Controle de Acesso de Terceiros no Gerenciamento de Identidade e Acesso: Uma Revisão da Literatura

Michelle Lícia S. Silva[1], Fernando A. A. Lins[1]

Departamento de Computação - Universidade Federal Rural de Pernambuco[1]
{michellelicia98@gmail.com, fernandoaires@ufrpe.br}

Resumo

O Gerenciamento de Identidade e Acesso (IAM) é composto por um conjunto de processos, políticas e tecnologias desenvolvidas para garantir que as pessoas tenham acesso à proteção aos recursos necessários, no momento adequado e por motivos justificáveis. O presente estudo tem como objetivo geral realizar uma revisão sistemática para investigar as soluções eficazes para o controle de acesso de terceiros no gerenciamento de identidade e acesso, com foco em garantir a segurança da informação e a conformidade regulatória. Este estudo utiliza uma revisão sistemática com abordagem qualitativa para explorar as melhores práticas, desafios e soluções relacionadas ao controle de acesso de terceiros no IAM. Através desta revisão, se verifica que o equilíbrio entre segurança, eficiência operacional e conformidade regulatória é o caminho para o sucesso do controle de acesso. Este estudo reforça a necessidade de aprofundar a investigação acadêmica sobre o tema, explorando novas abordagens e inovações que possam atender às demandas futuras de segurança e proteção de dados.

Palavras-chave: *Acesso de terceiros, Controle, Gerenciamento, Risco de terceiros.*

Abstract

Identity and Access Management (IAM) consists of a set of processes, policies, and technologies designed to ensure that individuals have access to the necessary resources with adequate protection, at the right time, and for justifiable reasons. This study aims to conduct a systematic review to investigate effective solutions for third-party access control in IAM, focusing on ensuring information security and regulatory compliance. A systematic review with a qualitative approach is used to explore best practices, challenges, and solutions related to third-party access control in IAM. Through this review, it is observed that balancing security, operational efficiency, and regulatory compliance is the key to successful access control. This study reinforces the need for further academic research on the subject, exploring new approaches and innovations that can meet future demands for security and data protection.

Keywords: *Third-party access, Control, Management, Third-party risk.*

1 Introdução

Nos últimos anos, com o avanço da transformação digital e a crescente dependência de sistemas informatizados nas organizações, o gerenciamento de identidade e acesso (IAM, do inglês Identity and Access Management) emergiu como uma área estratégica para a segurança da informação. O IAM consiste em um conjunto de processos, políticas e tecnologias específicas para garantir que os indivíduos corretos tenham acesso adequado aos recursos certos, no momento oportuno e por razões justificadas (FERNANDES; SOARES, 2020). Dentro desse escopo, o controle de acesso de terceiros tornou-se um desafio relevante devido à crescente interação de fornecedores, contas de serviço e parceiros externos com os sistemas internos das organizações (GARTNER, 2021).

Inicialmente, as redes de comunicação foram concebidas com propósitos acadêmicos e de pesquisa, tendo como foco a facilitação da conectividade entre os envolvidos, com pouca atenção à segurança. Contudo, com o aumento da demanda comercial e o uso estratégico dessas redes, a Segurança da Informação (SI) tornou-se uma prioridade para as organizações, que precisam proteger seus dados e sistemas contra ameaças (STALLINGS, 2019). A evolução das novidades cibernéticas e a complexidade dos ambientes tecnológicos atuais intensificaram a necessidade de medidas preventivas e reativas, transformando a segurança em elemento indispensável da governança corporativa (LIU et al., 2020).

A integração de terceiros ao ambiente corporativo requer níveis adicionais de segurança e gestão, considerando que, muitas vezes, esses proprietários têm acesso amplo e crítico (FARAHANI et al., 2022). Essa situação aumenta significativamente a superfície de ataque e o risco de exposição de dados sensíveis, sendo essencial implementar soluções robustas e eficazes para mitigar vulnerabilidades (MAVROULAS et al., 2021). O gerenciamento ineficaz desses acessos pode expor as organizações à transparência de dados e perdas financeiras expressivas, ou que reforçam a necessidade de práticas estruturadas e políticas consistentes (BESENYI; SHU; STALLINGS, 2020).

No contexto corporativo atual, o gerenciamento de identidade e acesso tornou-se cada vez mais essencial e desafiador. O crescimento constante da digitalização de processos e a ampliação do acesso a sistemas e informações importantes destacam a necessidade de um controle de acesso eficiente, inclusive para terceiros (KHAN; JAVED, 2023). O controle de acesso de terceiros representa um componente crucial no gerenciamento de identidade e acesso nas organizações (GARTNER, 2021). A falta de visibilidade e o controle inadequado desses acessos podem comprometer a resiliência cibernética, colocando em risco a continuidade do negócio (SENEVIRATNE; MOHAMMED, 2022).

