UM ESTUDO SOBRE A AVALIAÇÃO DO CONTROLE DE CONCESSÃO DE ACESSOS EM GERENCIADORES DE IDENTIDADE (IAM) EM COMPUTAÇÃO EM NUVEM PELA AUDITORIA DE SISTEMAS

A STUDY ON THE EVALUATION OF ACCESS GRANT CONTROL IN IDENTITY MANAGERS (IAM) IN CLOUD COMPUTING BY SYSTEMS AUDIT

Ana Carolina Toledo Bianchi[1]
Luciano Bernardes de Paula[2]

RESUMO:

O aumento da adoção da computação em nuvem pelas organizações resulta em benefícios ao mesmo tempo em que traz novos riscos para o ambiente de tecnologia. As ameaças devem ser identificadas, os riscos devem ser mapeados e controles devem ser atribuídos e implementados para garantir a segurança da informação no ambiente. Na computação em nuvem, existe o risco de acesso indevido e, para evitá-lo, é disponibilizado um serviço que possibilita realizar a gestão e controle de usuários denominado gerenciador de identidade e acesso (*Identity and Access Management* - IAM). O IAM, por ser o serviço que suporta a gestão de acessos no ambiente, deve ser avaliado pela auditoria de sistemas que irá validar se as configurações e políticas aplicadas pela organização, para este serviço, estão em conformidade com as medidas de prevenção a acessos indevidos. Neste contexto, este estudo busca identificar quais os controles devem ser avaliados pela auditoria de sistemas em um IAM, quais as configurações deste podem atender a estes controles e quais as recomendações de configuração para satisfazer a auditoria de sistemas.

PALAVRAS-CHAVE: Auditoria de Sistemas; Concessão de Acessos; Gerenciador de Identidade e Acesso.

ABSTRACT:

The increased adoption of cloud computing by organizations results in benefits while bringing new risks to the technology environment. Threats must be identified, risks must be mapped and controls must be assigned and implemented to ensure information security in the environment. In cloud computing, there is a risk of improper access and, to avoid this, a service is available that makes it possible to manage and control users called Identity and Access Manager (IAM). IAM, as it is the service that supports access management in the environment, must be evaluated by systems auditing that will validate whether the configurations and policies applied by the organization, for this service, are in compliance

[1]Tecnóloga em Análise e Desenvolvimento de Sistemas pelo Instituto Federal de São Paulo – IFSP, pós-graduanda no curso de Especialização em Gestão Estratégica de TI pelo IFSP – campus de Bragança Paulista. E-mail: actbianchi@gmail.com.
[2]Professor Doutor na área de Computação no Instituto Federal de São Paulo - campus Bragança Paulista. E-mail: lbernardes@ifsp.edu.br.

with measures to prevent unauthorized access. In this context, this study seeks to identify which controls must be evaluated by the systems audit in an IAM, which configurations can meet these controls and which configuration recommendations are to satisfy the systems audit.

KEYWORDS: System Audit; Access Granting; Identity and Access Manager.

1. INTRODUÇÃO

No contexto atual, no qual a segurança da informação se torna um pilar importante para o funcionamento dos sistemas, mapear riscos e implementar controles que mitigam a possibilidade de ocorrência daqueles identificados se torna algo fundamental para a operação e continuidade dos negócios nas empresas. Em (Imoniana, 2016) é descrito que a identificação de riscos em um sistema é uma dificuldade no processo de auditoria de sistemas mas, se não realizada, pode se tornar desastrosa. A falta de identificação das ameaças e as falhas de segurança, resultantes destes riscos não identificados, podem ser exploradas causando problemas em diversos aspectos para a organização, incluindo prejuízo financeiro.

O processo de análise e identificação de riscos é realizado pela área de controles internos da organização que, segundo Yang (2011) exerce uma atividade independente, utilizando abordagens sistemáticas para apoiar a organização a atingir seus objetivos por meio de melhorias nos processos de identificação e gestão de riscos, controles e governança. Existir uma equipe dedicada a esta atividade se torna um diferencial e pode prover às empresas vantagens competitivas, garantindo aos usuários e clientes envolvidos a integridade, confidencialidade e disponibilidade das informações da operação do negócio.

