FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Leonardo Felipe Pellegatti Borges
Raoni Vilela Bastos

AUTENTICAÇÃO MULTIFATOR E SUA APLICAÇÃO NA COMPUTAÇÃO EM NUVEM

Americana, SP
2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Leonardo Felipe Pellegatti Borges
Raoni Vilela Bastos

AUTENTICAÇÃO MULTIFATOR E SUA APLICAÇÃO NA COMPUTAÇÃO EM NUVEM

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Maxwel Vitorino da Silva

Área de concentração: Segurança em Sistemas Operacionais.

Americana, SP
2023

Leonardo Felipe Pellegatti Borges
Raoni Vilela Bastos

AUTENTICAÇÃO MULTIFATOR E SUA APLICAÇÃO NA COMPUTAÇÃO EM NUVEM

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança em Sistemas Operacionais

Americana, 02 de dezembro de 2023

Banca Examinadora:

Prof. Maxwel Vitorino da Silva (Presidente)
Mestre
FATEC Faculdade de Tecnologia de Americana – Ralph Biasi

Prof. Wagner José da Silva (Membro)
Mestre
FATEC Faculdade de Tecnologia de Americana – Ralph Biasi

Prof. Welljnton Aires da Cruz Pereira (Membro)
Mestre
FATEC Faculdade de Tecnologia de Americana – Ralph Biasi

Resumo

Este artigo visa discutir a importância dos métodos de autenticação multifator para acesso a serviços de computação em nuvem e como sua implementação auxilia de forma significativa a melhorar a segurança dos sistemas e dados armazenados e acessados nesses serviços. Durante o desenvolvimento deste artigo será abordado alguns conceitos, como segurança da informação e seus princípios, tipos de serviços de nuvem, tipos de nuvens, autenticação, tipos de autenticação e como a autenticação multifator pode ajudar a prevenir ataques e invasões maliciosas. Também serão discutidos os desafios de sua implementação, como resistência por parte dos usuários e complexidade. Ao final deste artigo, espera-se ter fornecido informações claras e conhecimento que possam elucidar quanto a adoção na prática da autenticação multifator no *Active Directory* como fator chave de segurança para serviços em nuvem.

Palavras-chave: Segurança da Informação; Computação em nuvem; Autenticação Multifator.

Abstract

This article aims to discuss the importance of multifactor authentication methods for accessing cloud computing services and how their implementation significantly helps to improve the security of systems, data stored and accessed in these services. During the development of this article, some concepts will be addressed, such as information security and its principles, types of cloud services, types of clouds, authentication, types of authentications and how multifactor authentication can help prevent attacks and malicious intrusions. Its implementation challenges, such as user resistance and complexity, will also be discussed. By the end of this article, we hope to have provided clear information and knowledge that can clarify the practical adoption of multifactor authentication in Active Directory as a key security factor for cloud services.

Keywords: *Information Security; Cloud Computing; Multi-factor Authentication.*

1 INTRODUÇÃO

Atualmente, a segurança da informação assume um papel cada vez mais proeminente e essencial, não apenas no âmbito da tecnologia da informação, mas também na sociedade como um todo. Grande parte dessa visibilidade decorre de eventos negativos, como notícias sobre empresas sendo vítimas de ransomware ou vazamentos de dados de usuários em determinados sistemas.

Além disso, observa-se um aumento significativo na utilização de serviços de computação em nuvem, tornando imperativa a necessidade de assegurar a proteção dos dados armazenados e acessados nesses serviços, bem como de toda a infraestrutura empregada para viabilizar esse acesso.

Para acessar qualquer serviço na nuvem, é essencial passar pelo processo de autenticação, comumente conhecido como login. Nesse procedimento, o usuário entra em um sistema informático restrito, utilizando credenciais previamente cadastradas, a fim de verificar a autenticidade e determinar se o solicitante é realmente quem afirma ser.

Mesmo diante dos significativos avanços na área de tecnologia da informação, o método de autenticação mais amplamente utilizado ainda se revela relativamente simples e, consequentemente, é considerado o menos seguro: a combinação tradicional de usuário e senha, baseada em um único fator de autenticação. Este método tem sua segurança comprovadamente frágil, especialmente quando confrontado com o poder computacional atual disponível para a quebra de senhas, aliado ao conhecimento e às sofisticadas técnicas dos invasores e demais agentes maliciosos.

Através da análise das questões abordadas no decorrer deste trabalho, procurou-se demonstrar de maneira prática como a autenticação multifator no Active Directory representa um diferencial significativo em termos de segurança na nuvem. Essa abordagem, estruturada em camadas, utiliza um ou mais fatores para substituir métodos menos seguros de autenticação de fator único, resultando em um processo mais robusto e seguro.

2 REFERENCIAL TEÓRICO

2.1 Segurança da Informação

De acordo com Adil (2020), a segurança da informação refere-se ao grupo de atuações para proteção de um conjunto de dados importantes e as informações relacionadas a eles. As suas práticas têm como propósito defender estes dados de desastres tecnológicos, ataques digitais ou de falhas humanas, cumprindo os parâmetros de confidencialidade.

Segundo Sêmola (2014), é indispensável identificar situações de riscos, em que se possa ocorrer a contaminação com vírus por exemplo, através de ferramentas de segurança que consigam avisar os gestores de segurança na detecção de ameaças para a organização.

Para Fontes (2008), é preciso deixar evidente para os usuários que possuem acesso e utilizam os dados, qual é a filosofia da entidade sobre esse recurso, certificando que toda informação da organização e de seus clientes estejam preservadas contra prováveis perdas, danos ou mau uso.

De acordo com Sêmola (2014), o conceito de segurança da informação está conectado a três princípios básicos, nos quais conduzem a confidencialidade, a integridade e a disponibilidade das informações que se deseja defender, porém atualmente estão sendo definidos cinco princípios básicos, que além dos citados acima, incluem autenticidade e não repúdio, que serão definidos a seguir segundo informações reunidas durante o curso:

2.1.1 Confidencialidade

Garantir a confidencialidade dos dados significa que eles ficarão mantidos em sigilo para aqueles que não deveriam ter acesso e que serão somente acessíveis às partes cabíveis. As informações serão organizadas conforme quem poderá ter acesso e em função da sua sensibilidade.

2.1.2 Integridade

A integridade dos dados trata-se da convicção de que os dados não serão alterados por pessoas não autorizadas. Existem resumidamente dois pontos ao longo do processo de comunicação no qual a integridade pode ser comprometida, enquanto carrega os dados ou quando coleta do banco de dados.

2.1.3 Disponibilidade

A disponibilidade garante que as informações estarão disponíveis quando for preciso e para que se evidencie isso, é necessário um sistema com um ótimo desempenho. Isso significa que em qualquer momento precisa estar acessível, estando sempre preparado para reagir quando ocorrerem falhas relacionadas a desastres naturais, de energia, *hardware,* atualizações de sistemas, entre outros.