Ao adotar práticas recomendadas e soluções adequadas, é possível mitigar os riscos de segurança associados a acessos não autorizados por parte de terceiros. Nesse sentido, a implementação de políticas claras, procedimentos rigorosos, monitoramento contínuo e tecnologias robustas é essencial para garantir a proteção eficaz de sistemas e dados corporativos (ISO/IEC 27001:2022). Entretanto, no estado atual da arte da área, observa-se uma lacuna em relação aos estudos sistematizados que abordem, de forma abrangente e profunda, as técnicas, processos e inovações que apoiam o controle de acesso de terceiros no âmbito do gerenciamento de identidade e acesso (IAM) (SCHNEIER, 2023).

O problema de pesquisa deste estudo é: "Como as organizações podem gerenciar o controle de acesso de terceiros, garantindo a segurança da informação e a conformidade regulatória?" Este problema ganha relevância em um cenário onde incidentes de segurança frequentemente decorrem de acessos indevidos ou comprometidos por atores externos.

O problema se agrava quando consideramos o contexto regulatório, como as exigências da Lei Geral de Proteção de Dados (LGPD) no Brasil e do Regulamento Geral de Proteção de Dados (GDPR) na Europa, que impõem diretrizes rigorosas sobre o acesso, tratamento e proteção de informações pessoais e corporativas (Brasil, 2018). A falta de uma gestão adequada de acesso pode resultar não apenas em perdas financeiras, mas também em danos à reputação e penalidades legais severas.

A justificativa para a escolha deste tema reside na importância crescente do gerenciamento de identidade e acesso no contexto organizacional moderno. Com o aumento de ataques cibernéticos direcionados a terceiros, torna-se indispensável que as organizações adotem estratégias efetivas de controle de acesso. A relevância deste tema está ancorada em seu impacto direto na proteção de ativos digitais e na construção de relações de confiança com stakeholders externos. À medida que as organizações se tornam cada vez mais dependentes de terceiros para suas operações, um IAM bem estruturado não é apenas desejável, mas essencial.

O presente estudo tem como objetivo geral realizar uma revisão sistemática para investigar as soluções existentes para o controle de acesso de terceiros no gerenciamento de identidade e acesso, com foco em garantir a segurança da informação e a conformidade regulatória. Os seguintes objetivos específicos emergem neste contexto: analisar os principais desafios e vulnerabilidades associados ao acesso de terceiros em organizações, identificar práticas e tecnologias inovadoras utilizadas no gerenciamento de identidade e acesso e avaliar o impacto das regulamentações LGPD e GDPR no controle de acesso de terceiros.

2 Metodologia

Este estudo utiliza uma revisão sistemática com abordagem qualitativa para explorar as melhores práticas, desafios e soluções relacionadas ao controle de acesso de terceiros no gerenciamento de identidade e acesso. Segundo Gunther (2016), uma vantagem da abordagem qualitativa é utilizar “dados que ocorrem naturalmente para encontrar sequências em que os significados dos participantes são exibidos e, assim, estabelecer o caráter de algum fenômeno”.

A busca dos artigos e coleta de dados foi realizada por meio das bases de dados renomadas, como: Scielo, Capes, ACM Digital Library. Foram utilizadas as strings de busca como: "controle de acesso de terceiros" OR "gerenciamento de identidade e acesso" OR "segurança da informação" OR "gerenciamento de risco de terceiros" AND "third-party access control" OR "identity and access management" OR "information security" OR "third-party risk management". A combinação de termos seguiu estratégias booleanas para refinar os resultados.

Os critérios de inclusão foram: 1) dissertações, artigos publicados em periódicos acadêmicos revisados por pares, 2) estudos publicados nos últimos 5 anos entre 2015 e 2025, 3) trabalhos que abordem especificamente o controle de acesso de terceiros ou questões relacionadas ao gerenciamento de identidade e acesso e 4) artigos escritos em inglês ou português.

Já os critérios de exclusão contemplaram: 1) resumos em eventos, 2) estudos com foco exclusivo em outros aspectos da segurança da informação que não envolvam o controle de acesso de terceiros, 3) publicações em formato de opinião ou revisões não sistemáticas e 4) artigos que não apresentem dados empíricos ou análises detalhadas.

Após a primeira seleção baseada nas strings de busca selecionadas, foram lidos os títulos dos artigos, e os que não abordaram o tema específico foram excluídos. A análise foi realizada após a leitura do resumo e do conteúdo integral do artigo. Em cada etapa, foi registrada a quantidade de estudos selecionados para a confecção do fluxograma, referente ao processo de seleção. Além disso, foram anotados os motivos de exclusão dos demais estudos, conforme ilustrado no Fluxograma apresentado na Figura 1.