Em paralelo, segundo Udagatti (2016), a migração dos dados para um ambiente em nuvem se popularizou devido aos benefícios que oferece, tais como recursos computacionais (processamento e armazenamento) gerenciados pelo provedor de serviços. A computação em nuvem é atualmente uma realidade para as companhias e, segundo Almulla (2010), a redução de custos e as vantagens resultantes de migrar para este ambiente é um dos principais motivos da sua adoção. Porém, é preciso considerar o impacto na segurança dos dados, da infraestrutura e das informações de usuários que estarão armazenados remotamente no ambiente em nuvem e devem ser protegidos conforme diretrizes de segurança dos provedores do serviço.

Um desafio para a segurança no ambiente em nuvem é gerenciar diferentes níveis de serviço relacionados a isolamento, entrega e escalabilidade. Estes níveis podem ser criados e gerenciados por políticas e devem ser protegidos de usuários não autorizados (Moghaddam, Emanidia, Wieder, Yahyapour, 2018). Um dos riscos comumente identificados nos ambientes de tecnologia é o risco de acesso indevido de usuários. Apesar de ambientes em nuvem serem modernos e fornecerem recursos de segurança, é importante que a organização utilize esses recursos, implemente controles e gerencie os usuários deste ambiente, garantindo que apenas aqueles legítimos obtenham acesso às informações e dados.

Segundo Naik, Jenkins (2016), temos a fusão de várias tecnologias no ambiente em nuvem e um dos maiores desafios desse ambiente é gerenciar identidades e realizar o controle de acesso de usuários. Para esta necessidade, foi desenvolvido um serviço chamado gerenciamento de identidade e acesso - IAM (do inglês *Identity and Access Management*). O IAM é um serviço disponível em ambientes de nuvem que permite autenticar, autorizar e gerenciar usuários com base nos recursos e funções de acesso atribuídas (Sharma, Sharma, Dave, 2015). Porém, além de gerenciar os usuários do ambiente é importante que os usuários com acesso ao IAM também sejam gerenciados e monitorados.

O objetivo deste trabalho é descrever conceitos de auditoria de Tecnologia da Informação (TI), computação em nuvem e gerenciadores de identidade e acesso (IAM) e relacioná-los, apresentando uma análise dos recursos e configurações existentes no IAM de ambiente em nuvem que podem apoiar a conformidade dos controles avaliados pela auditoria de sistemas.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta a metodologia utilizada para a elaboração deste trabalho; na Seção 3 é apresentada a fundamentação teórica, apresentando os conceitos de auditoria de sistemas, controle de concessão de acesso, como deve ser a conformidade do controle de concessão de acesso com a auditoria de sistemas, conceitos de computação em nuvem e IAM e como deve ser feita a conformidade do IAM com o processo de auditoria. Por fim, na Seção 4 é feita a conclusão do trabalho.

2. METODOLOGIA

A metodologia aplicada na realização deste trabalho é composta pela inspeção, análise e leitura de artigos e conteúdos disponíveis on-line sobre os assuntos abordados, com o objetivo de levantar conhecimento em conjunto com o método especialista. Neste contexto, a pesquisa é realizada com base no levantamento bibliográfico e experiência da autora, que serão utilizados para contextualizar e descrever a análise da auditoria de sistemas ao avaliar o controle de concessão de acessos no serviço IAM na computação em nuvem.

3. FUNDAMENTAÇÃO TEÓRICA

3.1. Auditoria de Sistemas

O processo de auditoria de sistemas é um dos pilares da segurança da informação que visa assegurar a confidencialidade, integridade e disponibilidades dos dados e sistemas de uma organização. Segundo Tingliao (2016), a auditoria de sistema de informação tem o papel de avaliar os riscos existentes em um sistema, assim como os controles que a organização utiliza para mitigar esses riscos. Mediante processo de coleta e avaliação de evidências, a auditoria de sistemas afere se os controles aplicados ao sistema de informação são efetivos de modo a proteger os ativos, manter a integridade dos dados e apoiar os objetivos de negócio.

A partir da auditoria de sistemas, utilizando-se de políticas de segurança da informação, regulamentações e matriz de riscos e controles, é elaborada uma estratégia para corroborar que os sistemas estão operando conforme padrões e práticas da organização. Zhou (2020) cita que o objetivo da auditoria de sistemas é identificar e controlar riscos potenciais do sistema, dentre eles, riscos relacionados à proteção de informações, intrusão e perda de dados, e reforçar a realização e gestão dos controles internos da organização garantindo a segurança nos sistemas de informação.