2.1.4 Autenticidade

Este princípio valida a autorização do usuário, para acessar, transmitir e receber as informações, serve para confirmar sua identidade, impedindo que pessoas não autorizadas as acessem. Um dos mecanismos mais básicos é usuário e senha, que com a constante evolução, hoje dispõe de outras formas mais seguras e modernas para tal, como diversos tipos de MFA.

2.1.5 Não Repúdio

O último princípio tem sua origem no conceito jurídico de irretratabilidade, que no contexto de segurança da informação, trata da garantia que uma pessoa ou entidade não pode negar a autoria da informação fornecida. Deste modo, não se pode negar o que e quando o fez, impossibilitando a negação das ações dos usuários. Neste princípio temos os certificados digitais e assinaturas digitais.

2.2 Computação em Nuvem

Agora que temos a definição de segurança na informação e seus princípios básicos, vamos entender o que é a computação em nuvem, como ela se subdivide e quais os seus tipos de serviço.

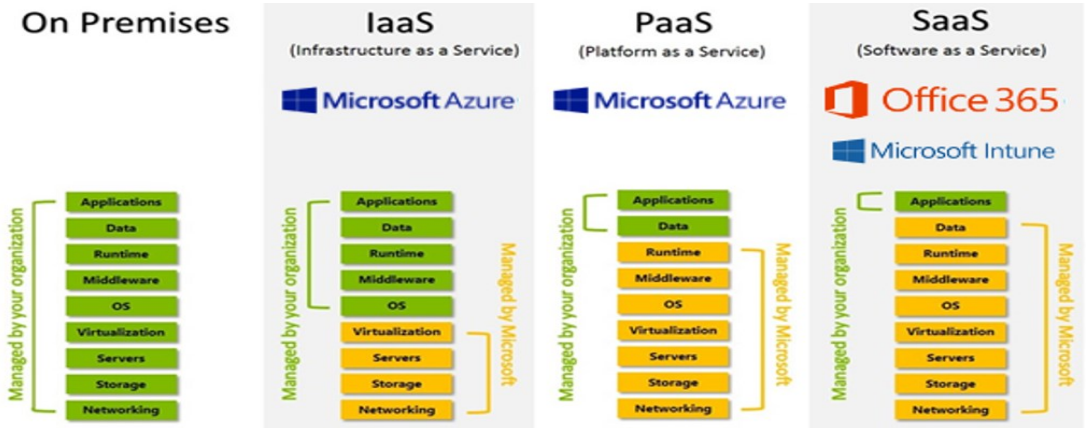
De acordo com Armbrust *et al* (2009) a computação em nuvem se concerne a entrega de serviços de computação através da Internet, incluindo *hardware* e *software* nos *data centers* que oferecem esses serviços. Os autores acima destacam que a nuvem seria o espaço onde são mantidas as informações dos usuários e para acessar estas informações

se dá com o apoio de *softwares* que são capazes de serem conectados a partir de qualquer aparelho que tenha conexão à Internet.

2.2.1 Tipos de Serviço de Nuvem

De acordo com Pedrosa e Nogueira (2011) os tipos de serviço são compostos em três classes como mostrado na Figura 1, essas classes consideram o grau de abstração do recurso possuído e o modelo de serviço do provedor, no qual as funções oferecidas das camadas superiores podem ser utilizadas pelas camadas inferiores.

Figura 1 - Tipos de serviço de nuvem



Fonte: Microsoft, 2017.

2.2.1.1 Infraestrutura como Serviço (IaaS – Infrastructure as a Service)

Segundo Orlando (2011), a infraestrutura como serviço é normalmente independente de plataformas e o seu alvo é em providenciar a infraestrutura ao usuário, englobando como por exemplo: banco de dados, processamento, armazenamento e redes. O autor ressalta que IaaS compreende uma fusão de recursos de *hardware* e *software*.

O *software* IaaS é desenvolvido em código de baixo nível e funciona de forma separada do sistema operacional, no qual sua obrigação é listar os recursos de *hardware* e destiná-los de acordo com a demanda.

Para Veras (2015), os principais pontos a serem destacado do IaaS são:

- Redução de investimentos em hardware, já que eles são proporcionados pelo provedor.
- Escolher um ótimo fornecedor, pois é ele que irá garantir um bom desempenho, segurança e qualidade de serviço.
- O usuário é encarregado por toda a administração, desde o sistema operacional até os aplicativos. Por muita das vezes preferirem manter o controle total sobre seus aplicativos e infraestrutura.

2.2.1.2 Plataforma como Serviço (PaaS – Platform as a Service)

Pedrosa e Nogueira (2011) denominam este serviço de camada intermediária, onde por exemplo um desenvolvedor pode produzir sem ter o trabalho de se preocupar com processamento ou consegue implantar na infraestrutura um *software* que ele desenvolveu, com a circunstância de que a tecnologia e a linguagem de programação sejam suportadas pelo provedor da plataforma.

Pasik (2012) afirma que os provedores de PaaS diminuem o trabalho que o setor de TI teria para cuidar de serviços como servidores, banco de dados e ambientes de desenvolvimento, mas neste caso o acesso seria mais restrito para a utilização dos ambientes e a implementação nestas camadas.

Brunetti (2011) destaca alguns pontos importantes do PaaS:

- O fornecimento e gerenciamento desde a conexão com a rede até o sistema operacional, pois eles são proporcionados pelo provedor.
- Diminui o excesso de trabalho de um desenvolvedor, pois o ambiente vai estar pronto e eles já conseguem começar a desenvolver.
- Oferece a capacidade de crescer a produtividade já que toda a parte de hardware é responsabilidade do provedor.

2.2.1.3 Software como Serviço (SaaS – Software as a Service)

Segundo Pedrosa e Nogueira (2011), neste serviço o provedor oferece uma aplicação que é executada em sua respectiva nuvem. Com o SaaS o provedor desenvolve o *software* e efetua as atividades de manutenções corretivas, *backup* e monitoramento.

Conforme Borges et al (2011), no SaaS os sistemas suportam aplicações concluídas ou conjuntos de aplicações das quais sua utilização é mesurada por modelos de negócios que autorizam personalização.

Para Taurion (2009) a popularidade deste serviço é vinculada as vantagens que ela apresenta, como as que são citadas abaixo:

- Redução em gastos com capital.
- Agilidade no processo de instalação e acesso de novas funcionalidades ou versões de um processo existente.
- Facilidade na manutenção e *upgrades* de aplicativos.