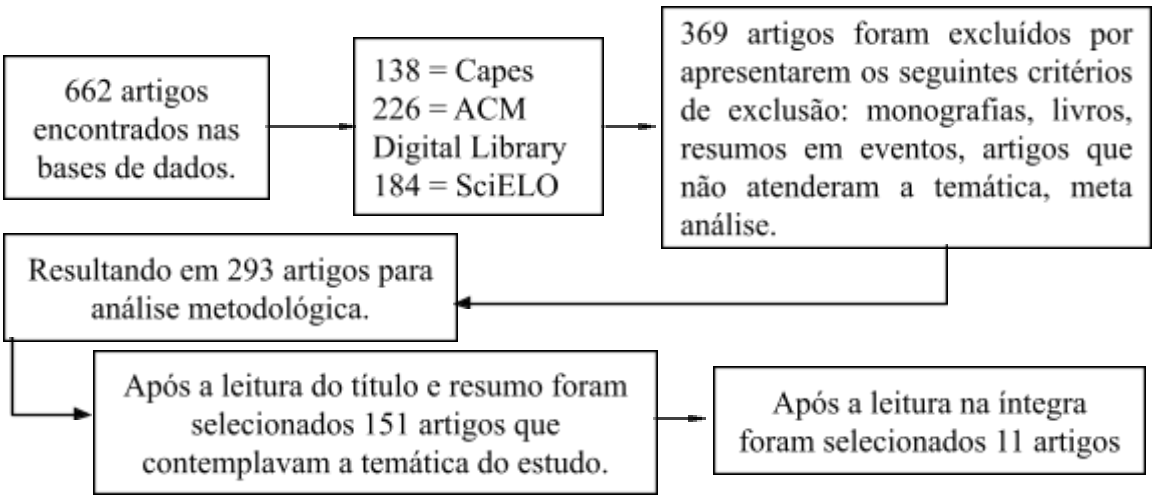

Figura 1. Seleção de artigos.
Fonte: Autora da pesquisa (2024).

Os dados foram analisados qualitativamente, utilizando técnicas de análise de conteúdo. A triagem inicial foi feita pelos títulos e resumos para selecionar os estudos potencialmente relevantes. Em seguida, a leitura completa foi realizada para confirmar se os artigos atendem aos critérios de inclusão e exclusão.

As estratégias de busca envolvem a aplicação das strings de busca nas bases de dados, com o uso de filtros para restringir a pesquisa aos critérios de inclusão. Foi realizada uma busca manual das referências citadas nos artigos selecionados para identificar estudos adicionais relevantes. Os resultados foram sintetizados em forma de texto narrativo, destacando as principais evidências encontradas na literatura.

Para obtenção dos dados foi elaborado um quadro sinóptico, que encontra-se na próxima seção, para coleta das informações, onde foi colhido as seguintes variáveis: título dos artigos, nome dos autores, tipos de pesquisa e bases de dados e resultados. Para a análise dos estudos, foi realizada uma leitura e categorização destes, com o propósito de melhor descrever e sintetizar os resultados obtidos na temática proposta.

4 Resultados e Discussão

Nesta revisão de literatura, de acordo com o protocolo de busca adotado, foram encontradas um total de 662 artigos nas bases de dados selecionadas para a busca, sendo 138

artigos na base de dados Capes, 226 na base de dados ACM Digital Library e 184 na base de dados SciELO.

Os resumos foram lidos e identificados nas bases citadas acima, de forma a reconhecer os métodos propostos e discutidos pelos autores abordando o tema do presente trabalho. Com os artigos em mãos, iniciou-se o processo de análise e síntese, a partir de uma leitura exploratória para identificar aqueles mais relevantes para a pesquisa. Em seguida, foi realizada uma leitura seletiva e interpretativa, com o objetivo de conferir um significado mais amplo aos resultados escolhidos, possibilitando uma melhor elaboração textual.

Como exposto anteriormente, foram selecionados 11 trabalhos que serviram de base para o debate proposto neste tópico, em que foram elencados as ideias e abordagens que correspondiam ao tema escolhido na pesquisa em questão. Estes artigos estão detalhados na Tabela 1.

Autor/Ano	**Título do Trabalho**
Sharma e Dave (2015)	Gerenciamento de Identidade e Acesso - Um Estudo abrangente
Melo (2017)	Mecanismos de autenticação e controle de acesso para uma arquitetura de Internet do futuro.
Hintzbergen (2018)	Fundamentos de segurança da informação com base na ISO 27001 e na ISO 27002.
Ferraz (2019)	Gestão de riscos em computação em nuvem para a Gestão de Identidade e Acessos aplicada ao Sistema Decom Digital do Ministério da Economia.
Souza, Santos e Lima (2020)	Privacidade no controle de acesso em sistemas de gerenciamento de identidade.
Maia (2022)	Modelo para controle de acessos baseado em função utilizando segurança em nível de linha.
Lopes (2024)	Gerenciamento de identidade e acesso (IAM): o que é e qual sua relevância no SI.
Bianchi e Paula (2024)	Um Estudo sobre a Avaliação do Controle de Concessão de Acessos em Ambientes de Computação em Nuvem.
Pohn e Hommel (2023)	Uma visão geral das limitações e abordagens em gerenciamento de identidade.
Montérémal (2024)	Gerenciamento de identidade e gerenciamento de acesso: definição, desafios e software IAM.
Deochake e Channapattan (2022)	Estrutura de gerenciamento de identidade e acesso para recursos multi locatários em computação em nuvem híbrida.