Os riscos do ambiente de tecnologia devem ser identificados e controles devem ser endereçados para mitigação destes riscos, compondo assim a matriz de riscos e controles de TI. O departamento de tecnologia deve garantir que os controles definidos na matriz foram implementados e estão operando em todo o ambiente, visto que, segundo Tingliao (2016) a

auditoria do sistema de informação baseia-se no risco e nas medidas de controles utilizadas pela organização para concluir se o sistema de informação é seguro e eficaz.

Segundo Islamova, Volkova (2017), ao auditar processos é necessário definir a abordagem de auditoria que pode ser composta de vários métodos como entrevistas, análise da documentação e monitoramento do processo. A entrevista é realizada com o proprietário do processo e, ainda segundo os autores, deve dar ênfase nos resultados, análise e ações de acompanhamento. O auditor também pode realizar uma análise de riscos junto ao dono de processo conduzindo questionamentos que irão determinar como, quando e por quem o processo é realizado, quais riscos são relevantes e qual a probabilidade dos riscos se materializarem no ambiente.

A análise da documentação e monitoramento do processo são realizados após a entrevista e consiste na verificação da implementação do próprio processo (Islamova, Volkova, 2017). Através de um caso selecionado, o auditor irá inspecionar o processo do início ao fim verificando evidências que demonstrem que o processo, conforme implementado, é suficiente para cobrir os riscos mapeados para o ambiente.

O resultado da auditoria de sistemas é compartilhado com a alta administração através de um relatório com o resultado da avaliação do auditor para cada processo. Segundo a Norma de Auditoria Número 5 (do inglês *Auditing Standard nº 5*) do Public Company Accounting Oversight Board (PCAOB, 2007), as deficiências de processos internos identificadas devem ser comunicadas à administração, antes do relatório ser emitido. O relatório com a opinião do auditor sobre os controles internos da organização contém recomendações que são escritas com base em boas práticas e devem ser implementadas pelos donos de processo para corrigir vulnerabilidades e cobrir riscos no ambiente de tecnologia da informação.

3.2. Controle de Concessão de Acesso

Segundo Hintzbergen, Baars, Hintzbergen, Smulders (2018), a concessão e gestão do acesso a usuários envolvem etapas que incluem a identificação, autenticação e autorização dos usuários. Estas etapas podem ser cumpridas através de atividades de controle para provisionamento de usuários e gestão de acesso que podem mitigar o risco de acesso

indevido no ambiente. O provisionamento de usuário é comumente implementado como um controle na matriz de riscos e procedimentos da organização, denominado controle de concessão de acessos.

O controle de concessão de acessos tem como objetivo assegurar que apenas usuários devidos tenham acesso concedido nos sistemas de informação da organização garantindo, segundo Kose, Coskun, Coskun (2023), uma restrição seletiva de acesso, no qual usuários autorizados acessem apenas o recurso devido, conforme condições estabelecidas antes da concessão do acesso.

No contexto da auditoria de sistemas, o controle de concessão de acessos é testado para determinar se este é efetivo e suficiente para mitigar o risco de acesso indevido. Segundo a Norma de Auditoria Número 5 do PCAOB (2007), o auditor deve avaliar a efetividade de um controle ao inspecionar se este é empregado conforme idealizado e observando se o dono do controle possui habilidades necessárias para executá-lo de maneira efetiva.

Ainda segundo a norma (PCAOB, 2007), os procedimentos que o auditor executa para avaliar a eficácia operacional de um controle incluem indagar o dono do controle, observar a operação do controle no ambiente da organização, inspecionar a documentação e a repetição do controle. Ou seja, o auditor responsável deve indagar o responsável do controle de concessão de acessos entendendo como é o processo para este controle, observar um caso em ambiente de produção para corroborar o entendimento obtido, inspecionar evidências selecionando alguns casos de concessão de acessos que demonstrem que o controle funciona de maneira efetiva no ambiente.

Para as organizações, manter um controle de concessão de acessos efetivo é essencial para garantir a segurança da informação da companhia, porém, segundo Kose, Coskun, Coskun (2023), gerenciar políticas de controles de acessos é um desafio devido aos novos sistemas que possuem infraestrutura multifacetadas como plataformas baseadas em nuvem e outras plataformas que apresentam riscos de segurança específicos. Sendo assim, é necessário que as empresas avaliem os recursos de gerenciamento de acessos de suas diferentes plataformas buscando meios e implementando controles que assegurem que o ambiente de tecnologia seja acessado apenas por pessoas devidas.