2.2.2 Modelos de Nuvem

O NIST - National Institute of Standards and Technology destaca que a análise da escolha de um modelo de nuvem que atenda às suas necessidades é essencial antes que ocorra a implantação. Para isso, é preciso entender para qual nicho cada tipo de modelo é destinado, os principais utilizados são: público, privado e híbrido de acordo com o NIST (2011) e Isaca (2009) como apresentado na Figura 2.

Figura 2 - Modelos de nuvem

Fonte: Microsoft, 2017.

2.2.2.1 Nuvem Privada

Neste modelo de nuvem seu gerenciamento é feito por terceiros ou pela própria organização, assim a nuvem privada seria criada em um *data center* particular. As ferramentas usadas para fornecer tais particularidades são capazes de ser em nível de administração de redes, configurações dos fornecedores de serviços e a utilização de tecnologias de autorização e autenticação.

2.2.2.2 Nuvem Pública

A nuvem pública é um modelo de computação em nuvem onde os recursos de infraestrutura, como servidores e armazenamento por exemplo, são disponibilizados pela provedora de serviços na internet para uso público.

Empresas e usuários podem acessar e utilizar esses recursos de maneira flexível, pagando apenas pelo consumo contratado. Oferece um ganho em escalabilidade, agilidade e redução de custos, permitindo que organizações foquem em suas operações sem a necessidade de gerenciar fisicamente a infraestrutura.

2.2.2.3 Nuvem Híbrida

O modelo híbrido é formado de dois ou mais modelos de nuvem: pública e privada, onde os aplicativos são usados em uma combinação de serviços, computação, armazenamento e se mantem como entidades únicas, sendo conectadas através de uma ferramenta padronizada ou proprietária.

2.3 Autenticação

Agora que já se definiu o que é o que é segurança na informação, os modelos e tipos de serviço em nuvem, abordaremos como a autenticação e seus tipos agem como métodos de verificação para que o usuário comprove que é ele mesmo que está tentando o acesso.

De acordo com a Raboy (2014), a autenticação é a ação de validar se algo ou alguém é autêntico, assim, certificando que qualquer argumento sobre algo é verídico. As maneiras de um usuário se autenticar em um dispositivo variam, seja por senhas, biometria, certificados e outros tipos.

Hoje em dia para que uma técnica de autenticação seja avaliada segura é preciso ser considerado que mesmo que um atacante identifique as credenciais de acesso de alguma pessoa através de furto ou espionagem da conexão do usuário com alguma aplicação, a permissão aos dados seja bloqueada.

A autenticação multifator garante esta metodologia, entretanto é necessário certificar que o método utilizado seja seguro, unidirecional e possa ser executado pelo usuário em qualquer dispositivo (ALOUL *ET A*L, 2009).

2.3.1 Autenticação multifator (MFA)

Segundo Aloul *et al* (2009), a autenticação multifator é um item essencial que faz parte do gerenciamento de acesso e identificação. Esse método requer pelo menos dois tipos de autenticação para que o usuário consiga acessar qual seja o dispositivo. O autor destaca que uma condição na autenticação é o método de comprovar a identidade no ato de tentar logar.

Para isso, a pessoa tem que misturar ao menos dois tipos diferentes de autenticação, os fatores são divididos em três níveis:

- Algo que a pessoa é: este grupo se encaixa dados biométricos, como impressão digital, varreduras de retina, reconhecimento facial e de voz.
- Algo que a pessoa sabe: geralmente um PIN, uma senha ou perguntas de segurança com resposta conhecida apenas pelo usuário.
- Algo que a pessoa tem: hoje são mais utilizados autenticadores instalados em smartphones para gerar chaves de segurança.

2.4 Active Directory (AD)

Conforme o Microsoft Learn (2023) Active Directory é uma estrutura hierárquica que armazena informações sobre os objetos na rede. Fornece os métodos necessários para armazenar dados de diretórios e disponibilizá-los para administradores e usuários da rede.

Esse armazenamento de dados, também conhecido como diretório, contém informações sobre os objetos do Active Directory. Esses objetos normalmente incluem recursos compartilhados, como servidores, volumes, impressoras, além das contas de usuário e de computador da rede.

A segurança é integrada ao Active Directory por meio da autenticação de logon e do controle de acesso aos objetos no diretório. Com um logon de rede único, os administradores podem gerenciar dados de diretório e da organização em toda a rede e os usuários de rede autorizados podem acessar recursos em qualquer lugar da rede.

2.4.1 Domínio

Um domínio é o agrupamento lógico de objetos relacionados, como usuários, computadores ou grupos, ou recursos compartilhados, como impressoras, arquivos ou pastas, todos controlados ou atendidos por um ou mais Controladores de Domínio.

Todos os objetos em um domínio específico compartilham o mesmo banco de dados do AD. Os domínios geralmente são identificados por um nome fornecido pelo DNS, como “artigofatec23.com”.

2.4.2 Controlador de Domínio (DC)

Um DC é o servidor que possui o AD instalado nele. A promoção de um servidor a um DC permite que ele gerencie permissões centralmente, controle a autenticação de identidades de usuários e autorize o acesso a vários recursos, incluindo armazenamento de arquivos, aplicativos e outras rede conforme Microsoft Learn (2023).

3 METODOLOGIA

3.1 Tipo de Pesquisa

Embasado pelo Microsoft Learn (2023), para este estudo foi realizada uma pesquisa experimental, envolvendo a criação de um Domínio no Active Directory na plataforma de cloud pública Azure, criação de usuários e configurações de acesso utilizando a autenticação multifator disponível para o tipo de usuário estudante, o qual os autores possuem acesso devido a parceria entre o Centro Paula Souza e a Microsoft.

3.2 Coleta de Dados

Esta pesquisa irá explorar a validação de segurança para acesso a um domínio no AD através da configuração de MFA disponível no Azure. A partir dos resultados obtidos, será possível trazer de maneira clara como é o processo para configuração e habilitação da