Tabela 1. Distribuição dos trabalhos quanto aos autores, ano e título.
Fonte: Autora da pesquisa (2024).

Os trabalhos apresentados na Tabela 1 são detalhados e debatidos a seguir.

Hintzbergen et al. (2018) definem o Gerenciamento de Identidade e Acesso (IAM) como uma área essencial da segurança e da gestão empresarial, que combina diferentes tecnologias e procedimentos para garantir que apenas pessoas ou máquinas autorizadas acessem os recursos apropriados, conforme suas funções e necessidades. Paralelamente, o IAM atua na prevenção de acessos não autorizados e fraudes, reforçando a segurança organizacional. O gerenciamento de acessos envolve etapas fundamentais, como identificação, autenticação e autorização, que desempenham um papel crucial na mitigação de riscos e na adaptação contínua das permissões ao longo do ciclo profissional do usuário. Essas práticas buscam possibilitar que os acessos sejam concedidos de forma controlada e alinhada aos requisitos de segurança da organização.

Com base nesses princípios, Hintzbergen et al. (2018) propõem mecanismos de autenticação e controle de acesso adaptados às arquiteturas da Internet do futuro, considerando desafios tecnológicos emergentes e padrões de segurança em evolução. Além disso, destacam a importância da implementação de um sistema de gestão da segurança da informação, detalhando processos e controles necessários para garantir conformidade e proteger informações sensíveis.

Lopes (2024) complementa a visão sobre o Gerenciamento de Identidade e Acesso (IAM) ao destacar que a gestão de acesso é uma etapa subsequente a esse processo. Após a confirmação da identidade de um usuário, a gestão de acesso define quais recursos ele pode utilizar, considerando fatores como função ocupada, tempo de serviço, certificação de segurança e envolvimento em projetos específicos. Esse controle é essencial para proteger dados sensíveis e garantir a segurança operacional das organizações.

Além disso, Lopes (2024) ressalta que os pilares da segurança da informação — confidencialidade, integridade e disponibilidade — são fundamentais para a proteção eficaz dos sistemas organizacionais. O estudo enfatiza os benefícios do IAM, como maior eficiência no controle de acessos, mitigação de riscos relacionados à credenciais comprometidas e conformidade com regulamentações como a LGPD e o GDPR. Os resultados apontam que o IAM desempenha um papel crucial na redução de vulnerabilidades associadas a acessos não autorizados, protegendo os recursos organizacionais e garantindo a conformidade regulatória.

Pöhn e Hommel (2023) analisaram as abordagens atuais em Gestão de Identidade e Acesso (IAM) e identificaram que a existência de múltiplos sistemas isolados dentro das organizações, sem integração eficiente entre si, representa uma barreira significativa para a

segurança e a gestão eficaz de acessos. Esse problema, chamado de fragmentação das soluções, pode resultar em inconsistências nas permissões de usuários, dificuldades no monitoramento centralizado e aumento do risco de acessos indevidos. Para superar essas limitações, os autores sugerem a integração dos sistemas e a padronização das práticas de IAM, enfatizando a importância de uma abordagem unificada, especialmente no controle de acesso de terceiros em ambientes corporativos complexos.

O estudo destaca as limitações dos sistemas tradicionais de IAM e propõe a adoção de soluções baseadas em tecnologia de nuvem para maior escalabilidade e segurança. Além disso, enfatiza a necessidade de autenticação multifatorial e controles de acesso dinâmico para enfrentar desafios específicos. A pesquisa oferece uma análise crítica das abordagens atuais, identificando a fragmentação das soluções como uma barreira significativa. Os autores propõem estratégias para a integração de sistemas e recomendam maior padronização de práticas em diferentes setores, visando melhorar a consistência na aplicação das práticas de Gestão de Identidade e Acesso.

Bianchi e Paula (2024) destacam a importância da parametrização das configurações no IAM para atender às exigências das auditorias de sistemas, enfatizando a necessidade de políticas bem definidas. Seu estudo aborda a relação entre IAM e auditorias, um tema pouco explorado, mas essencial para a conformidade organizacional. Com o crescimento exponencial das interações digitais e a crescente dependência de sistemas informatizados, o controle de acesso de terceiros no IAM tornou-se um aspecto central da segurança da informação. As organizações modernas estão cada vez mais conectadas a fornecedores, parceiros e prestadores de serviço, expandindo as fronteiras de suas redes e, consequentemente, elevando os riscos de acessos não autorizados.