3.3. Conformidade do Controle de Concessão de Acessos com a Auditoria de Sistemas

Segundo Pongsrisomchai (2019), durante a fase de planejamento da auditoria de TI, os auditores desenvolvem o programa de trabalho que irá basear toda a atividade e garantir que os riscos importantes da auditoria estão sendo considerados e avaliados. Os riscos são cobertos por controles que serão avaliados pelos auditores como, por exemplo, o controle de concessão de acessos.

Para o auditor de sistemas, o controle de concessão de acessos deve assegurar que somente usuários devidos e autorizados tenham acessos aos sistemas de informação. Algumas atividades que um controle de gerenciamento de contas de usuários deve abranger, segundo o catálogo de controles do Instituto Nacional de Padrões e Tecnologia (NIST) (2023), são:

- Definir e documentar os tipos de contas permitidas e proibidas no sistema;
- Exigir aprovação de pessoal para solicitações de criação de contas;
- Criar, ativar, modificar, desativar e remover contas de acordo com política, procedimentos, pré-requisitos e critérios definidos pela organização;
- Exigir pré-requisitos e critérios definidos pela organização para associação a grupos e funções.

Em relação aos tipos de contas permitidas e proibidas no sistema, o catálogo de controles do NIST (2023) cita exemplos de tipos de conta que podem existir, tais como individual, compartilhada, de grupo, de sistema, emergencial, temporária ou de serviço. Estes são exemplos que podem ser documentados em uma política de concessão de acessos que também pode descrever os requisitos para a criação, a ativação, a modificação, a desativação e a remoção de contas de usuário. Esta política irá basear todo o processo de concessão e será utilizado pela auditoria de sistemas como base para testar a efetividade do controle.

A exigência de pré-requisitos e critérios para associação a grupos e funções é relacionada ao controle de acesso baseado em funções no catálogo de controle do NIST (2023) que menciona que o controle de acesso baseado em atributos é uma política que restringe o acesso ao sistema a usuários autorizados com base em atributos organizacionais

baseados, por exemplo, em função de trabalho ou sua identidade. Um dos atributos avaliados pela auditoria de sistemas é inspecionar se as funções concedidas ao usuário são devidas e foram previamente aprovadas. Ter uma política ou documento que baseie quais funções no sistema um usuário pode ter acesso, com base em sua identidade ou função de trabalho, provê maior segurança ao ambiente e auxilia o auditor de sistemas a avaliar que os acessos concedidos são devidos.

Em relação à atividade de controle exigir aprovações de pessoal para solicitações de criação de conta assegura que somente usuários devidamente autorizados possuem acesso ao sistema. Segundo o catálogo de controles do NIST (2023), a imposição da aprovação pode proporcionar maior segurança e privacidade da informação. As aprovações antes da concessão de acesso aos usuários devem ser formalizadas e retidas para fins de auditoria e documentação.

O controle de concessão de acessos e a avaliação do controle pelo auditor de sistemas podem ser diferentes para cada organização dependendo dos riscos mapeados para o ambiente, porém, a implementação formal e documentada das atividades definidas acima são a base para demonstrar ao auditor que os usuários com acesso aos sistemas são devidos e não oferecem riscos ao ambiente de tecnologia da informação.

3.4. Computação em Nuvem e IAM

A computação em nuvem tem se disseminado nos dias de hoje devido aos inúmeros benefícios que oferece, tais como recursos independentes de localização, elasticidade e gerenciamento dos dados hospedados (Udagatti, 2016). Atualmente, a migração dos ambientes de tecnologia para a nuvem tem se tornado cada vez mais frequente pelas empresas que visam maior flexibilidade, escalabilidade e redução de custos.

Apesar das vantagens, segundo Banday, Mehraj (2017), há algumas organizações que ainda não confiam plenamente no ambiente em nuvem para transferir dados e serviços de TI para os provedores de serviço. Adicionalmente, no ambiente em nuvem as questões de gerenciamento de identidade e acesso se tornam mais difíceis. O ambiente da computação em nuvem é acessado por diversos usuários de diferentes funções e gerenciar o acesso e permissões desses usuários pode se tornar um desafio para as organizações. Desta maneira, no ambiente da computação em nuvem é disponibilizado o módulo de gerenciamento de

identidade e acesso (IAM) que permite às organizações centralizarem e administrarem o acesso dos usuários no ambiente.

O IAM é um conjunto de serviços que permitem gerenciar usuários e o acesso a recursos e funções do ambiente conforme definições de regras e políticas definidas pela organização em relação aos usuários do sistema, por meio de vários controles como autenticação via *login* e senha, atribuição de funções e recursos aos usuários e provisionamento de contas de usuário (Sharma, Sharma, Dave, 2015).