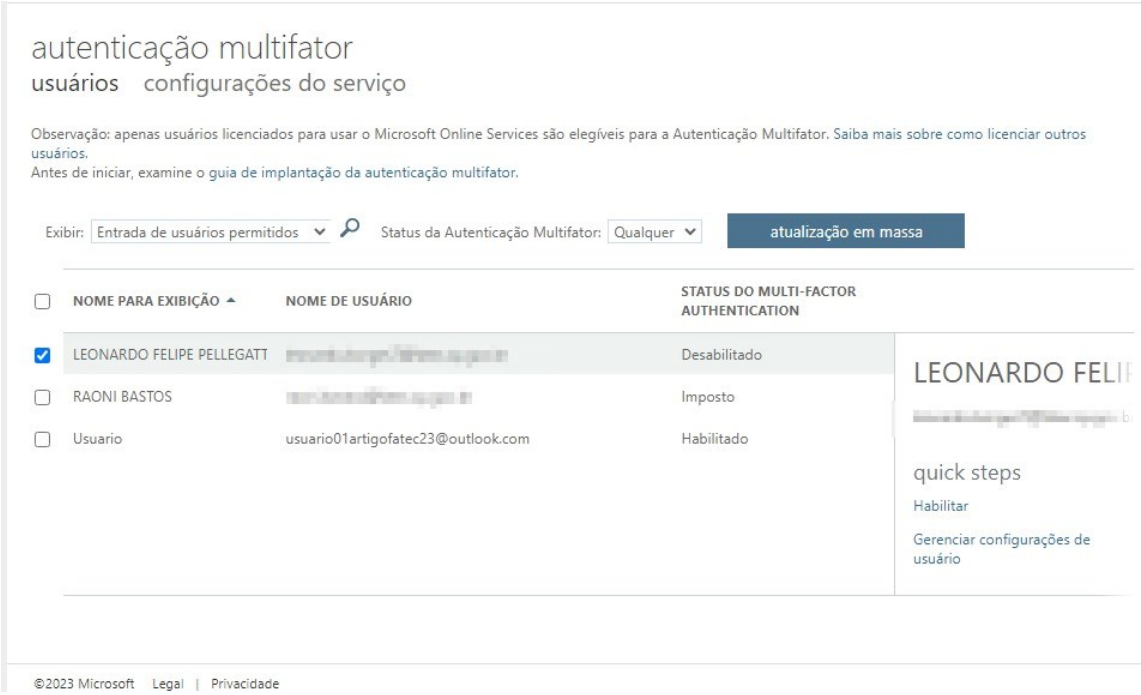
autenticação multifator de usuários utilizando recursos providos pela solução da Microsoft Azure Active Diretcoty e sua aplicabilidade na prática.

4 ANÁLISE E DISCUSSÃO DE RESULTADOS

4.1 Configurações Autenticação Multifator

Dentro do ambiente do Active Directory no Azure, como apresenta-se na Figura 3 o usuário denominado “Leonardo Felipe Pellegatti” está dentro do domínio, porém com o status da autenticação multifator “Desabilitado”.

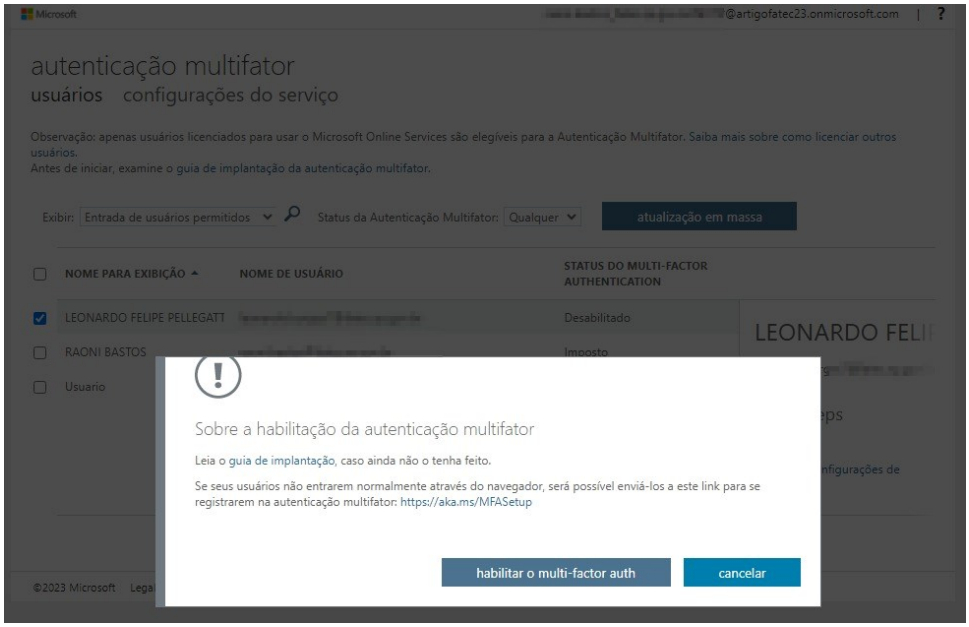
Figura 3 – Configurações Autenticação Multifator



Fonte: Autores

Desta forma como observado na Figura 4, habilitou-se a autenticação multifator para este usuário.

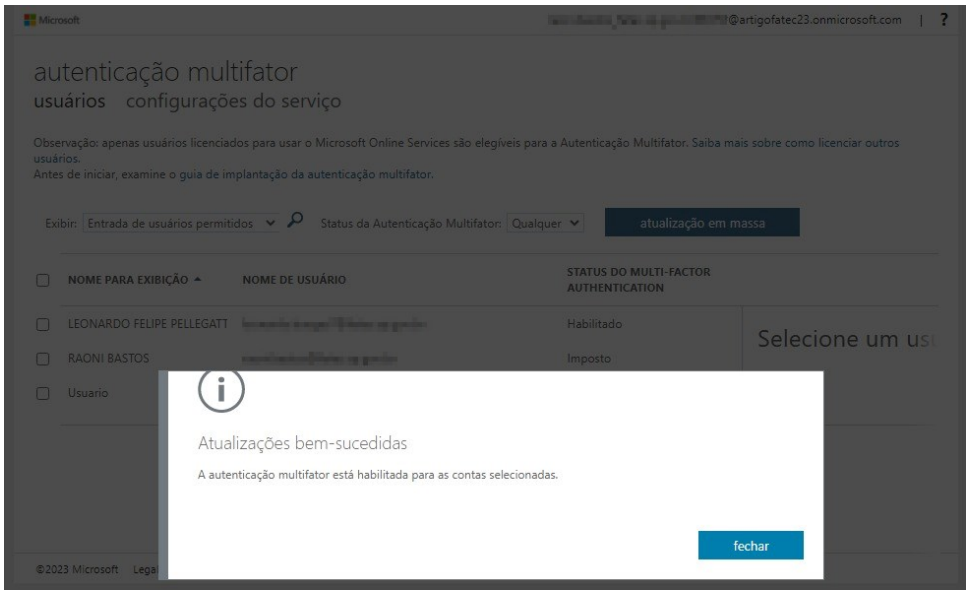
Figura 4 – Habilitar a autenticação multifator



Fonte: Autores

Na Figura 5 têm-se o informativo que a atualização para multifator foi habilitada com sucesso.