O estudo dos autores também busca identificar quais controles devem ser avaliados pela auditoria de sistemas em um IAM, quais configurações podem atender a esses controles e quais recomendações de parametrização são necessárias para satisfazer os requisitos da auditoria. Os resultados indicam que, embora o IAM ofereça diversas configurações de segurança, é fundamental que as organizações estabeleçam políticas claras e realizem a parametrização adequada para garantir um gerenciamento de acesso eficaz. Dessa forma, o IAM não apenas reforça a segurança do ambiente de tecnologia da informação, mas também apoia as análises da auditoria de sistemas.

Souza, Santos e Lima (2020) identificaram lacunas significativas na proteção de dados sensíveis e propuseram melhorias nos mecanismos de autenticação e autorização. Eles enfatizam a necessidade de padrões específicos para diferentes contextos organizacionais,

destacando como isso pode aprimorar a segurança e a confiança em ambientes corporativos que envolvem terceiros. Além disso, os autores observam que uma parcela considerável das violações de segurança ocorre devido ao comprometimento de credenciais de terceiros, evidenciando a necessidade de soluções robustas para mitigar esses riscos. Assim, o controle de acesso de terceiros deve ser estruturado de maneira a equilibrar a necessidade de acesso às informações corporativas com uma proteção eficiente contra ameaças internas e externas.

Sharma e Dave (2015) exploram os desafios no gerenciamento de identidade e acesso (IAM) em ambientes de computação em nuvem, destacando as limitações dos sistemas IAM tradicionais que comprometem a escalabilidade e a segurança em cenários modernos. Eles sugerem soluções como autenticação multifator e controles de acesso dinâmico, que são fundamentais para mitigar os riscos associados a terceiros. O objetivo do artigo é investigar os mecanismos e desafios do gerenciamento de identidade e acesso em nuvem, propondo a adoção de tecnologias emergentes, como gerenciamento de identidade federada, que utiliza protocolos como SAML 2.0, OAuth e OpenID Connect para permitir logins únicos e mais seguros; autenticação baseada em risco, que ajusta os níveis de autenticação conforme geolocalização e comportamento do usuário; e monitoramento contínuo, essencial para auditorias e conformidade regulatória. Além disso, os autores ressaltam que a implementação eficaz de sistemas IA exige o uso de diretórios centralizados, como LDAP e Active Directory, para provisionamento automatizado e revogação de acessos, garantindo maior controle sobre as permissões dos usuários.

Apesar dos benefícios, Sharma e Dave (2015) enfatizam que a implementação de sistemas IA exige uma abordagem estruturada para garantir eficiência e segurança. Os autores destacam a importância de protocolos como SAML 2.0, OAuth e OpenID Connect para facilitar a autenticação e a autorização de usuários em múltiplos serviços. Além disso, ressaltam que práticas como autenticação multifator e monitoramento contínuo são fundamentais para assegurar a conformidade regulatória e reduzir vulnerabilidades. Dessa forma, a adoção de IAM permite maior controle sobre acessos e identidade, contribuindo para a proteção dos dados e a eficiência operacional das organizações.

Montérémal (2024) aborda o Gerenciamento de Identidade e Acesso (IAM), destacando seus conceitos fundamentais e os desafios associados. O autor enfatiza que tecnologias e práticas automatizadas podem aumentar a eficiência e minimizar riscos, além de ressaltar os benefícios dos sistemas integrados, especialmente no ambiente corporativo, onde são essenciais para o controle de acesso de terceiros em redes interconectadas. Ele também destaca a importância de parametrizar configurações no IAM para atender às

exigências de auditorias, reforçando a necessidade de políticas bem estruturadas. Sua principal contribuição está na relação entre IAM e auditorias, um tema ainda pouco explorado, mas essencial para a conformidade organizacional.

Além disso, Montérémal (2024) relata que a adoção de políticas de acesso baseadas em risco permite que as organizações ajustem dinamicamente os níveis de acesso com base no comportamento do usuário e no contexto. Por exemplo, um prestador de serviço que tenta acessar um sistema corporativo de um local incomum pode ter suas permissões restringidas até que uma verificação adicional seja realizada. Segundo o autor, essa abordagem reduz significativamente as chances de violações de segurança e minimiza os impactos de acessos indevidos.

Deochake e Channapattan (2022) propuseram uma nova estrutura de IAM voltada para ambientes de nuvem híbrida multi locatária, com foco na escalabilidade e na aplicação em grandes plataformas de nuvem. O estudo se destaca por oferecer uma solução inovadora para o gerenciamento de identidade e acesso em cenários tecnológicos complexos, garantindo maior eficiência na administração de recursos compartilhados. A pesquisa apresenta uma abordagem abrangente e escalável, permitindo que empresas implementem um controle de identidade e acesso mais seguro e eficiente em sua infraestrutura de nuvem híbrida. Embora a implementação tenha sido testada no Google Cloud Platform, a estrutura proposta foi desenvolvida para ser facilmente adaptável a qualquer grande plataforma de nuvem pública, ampliando sua aplicabilidade no contexto corporativo.