De acordo com a Microsoft, as principais funcionalidades do IAM (2024) são:

- Gerenciamento de identidade – permite criar, armazenar e gerenciar as permissões e níveis de acesso associados a identidades no ambiente.
- Federação de identidade – permite que senhas do usuário de outro local (por exemplo, senha de rede corporativa) sejam utilizadas para acessar o ambiente.
- Provisionamento e desprovisionamento de usuários – permite realizar a criação e gerenciamento de contas, recursos, permissões e níveis de acesso dos usuários.
- Autenticação de usuários – realiza a autenticação dos usuários e permite adicionar MFA (*multi-factor authentication* - autenticação multifator) e SSO (*single sign-on* - acesso único) para o processo de autenticação de usuário, confirmando que os usuários são devidos.
- Autorização de usuários – permite gerenciar o acesso autorizando o usuário a apenas os níveis e recursos necessários. A autorização também pode ser concedida a grupos ou funções de usuários que irão receber o mesmo tipo de privilégio.
- Controle de acesso – regula o acesso a sistema e dados e permite definir os recursos, funções e permissões dos usuários e configurar os mecanismos de autenticação e autorização que serão utilizados no ambiente.
- Relatórios e monitoramento – permite gerar relatórios relacionados a conformidade, padrões de uso e segurança do ambiente. Os relatórios podem apoiar na análise e identificação de riscos.

Em relação à auditoria, o IAM é o serviço que fornece informações que permitem identificar o motivo pelo qual um usuário tem acesso ao ambiente (Thakur, Gaikwad, 2015).

As diversas funcionalidades do IAM, se configuradas em conformidade com as normas

regulatórias, podem apoiar nas análises de auditoria, ajudando a mitigar riscos relacionados a acesso indevido no ambiente de tecnologia da companhia.

3.5. Conformidade do IAM com a Auditoria de Sistemas

Segundo o plano de auditoria da ISACA (do inglês Information Systems Audit and Control Association) (ISACA) (2022), o aumento da adoção da computação em nuvem pelas organizações aumenta a necessidade de se realizar um gerenciamento efetivo do gerenciamento de identidade e acesso no ambiente. A implementação do IAM, desde que configurado e gerenciado corretamente, permite um melhor controle de acessos em todo ambiente de tecnologia, visto que, segundo o plano de auditoria do ISACA (2022), o IAM é a base para o acesso autorizado e autenticado e possui protocolos e configurações de segurança que permitem conceder níveis de acessos apropriados aos usuários no ambiente.

Segundo Microsoft (2024), a solução IAM atende a requisitos de conformidade e simplifica a geração de relatórios que podem apoiar nos processos de auditoria, demonstrando que o acesso a dados do ambiente está sendo gerenciado de maneira adequada. Para que os auditores tenham o conforto que o ambiente é gerenciado de maneira adequada, é necessário implementar controles de acesso no ambiente do IAM que irão assegurar que o acesso é restrito e concedido apenas a pessoas devidas.

De acordo com o plano de auditoria de gerenciamento de identidade e acesso do ISACA (2022), diversos controles em relação ao plano de auditoria em um IAM devem ser analisados. Para este trabalho, considerando as atividades relacionadas com a concessão de acessos, foram considerados os seguintes controles: gerenciamento de identidade; autorização e controle de acesso.

Neste trabalho foram considerados os controles existentes na plataforma Microsoft Azure, por questões de familiaridade dos autores. Entretanto, é possível afirmar que o serviço IAM, assim como seus recursos, são comuns e presentes em diversos outros provedores de serviço em nuvem, tais como AWS da Amazon, Google Cloud Platform da Google, entre outras.

3.5.1. Gerenciamento de Identidade

Segundo o plano de auditoria de gerenciamento de identidade e acesso do ISACA (2022) o controle de gerenciamento de identidade tem como objetivo assegurar que o gerenciamento de contas de usuários é centralizado, realizado por meio de um diretório ou serviço de identidade.

Ainda segundo o plano de auditoria de IAM do ISACA (2022), para o controle de gerenciamento de identidades, os auditores irão avaliar, através de entrevistas e análises de documentação, os processos e ferramentas utilizados para gerenciar as identidades e contas de usuários do ambiente. Se identificados processos diferentes para gerenciar identidades, o auditor deve entender e avaliar todos os processos.