Figura 5 – Autenticação Multifator habilitada



Fonte: Autores

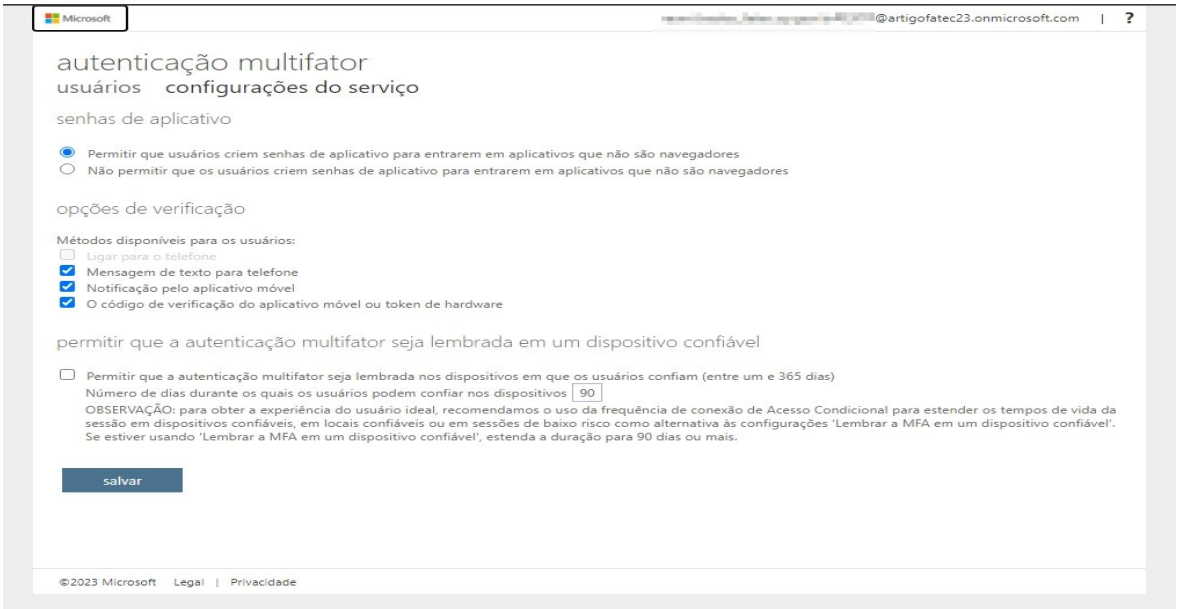
A Figura 6 mostra-se as configurações do serviço de autenticação multifator, onde é interessante frisar que habilitamos três métodos diferentes para tal:

- Mensagem de texto para telefone

- Notificação pelo aplicativo móvel

- Código de verificação do aplicativo móvel ou token de hardware

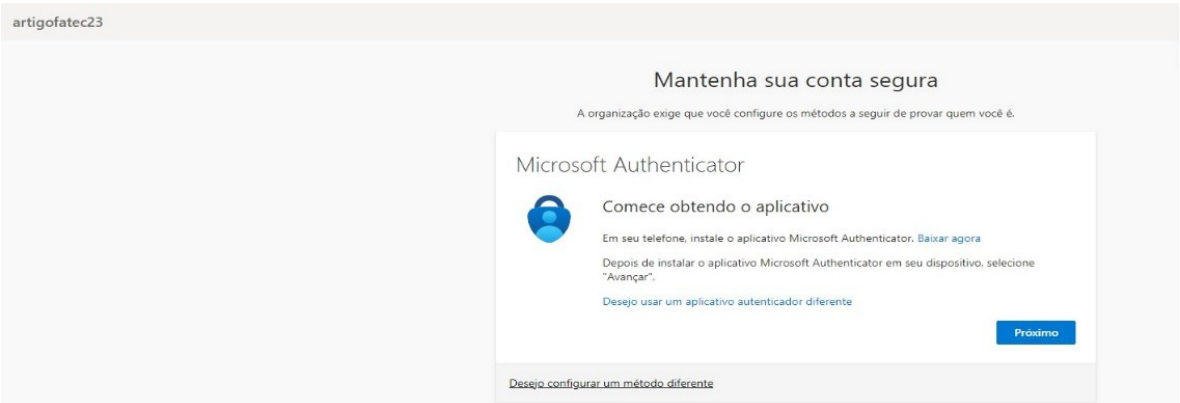
Figura 6 – Configurações Autenticação Multifator



Fonte: Autores

Após a implementação das configurações delineadas na Figura 6, quando o usuário tenta acessar qualquer serviço dentro do domínio configurado, é imperativo que ele conclua a autenticação multifator, conforme evidenciado na Figura 7.

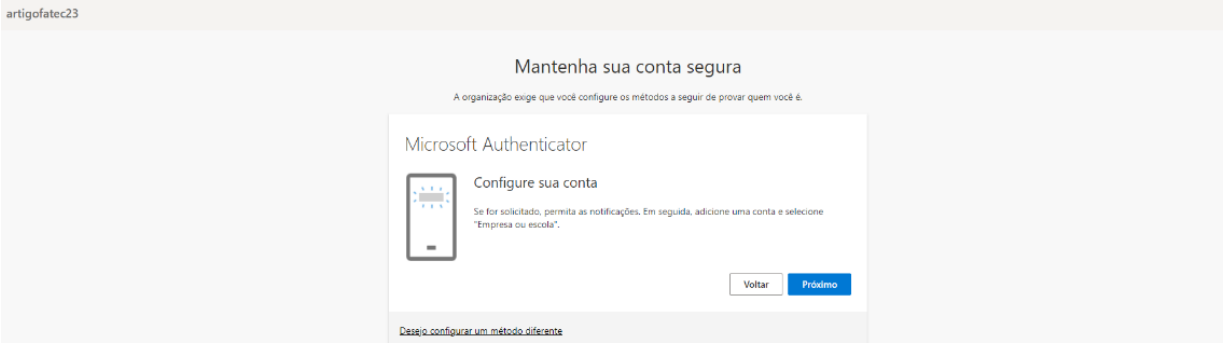
Figura 7 – Microsoft Authenticator 01



Fonte: Autores

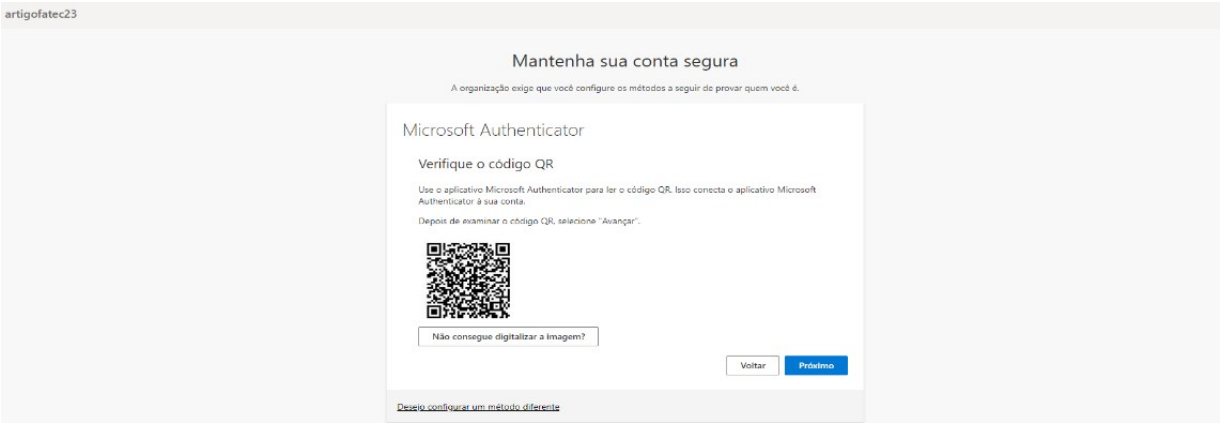
A Figura 8 e Figura 9 observa-se o usuário efetuando as configurações no Microsoft Authenticator.