Nesse contexto, o estudo apresenta uma nova estrutura de Gerenciamento de Identidade e Acesso (IAM) voltada para recursos compartilhados em ambientes de nuvem híbrida multi locatária. Os resultados indicam que a solução proposta é escalável e pode ser aplicada a diferentes plataformas de nuvem, garantindo um controle eficiente de identidade e acesso. Embora tenha sido testada no Google Cloud Platform, sua aplicabilidade se estende a qualquer grande provedor de nuvem pública.

Melo (2017) destaca a importância de considerar requisitos específicos de segurança ao utilizar a computação em nuvem, uma vez que, além dos controles tradicionais aplicados à infraestrutura local, tanto os provedores de serviços em nuvem quanto seus clientes devem se atentar a aspectos como controle de acesso interno e externo e riscos de vazamento de informações compartilhadas no ambiente de nuvem.

A crescente adoção da computação em nuvem se deve aos diversos benefícios que essa tecnologia proporciona, incluindo maior flexibilidade, escalabilidade e redução de custos, além da facilidade na gestão de dados armazenados. No entanto, apesar dessas

vantagens, algumas organizações ainda demonstram receio em transferir seus dados e serviços de TI para provedores de nuvem, especialmente devido a preocupações com segurança e controle. Nesse contexto, o gerenciamento de identidade e acesso torna-se um desafio ainda mais complexo. Para enfrentar esses desafios, o estudo de Melo (2017) propõe mecanismos de autenticação e controle de acesso adaptados às novas demandas da computação em nuvem, como o uso de autenticação para reforçar a segurança no acesso remoto, modelos de controle de acesso baseados em atributos (ABAC), que permitem conceder permissões dinâmicas com base no contexto do usuário, e protocolos de federação de identidade, que facilitam o gerenciamento seguro de credenciais em múltiplas plataformas. Essas soluções são projetadas para mitigar riscos e garantir que apenas usuários autorizados acessem recursos sensíveis em ambientes distribuídos

Maia (2022) destaca a importância da segurança das credenciais no Gerenciamento de Identidade e Acesso (IAM), recomendando o uso de técnicas de criptografia para evitar a interceptação de dados sensíveis. Além disso, enfatiza a relevância da Autenticação de Múltiplos Fatores (MFA) como uma medida eficaz para prevenir violações de dados, embora alerte para desafios relacionados à privacidade e dificuldades técnicas enfrentadas por usuários menos familiarizados com a tecnologia. O estudo ainda busca fornecer uma explicação prática e acessível sobre o IAM, suas funções e sua importância no contexto organizacional. Os resultados indicam que a implementação do IAM contribui para maior eficiência no controle de acessos, mitigação de riscos associados a credenciais comprometidas e conformidade com regulamentações como a LGPD e o GDPR.

Deochake e Channapattan (2022) argumentam que, além dos aspectos tecnológicos e regulatórios, a cultura organizacional desempenha um papel fundamental na segurança da informação. A adoção de treinamentos e programas de conscientização contribui significativamente para a redução de incidentes causados por erros humanos, fortalecendo a proteção dos sistemas.

Além disso, os autores reforçam que o controle de acesso de terceiros é um elemento essencial para a segurança nas organizações modernas. A combinação de tecnologias avançadas, conformidade regulatória, cultura organizacional e integração de ferramentas de segurança proporciona uma abordagem abrangente para mitigar os riscos associados a acessos externos.

Ferraz (2019) enfatiza a relevância da integração de soluções de Gerenciamento de Identidade e Acessos (IAM) com plataformas de Gerenciamento de Eventos e Informações de

Segurança (SIEM). Essa integração permite a correlação de eventos de acesso com atividades suspeitas na rede, aprimorando a capacidade de resposta a ameaças e facilitando a detecção de padrões de comportamento malicioso. O objetivo do estudo foi desenvolver uma abordagem de gestão de riscos em computação em nuvem externa para o gerenciamento de IAM, especificamente aplicada ao Sistema Decom Digital do Ministério da Economia. Os resultados demonstraram uma estrutura para identificar vulnerabilidades e propor estratégias de mitigação em sistemas de IAM ressaltando a necessidade de alinhar a segurança da informação aos requisitos de negócio em ambientes de nuvens públicas e privadas.

Os autores mencionados ao longo desta seção convergem para a ideia de que a adoção de práticas robustas e tecnologias avançadas é essencial para garantir a segurança digital. De maneira geral, os estudos revisados enfatizam a necessidade de autenticação aprimorada, integração de sistemas e adoção de padrões rigorosos para atender às exigências de segurança e privacidade. Embora as soluções propostas apresentem variações, todas ressaltam a importância de políticas bem estruturadas e adaptadas ao contexto organizacional.