É válido mencionar que não ter um processo centralizado para gerenciar identidades não caracteriza o processo como inefetivo, neste caso, o auditor irá conduzir análises mais extensas, pois terá que entender como é o processo de gerenciamento de identidades para cada uma das instâncias nas quais este é realizado. Porém, ter um processo centralizado pode reduzir a probabilidade de o ambiente ter lacunas de segurança.

Para garantir que o gerenciamento de identidade seja realizado em um recurso centralizado no IAM, é possível aplicar uma Azure Policy ao ambiente. De acordo com Microsoft (2023), o Azure Policy impõe padrões de processos, de maneira granular, e permite avaliar a conformidade do ambiente em escala. Uma das políticas padrões disponibilizadas no Azure Policy, segundo o artigo da Microsoft (2023), é a política “tipo de recursos permitidos” que possibilita definir quais tipos de recursos podem ser criados no ambiente. Configurar a política para negar toda a criação de recursos relacionados a IAM na computação em nuvem poderia apoiar na centralização do gerenciamento de identidades, garantindo que o gerenciamento e controle das contas de usuários são realizados apenas em um recurso já criado.

3.5.2. Controle de Autorização

Segundo o plano de auditoria de gerenciamento de identidade e acesso do ISACA (2022) o controle de autorização tem como objetivo assegurar que os usuários recebam apenas acessos autorizados por aprovação documentada. A aprovação deve ser registrada antes da concessão do acesso ao usuário.

Para o controle de autorização, os procedimentos que o auditor deve realizar, segundo o plano de auditoria da ISACA (2022) são: inspecionar se as políticas de controle de acesso definem como as aprovações são obtidas e mantidas (preferencialmente devem ser obtidas e mantidas em um sistema de *tickets*), examinar se os privilégios foram concedidos aos usuários conforme aprovação formal e não conflitam entre contas do usuário únicas ou múltiplas e examinar se a aprovação foi realizada por pessoa autorizada, com conhecimento para aprovar o privilégio ao usuário.

Para garantir o controle de autorização, é recomendado documentar uma política do controle de concessão de acessos descrevendo quais análises e aprovações devem ser formalizadas e por qual meio estas devem ser realizadas. Os aprovadores também devem ser predefinidos e os usuários que possuem permissão para conceder um novo acesso no IAM devem ser instruídos, de maneira que apenas acessos previamente aprovados sejam concedidos aos usuários.

3.5.3. Controle de Acesso

Segundo o plano de auditoria de gerenciamento de identidade e acesso do ISACA (2022) o controle de acesso tem como objetivo assegurar que a concessão de funções do sistema é padronizada, de acordo com a política de acesso definida. Os acessos são concedidos (no nível de privilégios mínimos) conforme responsabilidades do usuário na organização.

Para o controle de acesso, segundo o plano de auditoria da ISACA (2022), dentre outros procedimentos, o auditor deve: inspecionar se o controle de acesso baseado em função foi definido e examinar as configurações de acesso dos usuários, inclusive os privilegiados, verificando, através de procedimentos de indagação com a gestão e inspeção de documentação, se o acesso está de acordo com as responsabilidades de trabalho dos usuários.

Para garantir que os usuários terão acesso apenas às funções e recursos devidos é possível utilizar a configuração do controle de acesso baseado em papel da Azure, o RBAC (*Role-Based Access Control*), que faz parte do IAM. De acordo com Microsoft (2024), o RBAC do Azure apoia o gerenciamento do acesso no ambiente possibilitando definir quais usuários devem ter acesso aos recursos da Azure e o que estes usuários podem fazer no ambiente. Configurando o RBAC é possível definir quais funções e recursos o usuário ou

um grupo de usuários deve acessar no IAM garantindo assim um ambiente com acessos devidos e padronizados.

3.6. Relação do plano de auditoria e os recursos do IAM

Na Tabela 1, a seguir, foram consolidados os controles de acesso discutidos neste artigo e as configurações do IAM. Na primeira coluna é apresentado o nome e objetivo do controle conforme descrito no plano de auditoria de IAM do ISACA (2022), na segunda coluna são apresentadas as configurações do IAM descritas em artigo da Microsoft (2024) e na terceira coluna é apresentada uma recomendação vinculando os controles de acesso e a configuração IAM correspondente que pode apoiar a organização a atingir a conformidade dos controles na avaliação da auditoria de sistemas.

Tabela 1 - Relação entre controle e configuração no IAM.