Figura 8 – Microsoft Authenticator 02



Fonte: Autores

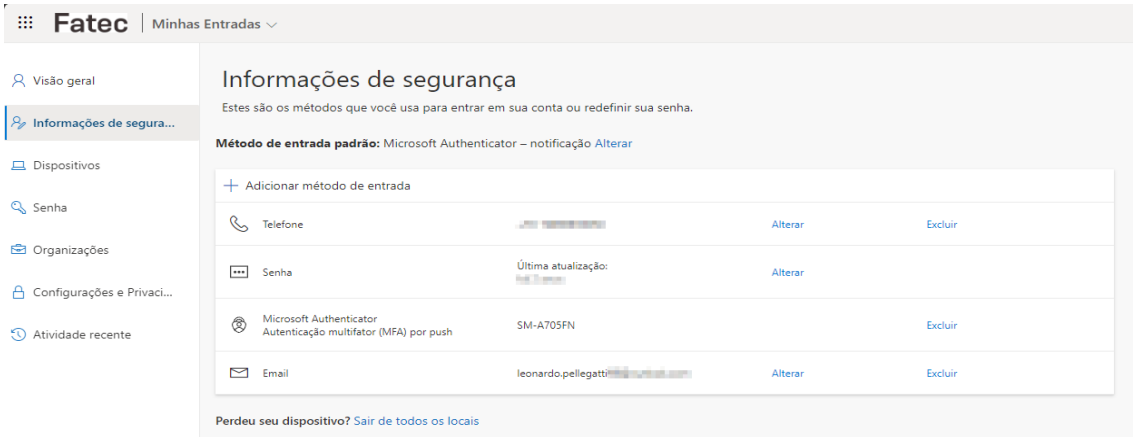
Figura 9 – Leitura do código QR através de um dispositivo móvel



Fonte: Autores

Após as configurações das Figuras 8 e 9, ficou disponível dentro do Active Directory, as informações de segurança deste usuário, com o método de autenticação utilizado, neste caso, o Microsoft Authenticator como apresentado na Figura 10.

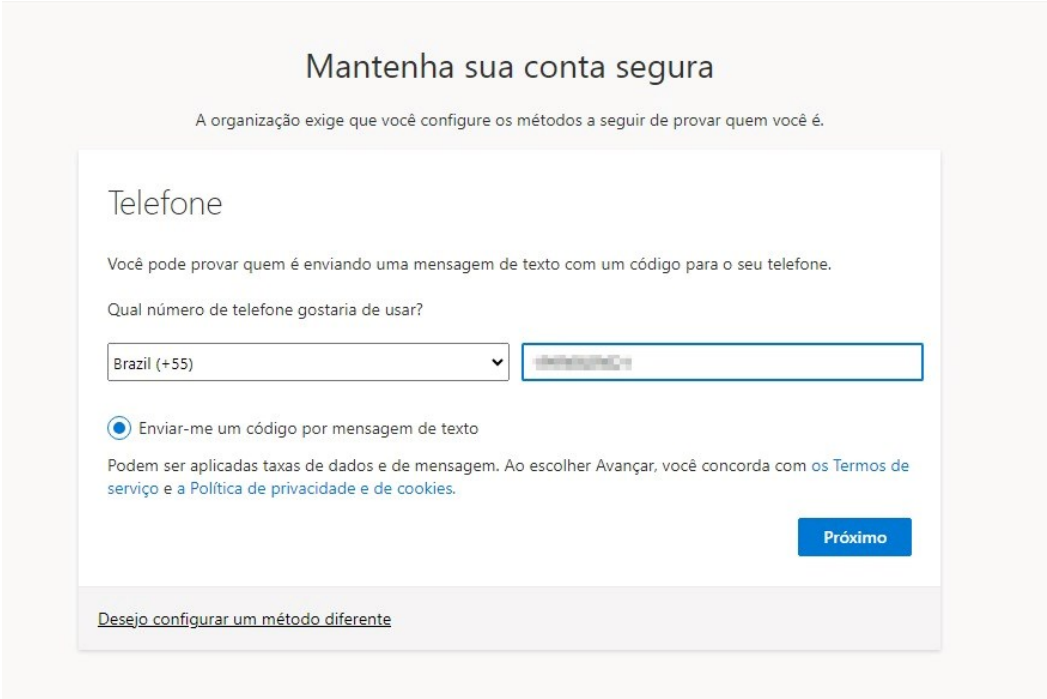
Figura 10 – Informações de Segurança



Fonte: Autores

Outro método disponível, é a autenticação multifator com validação de identidade como mostrado na Figura 11, através dessa mensagem de texto (SMS) enviada para o número de telefone, o mesmo irá gerar o código validador.

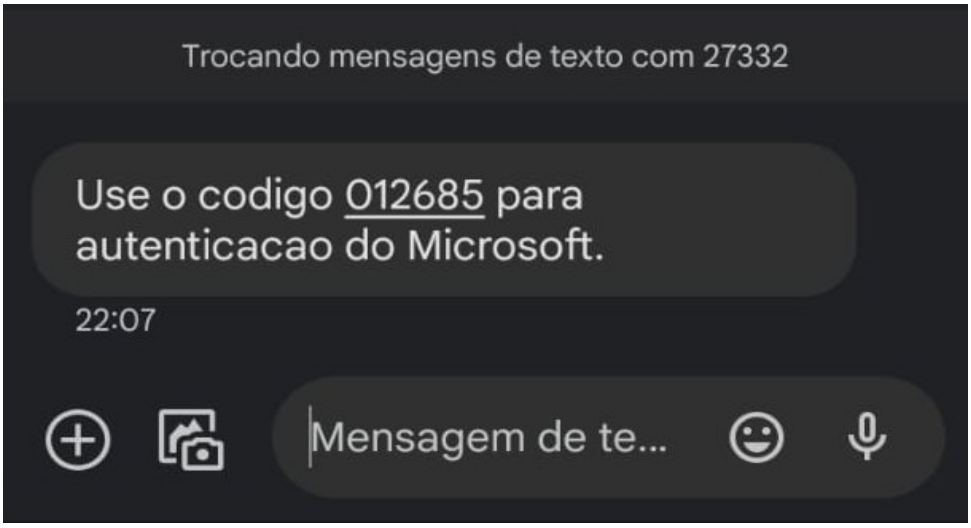
Figura 11– Autenticação por mensagem de texto



