociedade Brasileira de Computação, 2009.

GOOGLE CLOUD. Security foundations blueprint guide. Google Cloud, 2023. Disponível em: https://cloud.google.com/security. Acesso em: 19 mar. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27001:2013 - Information security management systems – Requirements. ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

MARCHISOTTI, Gustavo Guimarães; JOIA, Luiz Antonio; CARVALHO, Rodrigo Baroni de. A representação social de cloud computing pela percepção dos profissionais brasileiros de tecnologia da informação. **Revista de Administração de Empresas**, v. 59, n. 1, p. 16-28, 2019.

MICROSOFT CORPORATION. Zero Trust Adoption Framework. Microsoft Security, 2023. Disponível em: https://www.microsoft.com/security. Acesso em: 19 mar. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Security and Privacy Controls for Information Systems and Organizations. Special Publication 800-53. Disponível em:

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Acesso em: 19 mar. 2025.

OWASP. OWASP API Security Top 10, 2023. Disponível em: https://owasp.org/www-project-api-security/. Acesso em: 19 mar. 2025.

PONTAROLLI, Ricardo Pasquati et al. Automação e Controle de Processos usando Microsserviços: Uma solução para a aplicação da Indústria 4.0.

Relatórios de Incidentes: FACEBOOK. Facebook Security Incident, 2018. Disponível em: https://about.fb.com/news/2018/09/security-update/. Acesso em: 19 mar. 2025.

SOLDAN, Evandro Luis; DE ÁVILA, Cleiton Silva; NETO, Silvio Petroli. A SEGURANÇA DE UMA ESTRUTURA DE DISASTER RECOVERY PLAN EM CLOUD COMPUTING. **Ensaios USF**, v. 1, n. 1, p. 103-116, 2017.
UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). Jornal Oficial da União Europeia, 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 19 mar. 2025.