Controle e seu objetivo (ISACA, 2022)	**Configuração no IAM (Microsoft, 2024)**	**Recomendação**
Gerenciamento de identidade – existe um processo centralizado e padronizado para o gerenciamento de identidade e concessão de acessos no ambiente.	Azure Policy – criar uma política que determine que haja somente um recurso responsável pela criação de usuários e gerenciamento de identidades.	Os auditores irão inspecionar se há recurso único e centralizado para a concessão de acessos. Caso identificados recursos descentralizados para este fim, deverão ser realizadas avaliações adicionais. Desta maneira, para que este processo aconteça de forma centralizada, como definido pela ISACA, é recomendado que haja uma Azure Policy que não permita a criação de novos recursos no ambiente para a mesma finalidade, no caso, concessão de acesso. Essa recomendação deve-se ao fato de que o processo centralizado

		permite a implementação de medidas de segurança mais facilmente, diminuindo a probabilidade de erros e lacunas de segurança no ambiente.
Controle de acesso – as funções de acesso concedidas aos usuários são devidas e inerentes às atividades do usuário.	RBAC - possibilita a definição de quais ações são permitidas a um usuário (ou grupo de usuários) baseado no papel que este exerce na organização.	A auditoria deverá validar se as ações permitidas ao usuário (ou grupo de usuários) estão de acordo com o seu papel. O RBAC da Azure permite adicionar ações predefinidas ou até mesmo criar outras personalizadas para cada usuário (ou grupo de usuários).
Controle autorização – as funções de acesso concedidas aos usuários não possuem conflitos entre si.	RBAC – permite configurar quais funções serão concedidas a um usuário (ou grupo de usuários).	Os auditores irão inspecionar as funções atribuídas e verificar se o usuário (ou grupo de usuários) possui permissões conflitantes e, caso ocorra, questionar a esse respeito. Desta maneira, é recomendado que na configuração do RBAC, seja realizada uma avaliação das funções que serão atribuídas ao usuário (ou grupo de usuários) verificando se essas não conflitam entre si. É preciso atenção em relação a usuários que participem de grupos em relação a suas funções individuais e aquelas relacionadas ao grupo, que podem ser conflitantes.

Controle de acesso – funções administrativas são concedidas apenas a usuários devidos.	RBAC – permite configurar quais funções serão concedidas a um usuário (ou grupo de usuários).	Os auditores deverão validar, junto à gestão, se os usuários que possuem acessos administrativos realmente possuem esse direito. Desta maneira, é recomendado que na configuração do RBAC, seja realizada a atribuição de funções administrativas apenas a usuários (ou grupo de usuários) que realmente tem essa necessidade.

Fonte: os autores.

Estes são os controles indicados no plano de auditoria do ISACA, relacionados à concessão de acessos e definidos para IAM, que devem ser avaliados em um processo de auditoria. O IAM possui recursos que apoiam todo o processo de auditoria de sistemas, porém, é necessário que estes recursos sejam configurados conforme o ambiente que está inserido, apoiando a mitigar os riscos de segurança da informação.

4. CONCLUSÃO

A utilização do IAM na computação em nuvem possibilita às organizações realizarem uma melhor gestão de usuários utilizando funcionalidades como gerenciamento de identidade, provisionamento de usuários, controle de acesso, autenticação e autorização de usuários, dentre outros. A identificação de riscos de acesso do ambiente é uma das fases mais importantes e irá apoiar a organização na definição de quais funcionalidades devem ser utilizadas e configuradas no IAM.

Em paralelo, a auditoria de sistemas realiza uma avaliação independente do ambiente e com base em catálogos de controle e planos de auditoria define quais atributos para o controle de concessão de acesso serão considerados em sua análise, incluindo os controles avaliados para o IAM. Utilizando de métodos de entrevista, análise da documentação e monitoramento do processo é possível ao auditor entender o processo de concessão de acessos no IAM, assim como quais são as configurações que garantem que o processo de

concessão de acessos é devidamente implementado de modo a mitigar o risco de acesso indevido no ambiente.

A partir da revisão de literatura realizada neste artigo, foram identificados os possíveis atributos relacionados ao controle de concessão de acessos que serão avaliados pela auditoria de sistemas e, para cada um destes, foi atribuída uma configuração correspondente no IAM, sendo assim, é possível concluir que o IAM disponibiliza inúmeras configurações de segurança, porém, é necessário que a organização estabeleça políticas e parametrize as configurações para que o IAM atinja plenamente o objetivo de prover maior segurança no gerenciamento de acesso ao ambiente de tecnologia da informação apoiando também as análises da auditoria de sistemas.