4 Conclusões e Trabalhos Futuros

O controle de acesso de terceiros no gerenciamento de identidade e acesso (IAM) é um dos desafios mais complexos e críticos para a segurança da informação nas organizações modernas. A interação cada vez maior com fornecedores, parceiros e discussões de serviços externos, associada à dependência crescente de sistemas informatizados, amplia consideravelmente as superfícies de ataque, exigindo medidas robustas para garantir a proteção dos ativos digitais.

Esta revisão sistemática revelou que as práticas tradicionais de IAM já não são suficientes para atender às demandas contemporâneas. Tecnologias como autenticação multifator, controles de acesso dinâmicos e granularidade na gestão de permissões surgem como alternativas indispensáveis para garantir a segurança e a eficiência no gerenciamento de acessos. Além disso, as abordagens baseadas em risco têm se mostrado relevantes, permitindo ajustar permissões de forma dinâmica, dependendo do comportamento e do contexto dos usuários. Essa capacidade adaptativa reduz significativamente a visibilidade de vulnerabilidades de segurança, ao mesmo tempo que minimiza os impactos decorrentes de acessos não autorizados.

No entanto, a implementação de sistemas avançados de IAM apresenta desafios. Os

custos iniciais, a complexidade de integração e a resistência à mudança por parte dos usuários frequentemente dificultam a adoção dessas soluções. Para superar essas barreiras, é essencial que as organizações realizem análises de custo-benefício projetadas, planejem implementações graduais e invistam em treinamentos para usuários e gestores. A criação de uma cultura organizacional voltada para a segurança da informação também desempenha um papel crucial, educando todos os envolvidos sobre boas práticas e conscientizando-os sobre os riscos de comportamentos inseguros, como compartilhamento de credenciais e uso de dispositivos não autorizados.

Outro aspecto crítico abordado pelos estudos revisados é a conformidade com regulamentações locais e internacionais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na Europa. Estas normas impõem requisitos para o tratamento e proteção de dados pessoais, exigindo que as organizações adotem práticas de monitoramento contínuo, auditorias regulares e documentação detalhada das atividades de acesso (BRASIL, 2018; EUROPEAN UNION, 2019). O alinhamento com essas regulamentações não apenas reduz riscos legais, mas também fortalece a confiança das partes interessadas e melhora a confiança organizacional.

A revisão também destacou a importância de integrar soluções de IAM com outras ferramentas de segurança, como plataformas de gerenciamento de eventos e informações de segurança (SIEM). Essa integração permite a identificação precoce de ameaças e comportamentos maliciosos, oferecendo uma resposta mais ágil e eficaz a incidentes de segurança. Além disso, soluções baseadas em computação em nuvem apresentam vantagens ao oferecer escalabilidade, flexibilidade e melhor custo-benefício em ambientes corporativos dinâmicos.

Por fim, os benefícios de longo prazo associados a um gerenciamento eficiente de identidade e acesso superam os desafios de sua implementação. A adoção de práticas modernas e inovadoras não apenas protege informações críticas, mas também contribui para a eficiência operacional e para a construção de um ambiente de negócios mais seguro e confiável. Diante disso, o controle de acesso de terceiros deve ser tratado como uma prioridade estratégica, sendo fundamental para organizações que buscam prosperar em um cenário cada vez mais digital e interconectado.

Como possibilidade de continuidade deste trabalho, se destaca a possibilidade de analisar referências técnicas (como relatórios técnicos de empresas) e literatura cinza (ex.: notícias de veículos especializados da área) para um aprofundamento ainda maior da revisão realizada. Além disto, também se vislumbra verificar, através de estudos de caso, como os

conceitos e tecnologias encontrados nesta revisão estão sendo efetivamente utilizados nas organizações.

Referências

BESENYI, E.; STALLINGS, M. O papel da gestão de identidade e acesso na estratégia de segurança digital. **International Journal of Cybersecurity Intelligence and Cybercrime**, v. 3, n. 2, p. 90-106, 2020.

BIANCHI, ATO; PAULA, LB. **Um Estudo sobre a Avaliação do Controle de Concessão de Acessos em Ambientes de Computação em Nuvem.** Revista GETEC, v. 9-26, 2024. Disponível em: https://www.revistas.fucamp.edu.br/index.php/getec/article/view/3436/2164?utm_source=chatgpt.com. Acesso em: 28 abr. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 jan. 2025.

EUROPEAN UNION. **General Data Protection Regulation (GDPR)**. Disponível em: https://gdpr-info.eu/. Acesso em: 29 jan. 2025.

DEOCHAKE, S.; CHANNAPATTAN, V. **Estrutura de gerenciamento de identidade e acesso para recursos multi locatários em computação em nuvem híbrida.** arXiv preprint arXiv:2203.11463, 2022. Disponível em: https://arxiv.org/abs/2203.11463. Acesso em: 10 de jan. 2025.