Fonte: Autores

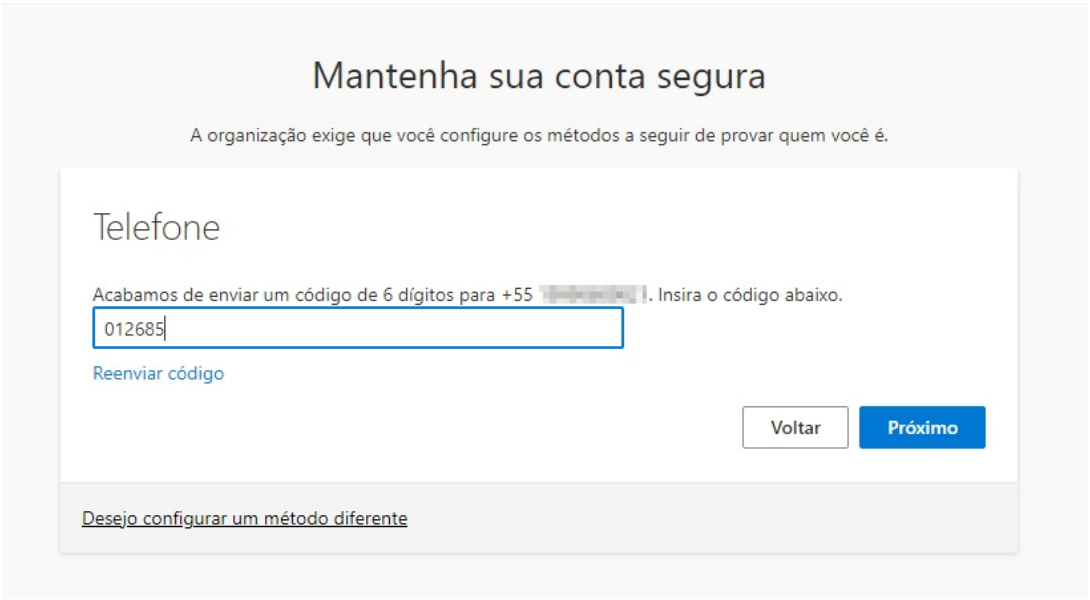
Na Figura 12 observa-se o código recebido via mensagem de texto (SMS) no aparelho celular do usuário e na Figura 13 a inserção deste código dentro do autenticador.

Figura 12 – Recebimento da mensagem de texto com código para autenticação



Fonte: Autores

Figura 13 – Inserção de código validador



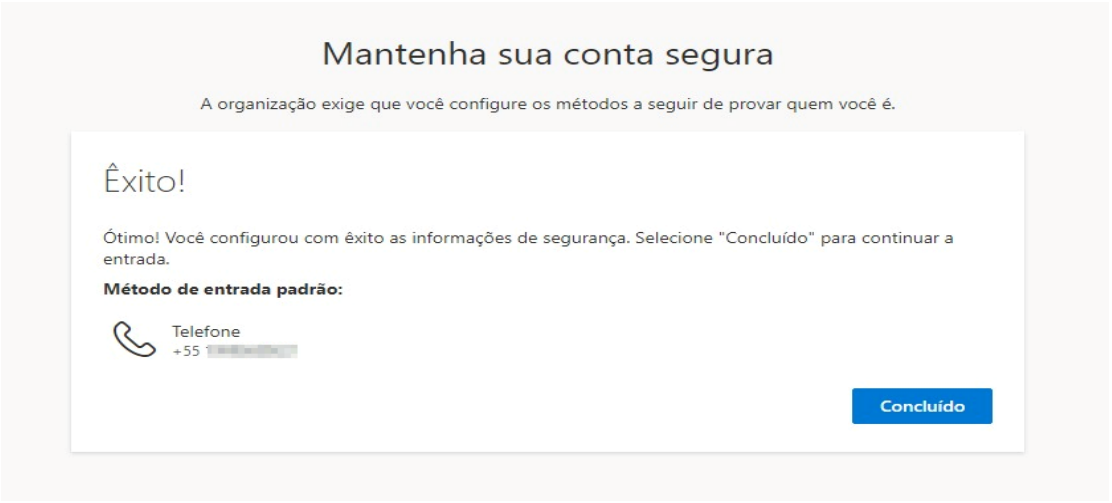
Fonte: Autores

Após a inserção do código mostrada na Figura 13, temos a mensagem de confirmação de “SMS verificado” na Figura 14 e na Figura 15 e mensagem de “Êxito” juntamente com o método padrão de entrada utilizado e o número do telefone.

Figura 14 – Confirmação de validação 01

Fonte: Autores

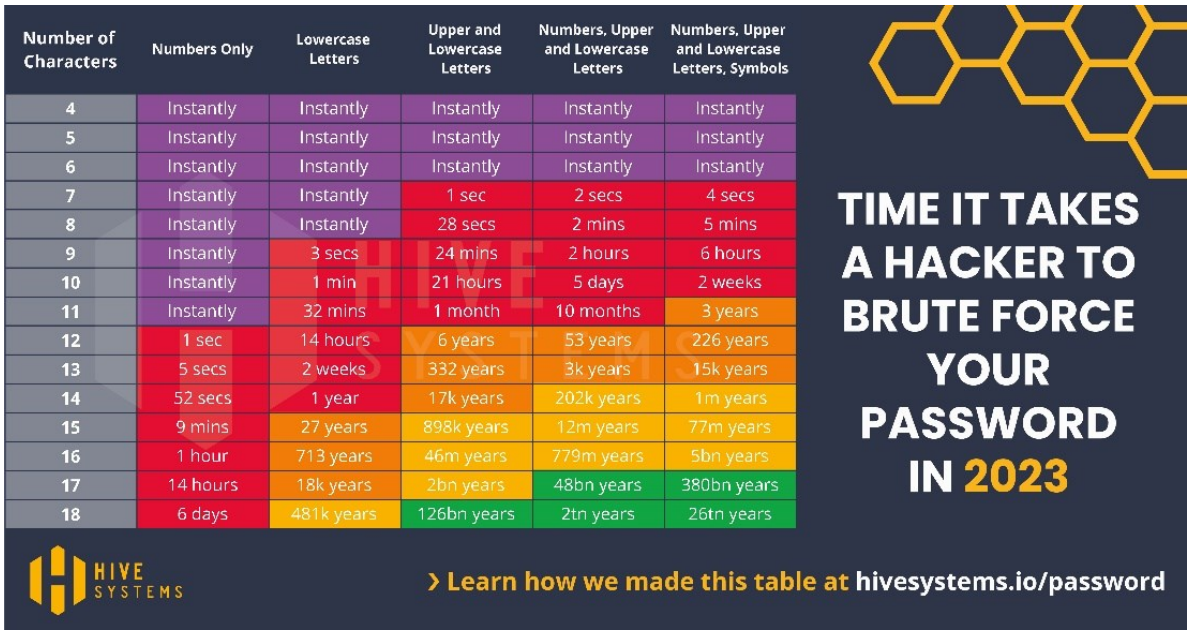
Figura 15 – Confirmação de validação 02



Fonte: Autores

Na Figura 16 apresenta-se uma imagem com uma tabela do tempo que um hacker levaria para quebrar uma senha, utilizando força bruta, no ano de 2023 com a tecnologia disponível.