REFERÊNCIAS

ALMULLA, Sameera Abdulrahman; YEUN, Chan Yeob. **Cloud Computing Security Management**. 2010. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/5542654. Acesso em: 20 fev. 2024.

BANDAY, M. Tariq; MEHRAJ, Saima. **Directory Services for Identity and Access Management in Cloud Computing**. 2017. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/8389157. Acesso em: 13 abr.2024.

HINTZBERGEN, Jule; HINTZBERGEN,Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Editora Brasport. 2018. Acesso em: 20 fev. 2024.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação**. Editora Atlas. 2016. Acesso em: 05 dez. 2023.

ISACA. **Identity and access management audit program**. Schaumburg, IL: ISACA, 2022. Disponível em: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000005Grc7EAC. Acesso em: 29 abr. 2024.

ISLAMOVA, Oksana V; VOLKOVA, Rimma M. **Effectiveness of Internal Audit of Processes in the Organization**. 2017. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/8085852. Acesso em: 10 abr. 2024.

KOSE, Busra Ozdenizci; COSKUN, Vedat; COSKUN, Arslan. **An Innovative Risk Score Based Corporate Access Control Management System.** 2023. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/10391575. Acesso em: 12 abr. 2024.

MOGHADDAM, Faraz Fatemi; EMADINIA, Tayyebe; WIEDER, Philipp; YAHYAPOUR, Ramin. **A Sequence-Based Access Control Framework for Reliable**

Security Management in Clouds. 2018. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/8458000. Acesso em: 10 fev. 2024.

MICROSOFT. **O que é gerenciamento de identidades e acesso (IAM)?**. 2024. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-identity-access-management-iam. Acesso em: 28 abr. 2024.

MICROSOFT. **O que é gerenciamento de identidade e acesso (IAM)?**. 2024. Disponível em: https://learn.microsoft.com/pt-br/entra/fundamentals/introduction-identity-access-management. Acesso em: 28 abr. 2024.

MICROSOFT. **O que é o Azure Policy?**. 2023. Disponível em: https://learn.microsoft.com/pt-br/azure/governance/policy/overview. Acesso em: 29 abr. 2024.

MICROSOFT. **O que é o RBAC do Azure (controle de acesso baseado em função do Azure)?**. 2023. Disponível em: https://learn.microsoft.com/pt-br/azure/role-based-access-control/overview. Acesso em: 29 abr. 2024.

NAIK, Naik; JENKINS, Paul. **A Security Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards**. 2016. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/7474415. Acesso em: 10 fev. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Security and privacy controls for information systems and organizations**. Gaithersburg, MD: NIST, 2020. Disponível em: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. Acesso em: 25 abr. 2024.

PONGSRISOMCHAI, Sutthinee; NGAMSURIYAROJ, Sudsanguan. **Automated IT Audit os Windows Server Access Control**. 2019. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/8701931/metrics#metrics. Acesso em: 25 abr. 2024.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD. **Auditing Standard No. 5: an audit of internal control over financial reporting that is integrated with an audit of financial statements**. Washington, D.C.: PCAOB, 2007. Disponível em: https://pcaobus.org/oversight/standards/auditing-standards/details/Auditing_Standard_5. Acesso em: 12 abr. 2024.

SHARMA, Anuja; SHARMA, Sarita; DAVE, Meenu. **Identity and Access Management - A Comprehensive Study.** 2015. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/7380701. Acesso em: 13 abr. 2024.

THAKUR, Manav A.; GAIKWAD, Rahul. **User Identity and Access Management Trends in IT Infrastructure - an Overview**. 2015. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/7086972. Acesso em 12 abr. 2024.

TINGLIAO, Li. **The IT audit research based on the information system success model and COBIT.** 2016. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/7727117/authors. Acesso em: 20 fev. 2024.

UDAGATTI, Anusha Koteppa; SUNITHA, N R**. Fault Tolerant Public Auditing System in Cloud Environment**. 2016. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/7912023. Acesso em: 20 fev. 2024.

YANG, Luqiang. **Study on the Improvement of the Internal Audit Work in IT Environment.** 2011. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/6137623. Acesso em: 10 fev. 2024.

ZHOU, Xinyu**. Improvement of information System Audit to Deal With Network Information Security.** 2020. Disponível em: https://ieeexplore-ieee-org.ez338.periodicos.capes.gov.br/document/9258810. Acesso em: 18 fev. 2024.