FARAHANI, B.; SARDAR, M.; KONG, X. **Gerenciamento de Riscos e Identidades de Terceiros:** Desafios e Soluções. Computadores e Segurança, v. 117, 2022.

FERRAZ, Claudio Augusto Novais. **Gestão de riscos em computação em nuvem para a Gestão de Identidade e Acessos aplicada ao Sistema Decom Digital do Ministério da Economia**. xv, 171 f., il. Dissertação, Universidade de Brasília, Brasília, 2019. Disponível em: http://www.rlbea.unb.br/jspui/handle/10482/37502. Acesso em: 10 de jan. 2025.

FERNANDES, AA; SOARES, LF. **Gestão de identidade e acesso:** fundamentos e práticas. São Paulo: Atlas, 2020.

GARTNER. **Guia de mercado para governança e administração de identidade. Gartner** Research, 2021. Disponível em: https://www.gartner.com. Acesso em: 20 de mar. 2025.

GUNTHER, Hartmut. **Pesquisa qualitativa versus pesquisa quantitativa:** esta é a questão? Psic.: Teor. e Pesq. [online], vol.22, n.2, pp.201-209. ISSN 0102-3772. 2016.

LIU, H.; XU, H. Segurança cibernética na transformação digital: desafios e futuras direções de pesquisa. Information & Management, v. 57, n. 8, 2020.

LOPES, Kelvin Dias. **Gerenciamento de identidade e acesso (IAM):** o que é e qual sua relevância no SI. AFD. Academia de Forense Digital, 2024. Disponível em: https://academiadeforensedigital.com.br/gerenciamento-de-identidade-e-acesso-o-que-e-e-qual-relevancia/. Acesso em: 10 dez. 2024.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

ISO/IEC 27001:2022. **Segurança da informação, segurança cibernética e proteção da privacidade — Sistemas de gestão da segurança da informação — Requisitos**. Organização Internacional para Padronização. 2022.

KHAN, S.; JAVED, M. Uma revisão de frameworks de gerenciamento de identidade e acesso em empresas modernas. **Journal of Network and Computer Applications**. v. 211, 2023.

MAIA, Filipe Beserra. **Modelo para controle de acessos baseado em função utilizando segurança em nível de linha.** Anápolis: Instituto Federal de Goiás, 2022. Trabalho de conclusão do curso de Ciência da Computação. Orientador: Prof. Alessandro Rodrigues. Disponível em: https://repositorio.ifg.edu.br/bitstream/prefix/1390/1 /tcc_filipe_final_ .pdf . Acesso em: 15 dez. 2024.

MAVROULAS, G.; MANSO, M. Segurança de acesso de terceiros em infraestruturas críticas de informação. **Future Generation Computer Systems**, v. 122, p. 172-185, 2021.

MELO, Pedro Henrique Aparecido Dâmaso de. **Mecanismos de autenticação e controle de acesso para uma arquitetura de internet do futuro.** Uberlândia: Universidade Federal de Uberlândia, 2017. Dissertação (Mestrado). Disponível em: https://repositorio.ufu.br/bitstream/123456789/18381/1/mecanismosautenticacaocontrole.pdf. Acesso em: 15 dez. 2024.

MONTÉRÉMAL, J. **Gerenciamento de identidade e gerenciamento de acesso: definição, desafios e software IAM.** Appvizer Revista, 2024. Disponível em: https://www.appvizer.com.br/revista/ti/ids-e-acesso/gerenciamento-de-identidade. Acesso em: 13 jan. 2025.

POHN, D.; HOMMEL, W. **Uma visão geral das limitações e abordagens em gerenciamento de identidade.** arXiv preprint arXiv. 2023. Disponível em: https://arxiv.org/abs/2301.00442. Acesso em: 13 jan. 2025.

SOUZA, AM; SANTOS, GR; LIMA, OS. **Privacidade no controle de acesso em sistemas de gerenciamento de identidade.** Revista Brasileira de Computação Aplicada, v. 1, pág. 45-58, 2020. Disponível em: https://repositorio.ufsc.br/handle/123456789/192912. Acesso em: 13 jan. 2025.

SCHNEIER, B. A mente de um hacker: como os poderosos distorcem as regras da sociedade e como revertê-las. **WW Norton & Company**, 2023.

SENEVIRATNE, P.; MOHAMMED, S. Mitigando riscos de terceiros por meio da governança de identidade: uma proposta de estrutura. **Journal of Information Security and Applications** , v. 67, 2022.

SHARMA, A.; SHARMA, S.; DAVE, M.. **Gerenciamento de Identidade e Acesso - Um Estudo abrangente**. In: INTERNATIONAL CONFERENCE ON GREEN COMPUTING AND INTERNET OF THINGS (ICGCIoT), 2015. Anais... IEEE, 2015. p. 1481-1484.