Figura 16 – Tabela de quebra de senhas 2023



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Fonte: Hive Systems

A partir da tabela apresentada na Figura 16 e as práticas realizadas nesse artigo, demonstrou-se que a abordagem em camadas da autenticação multifator, utilizando um ou mais fatores, além do tradicional usuário e senha, é uma resposta eficaz aos desafios de segurança enfrentados pelos métodos de autenticação de fator único, que oferece mais resistência e robustez contra ataques maliciosos ao reconhecer as vulnerabilidades associadas ao uso exclusivo de usuário e senha.

Apesar de a implementação em si não ser excessivamente complexa, é imperativo lidar com a resistência dos usuários, visto que a eficácia de qualquer sistema de segurança está intrinsecamente ligada à aceitação e compreensão por parte dos usuários. A disseminação da conscientização sobre os benefícios da autenticação multifator, como uma camada adicional de segurança, desempenha um papel crucial na superação desses desafios.

5 CONSIDERAÇÕES FINAIS

Este artigo apresentou uma análise dos desafios da segurança da informação, com foco na autenticação dos usuários. Como visto durante o desenvolvimento e exemplo prático, conclui-se que a implementação de autenticação multifator no Active Directory dentro do Azure representa um avanço significativo na segurança dos serviços em nuvem,

destacando-se a necessidade de métodos mais robustos de autenticação para proteger desde a infraestrutura até os dados mais sensíveis.

A implementação bem-sucedida no Active Directory não apenas fortalece a segurança dos serviços em nuvem, uma vez que enfatiza a responsabilidade compartilhada na proteção dos dados. Para isso, é fundamental incluir a promoção contínua da conscientização e educação em segurança cibernética, garantindo que a autenticação multifator seja percebida não apenas como uma medida de segurança, mas como algo essencial na era da computação em nuvem.

Por fim, este artigo tem como objetivo central deixar como legado a compreensão de que a segurança da informação é uma responsabilidade compartilhada, e que a conscientização e educação dos usuários são elementos cruciais para fortalecer a postura defensiva contra as ameaças cibernéticas em constante evolução.

REFERÊNCIAS

ADIL, J. **Segurança da informação:** o que é e qual sua importância. ACADI-TI, [s.d.]. Disponível em: https://acaditi.com.br/seguranca-da-informacao-o-que-e-e--qual-sua-importancia/. Acesso em: 03 mar. 2023.

ALOUL, F., *et al*. Multi factor authentication using mobile phones. **International Journal of Applied Mathematics and Computer Science**, v. 2, p. 65–80, 2009. Disponível em: https://www.researchgate.net/publication/228972704_Multi_Factor_Authentication_Using_Mobile_Phones. Acesso em: 04 abr. 2023.

ARMBRUST, M., *et al*. **Above the clouds:** a Berkeley view of cloud computing. Berkeley EECS, 2009. Disponível em: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf. Acesso em: 26 mar. 2023.

BORGES, H., *et al*. **Computação em nuvem**. Fortaleza: [s.n], 2011. 42 p.

BROOK, J. **CIPP/US prep guide**. Estados Unidos: [s.n], 2016. 53 p.

BRUNETTI, R. **Windows Azure step by step**. Estados Unidos: Microsoft Press. 2011. 120 p.

FONTES, E. **Praticando a segurança da informação**. São Paulo: Brasport, 2008.

ISACA, A. **Emerging Technology. Cloud Computing**: Business benefits with security, governance and assurance perspectives. 2009. Disponível em: http://viewer.media.bitpipe.com/1234308720_690/1300892427_939/Cloud-Computing-28Oct09-Research.pdf. Acesso em: 15 abr. 2023.

ORLANDO, D. **Modelos de serviço de computação em nuvem**: infraestrutura como serviço. 2011. Disponível em: http://www.ibm.com/developerworks/br/cloud/library/cl-cloudservices1iaas/. Acesso em: 24 mar. 2023.

PASIK, A. **Considerações sobre o modelo de cloud e desafios da integração de sistemas**. 2012. Disponível em: http://informationweek.itweb.com.br/6588/os-pros-e-contras-da-computacao-emnuvem/. Acesso em: 18 mar. 2023.

PEDROSA, P. H. C; NOGUEIRA, T. **Computação em nuvem.** 2011. Disponível em: http://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf. Acesso em: 20 mar. 2023.

NIST (National Institute of Standards and Technology). **The NIST definition of cloud computing.** 2011. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-145/final. Acesso em: 27 mar. 2023.

RABOY, N. **Generate time-based one-time passwords with JavaSript.** THE POLYGLOT DEVELOPER. 2014. Disponível em: https://www.thepolyglotdeveloper.com/2014/10/generate-time-based-one-time-passwords-javascript/. Acesso em: 01 abr. 2023.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Editora Campus, 2014.

TAURION, C. **Cloud computing** - computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009. 201p.

VERAS, M. **Computação em nuvem:** nova arquitetura de TI. Rio de Janeiro: Brasport, 2015. 174 p.

MICROSOFT. Documentação de autenticação do Microsoft Entra, 2023. Disponível em: https://learn.microsoft.com/pt-br/entra/identity/authentication/, Acesso em 02, Nov, 2023.

MICROSOFT. Como usar o aplicativo Microsoft Authenticator, 2023. Disponível em: https://support.microsoft.com/pt-br/account-billing/como-usar-o-aplicativo-microsoft-authenticator-9783c865-0308-42fb-a519-8cf666fe0acc, Acesso em 02, Nov, 2023.

APL TIC - Associação dos Profissionais e Empresas de Tecnologia da Informação. 5 pilares da segurança da informação, 2023. Disponível em: https://apeti.org.br/blog/os-5-pilares-da-seguranca-da-informacao, Acesso em 07, Nov, 2023.

HIVE SYSTEMS. Hive Systems Password Table, 2023. Disponível em: https://www.hivesystems.io/password-table, Acesso em 07, Nov, 2023.